Communications of the Association for Information Systems

Volume 3 Article 18

June 2000

Electronic Commerce: A Half-Empty Glass?

Sasha Dekleva
DePaul University, sdekleva@condor.depaul.edu

Communications of the Association for Information Systems

Volume 3, Article 18
June 2000

ELECTRONIC COMMERCE:
A Half-Empty Glass?

Sasa Dekleva
DePaul University
sdekleva@depaul.edu

ELECTRONIC COMMERCE

ELECTRONIC COMMERCE: A Half-Empty Glass?

Sasa Dekleva
DePaul University
sdekleva@depaul.edu

ABSTRACT

This article introduces an electronic commerce paradox by observing that while electronic commerce grows rapidly it is, at the same time, based on unsettled foundations. It describes how 22 constraints for global electronic commerce were identified, and analyzes them in depth. The constraints fall into four themes:

- Building trust for users and consumers
- Establishing ground rules for the digital marketplace
- Enhancing information infrastructure
- Maximizing benefits.

Each of these themes contains a number of critical issues. The first theme--building trust for users and consumers--involves privacy protection, security, consumer protection, authentication and confidentiality, and access blocking. The second theme includes legal framework, acceptance of electronic transactions, taxation, tariffs, intellectual property protection, commercial policy, and payment systems. Enhancing information infrastructure covers the needed infrastructure enhancements and includes Internet infrastructure and governance, interconnectivity and technical convergence, technical standards, bandwidth and accessibility, and the question of how to further the competition. The last theme is about maximizing the benefits of electronic commerce and includes the understanding of digital economy, its measurement, seamless globalization, and involvement of small businesses. At the time that this paper

was written (February 2000) none of these 22 issues had been resolved. Yet, they need to be worked out if electronic commerce is to be successful in both the developed and the underdeveloped world.

A fast way to read this extensive paper is to read the first three sections and then skip to the summary and conclusions presented in the last two sections, referring to the four detailed sections that form the body of the paper as needed.

Keywords: Electronic commerce, electronic business, global digital economy, global e-commerce, global marketplace, e-commerce constraints, e-commerce impediments, Internet

Editor's Note: The author's work on the material in this article was completed in February 2000. The author added endnotes that cover events that occurred while the paper was in the publication process. By the time the reader sees the article, events may have occurred that either reinforce or contradict the findings. These are differences in detail and, in the editor's opinion, do not contradict the basic results.

"The newest innovations, which we label information technologies, have begun to alter the manner in which we do business and create value, often in ways not readily foreseeable even five years ago."

Alan Greenspan
Chairman, Federal Reserve Board, May 6, 1999

I. INTRODUCTION

The following two quotes exemplify a paradox of electronic commerce: it is thriving but has rickety foundations.

"Any doubts about the viability of E-commerce were erased by last December's holiday shopping season, when Web sales tripled over the

same period the year before, according to the Boston Consulting Group and Forrester Research" [Larsen 1999].

"But what if the products don't arrive, or the wrong product is delivered, or somehow the advertising, marketing or sale by the seller is inconsistent with the laws of the consumer's country? Should an American firm that compares the merits of different diet colas be subject to prosecution in northern Europe for violating a law prohibiting comparative advertising? Should a clothing store be subject to prosecution in a Muslim country for exposing a woman's arms? Should a toy store be subject to prohibitions on advertising to an under-age audience? And does the consumer have to bring an action in the foreign country if the product or service never arrives or is not what was ordered?" [Pitofsky 1999]

This paper first identifies issues that the U.S. government and the Organisation for Economic Co-operation and Development (OECD) recognize as current constraints on global electronic commerce. We analyze these obstacles in some detail and then try to assess the likelihood of the global digital economy ever flourishing.

The article is rather extensive. Its gist can be obtained by reading sections II and III, skipping straight to the Summary and Conclusions (Sections VIII and IX), and referring to the body of the article as needed. More inquisitive readers should read the article sequentially as it is presented.

The general tone of this article is admittedly negative, perhaps "devil's advocacy." And it is so for a reason, and a positive reason at that. Many writings reflect buoyant optimism about the growth of electronic commerce and growth of services on the Internet. Such works of technological utopianism fail to carefully engage in critical questions about the downsides of the explosion of excitement over computer networks. Although utopian visions often serve important roles in giving people a positive sense of direction, they can mislead when their architects exaggerate the likelihood of easy and desirable social changes [Kling 1996].

It is possible that the stunning and almost continuous improvements in technologies and their applications created an overwhelmingly positive situation. Public discussion of electronic commerce, especially in the media, centers around global electronic commerce as a *fait accompli*, a done deal. The world is wired, the globe is booted, and all we need now do is click, sell and shop to our heart's content. But the realities of the situation--which form the bulk of the analysis in this article--are far different from the public perception. Many serious issues are unresolved, fundamental issues such as legal and political infrastructures, for example, or security, fraud prevention, privacy protection, agreement on business practices, tariffs and taxes, to mention a few. A corrective is, we feel, needed, to focus attention on what still needs to be done before the dreams of global electronic commerce can be realized. Thus the tone of warning, of caution in this article. We have far to go, many obstacles to overcome, and tough work ahead.

II. ELECTRONIC COMMERCE IS EXPLODING

It is not hard to find enthusiastic praise for the potential of electronic commerce and the commercial use of the Internet in general. Mass media keep reporting about it and trade journals even more so. *Fortune*'s Dec. 7, 1998 cover page, for example, screamed to readers "INTERNET or BUST!" and in a somewhat smaller print "Don't get left in the dust. The smartest companies are using the Net to create a whole new way of doing business. Call it the E-Corporation" [Anonymous 1998a]. Another analyst was only slightly more tentative: "When it comes to creating value in the network economy, questions still outnumber answers. But the evidence is growing. Firms that don't reinvent their business models around the Net will be bypassed and fail" [Tapscott 1999].

Washington Post analysts similarly concluded that "The fanfare, inflated stock prices and overnight paper fortunes that surround the Internet's manic incursion into American life obscured an important shift: The industry is graduating from a speculative casino into a measurable force that is changing nearly every corner of modern capitalism" [Leibovich, Smart, and Dugan 1999].

The evidence for a fast expansion of electronic commerce is, indeed, growing. Three years ago, during the early period of Internet commercialization, market researchers' predictions for Web sales by 2001 varied from a few billion to more than $100 billion. Recalling all-over-the-map market projections, S. Eckert, director of Dell Online, commented "The only thing we knew was that none of them was right. But they all had a positive trend" [Kalin 1998]. We know now that all these reports underestimated the growth of Internet commerce. For example, economists at the University of Texas attempted to provide a comprehensive accounting of the "Internet economy" by examining spending on computers, telecommunications gear, consultants, software, brokerage firms and advertising, as well as electronic commerce. U.S. Internet-related businesses accounted for $301 billion in revenue and 1.2 million jobs in 1998. Electronic commerce accounted for about one-third of the total, or $102 billion. Researchers suggest that Internet-related industries roughly rival the automobile or energy sector in size. [Anonymous June 1999]

The U.S. Secretary of Commerce, William Daley observed: "Last spring, I released *The Emerging Digital Economy*, the Department of Commerce's first report measuring the development of electronic commerce. I wrote then that the report aimed to provide us with a clearer understanding of the 'promise' of electronic commerce -- 'a future with more opportunity and prosperity' for all Americans. That promise is being fulfilled" [Daley, 1999b].

These assessments suggest that the growth of the digital economy and Internet-based global electronic commerce surpass all our expectations. We seem to be experiencing the dawn of a new era where our world will be smaller, little players will have easy access to global markets, and newly generated wealth will energize economies all over the world.

When we look into this prospect analytically, however, the forecast evolution does not appear, as various reports and media suggest, smooth, sweeping, and immediate.

III. IMPORTANT ISSUES

Despite wild enthusiasm about the explosion of the business use of the Internet, and because of the related paradigm shift, many fundamental issues still need to be resolved. Two of the most arguably important documents fostering electronic commerce were used to compile a list of such issues, as was a third document, which is an update of the first one.

- President Clinton and Vice President Gore issued the first document [Clinton and Gore 1997] on July 1, 1997. They presented a number of issues to be resolved by the start of the year 2000 to facilitate a global "digital economy."
- The second document [OECD 1998a] and related materials present the conclusions of OECD Ministerial Conference held in Ottawa in Oct. 1998.
- The third source used in compiling the important issues is a report [WGEC 1998] by the U.S. Government Working Group on Electronic Commerce, published in November 1998. The Working Group presented an update on activities requested by Clinton and Gore and added five newly recognized issues in need of governmental or international attention and resolution. The latest update [WGEC 1999] did not identify any new issues.

The list of critical issues used for this study thus contains obstacles to a global digital economy, as defined by the Clinton Administration, the U.S. Government Working Group on Electronic Commerce, and the most active and influential international entity involved in setting up the rules of electronic commerce, the OECD. We do not claim that the list is complete but argue that it defines issues that the U.S. and other governments of the developed countries are addressing in an attempt to facilitate the transition into the global digital economy. We will discuss the state of resolution of each issue listed to assess how easy, extensive, and rapid this transition is likely to be.

CEOs from leading companies from all regions of the world met on January 14, 1999 in New York to launch the Global Business Dialogue on

Electronic Commerce (GBDe) [GBDe 1999]. Working groups were established to "pursue action-oriented policy initiatives including a conference on the issues of protection of personal data, consumer confidence, liability, taxation and tariffs, jurisdiction, infrastructure (including interoperability and Internet governance), content, protection of intellectual property rights, as well as authentication and security." We address all of these issues and a few additional ones in this article, which reassures us that at least the major constraints are being examined.

The Ottawa Ministerial Conference report (Document 2) identifies the following four "important themes" to facilitate global electronic commerce:

1. Building trust for users and consumers
2. Establishing ground rules for the digital marketplace
3. Enhancing the information infrastructure for electronic commerce
4. Maximizing the benefits

These themes can be used as broad categories of issues important for electronic commerce. Although not perfectly orthogonal, the categories help deal with the large number of issues. Table 1 presents a list of important electronic commerce issues within each of the above four categories. In the next four sections of this article, we evaluate the state of resolution of these issues, critical for the conception of global electronic commerce.

III. TRUST FOR USERS AND CONSUMERS

PRIVACY PROTECTION

The New York Times on the Web [Clausing June 1, 1999] reported that European and United States trade negotiators failed to find an agreement over data privacy issues, "sending the issue of continued electronic commerce between the regions into a new realm of uncertainty." The essence of the disagreement was the difference between the U.S. government and European Union (EU) on how privacy protection can be achieved and regulated. The U.S. supports the self-regulation of businesses while the EU accepted the privacy directive last year and regulated this issue. *Newsbytes* reported that [MacMillan 1999]:

Table 1. Fundamental Electronic Commerce Issues Discussed in Sections III through VI

Section III. Building trust for users and consumers Privacy protection Secure environment for commerce Consumer protection Authentication and confidentiality Access blocking
Section IV. Establishing ground rules for the digital marketplace Legal framework Acceptance of electronic transactions Taxation Tariffs Intellectual property protection Commercial policy Payment systems
Section V. Enhancing information infrastructure Development of information infrastructure Internet governance Interconnectivity and technological convergence Internet technical standards Ensuring adequate bandwidth and access Furthering competition
Section 6 Maximizing the benefits Understanding the digital economy Measuring electronic commerce Global participation, seamless global marketplace Small and medium size businesses and the Internet

"So far, the EU has been dissatisfied with what they see as a lax, self-regulatory approach in the U.S. toward online data privacy. To counter that claim, the U.S. government is working on a proposal to have companies inform users of their data-collection practices, allow them to opt out of releasing their personal information, and state the identity of those who will share access with. More importantly, it will address the issue of how industry's self-regulation on privacy protection will be monitored. Temporarily, the U.S. has been unwilling to sign onto the EU's strict data protection guidelines, which the Commerce Department claims are too onerous to enforce stateside."

European regulation created a great hurdle in communicating information between EU member countries and those that do not have strict regulations, including the U.S. The U.S. Government worried about how effective the law will be in the control of such widely available and easily accessible information over the Internet [The Economist, Dec.18, 1999].

This issue, a serious crack in global coordination of electronic commerce, was mediated by discussion between the U.S. and the European Commission. The parties were moving closer to finding a way for U.S. firms to trade data gathered about Europeans without violating EU data-protection laws.[1] The tough EU privacy directive that went into effect in 1999 was likely influenced by the findings of the March 1998 survey by the U.S. Federal Trade Commission (FTC), which established that only 14 percent of U.S. commercial Web sites provide any notice of their information collection practices [FTC 1998]. More recent research, conducted in March 1999, found that 87 percent of surveyed commercial Web sites included at least one notice reflecting fair information practices [Culnan 1999]. Although Culnan advises that the two studies are not easily comparable, it appears that corporate America is improving its handling of privacy protection.

Can we afford to wait for self-regulation, though, before some widely publicized cases of mishandled information practices destroy public confidence in electronic commerce? The Center for Media Education thinks that we cannot wait. It surveyed 80 popular children's sites and recorded that only a quarter of them try to ask for parental permission before collecting information about minors [McCullagh July 1999].[2]

Moreover, dissatisfaction with the slow progress at the federal level is forcing some states in the U.S. to move ahead. Critics charge that the U.S. Commerce Department failed to sink its teeth into consumer privacy [Oakes June 1999]. Consequently, the New York State Assembly passed legislation to implement privacy safeguards for consumer information. This initiative pleased

---

[1] EU and U.S. negotiators agreed on March 14, 2000 to recommend a deal on data protection in a breakthrough aimed at ending a two-year dispute [Smith 2000].

[2] In October 20, 1999, the FTC passed rules regarding parental consent. This regulation is discussed further in section Access Blocking below.

privacy experts and advocates. Marc Rotenberg, executive director of the Electronic Privacy Information Center, said: "It's not surprising that states are moving when Washington policy legislators are largely sitting on their hands." He and the American Civil Liberties Union (ACLU) agree that the federal government should set broad limitations on what user information companies may collect. Still others, such as Eugene Volokh, UCLA law professor specializing in constitutional law and a speaker at the Competitive Enterprise Institute conference, believe that restrictions of this kind would violate the First Amendment [McCullagh Dec. 1999].

The Canadian government voted in favor of the Personal Information Protection and Electronic Documents Act in the House of Commons by a margin of 200-49 [Friedman Oct. 1999]. The legislation requires Canadian companies and institutions to obtain informed consent before they collect or disclose personal information. This act still has to make its way through the Senate. Privacy advocates fear the law's opponents in the insurance and health care industries will try to influence the decision.[3] Incidentally, only two days later U.S. President Clinton announced new regulations to protect the confidentiality of electronic medical records. He also called on Congress to pass legislation so that all medical records would be protected [Keto 1999].

Another example of privacy protection concerns was the proposal by the Internet Engineering Task Force (IETF). In the process of creating a new Internet address system known as IPv6 (further discussed in the section Development of Information Infrastructure), this international standards body proposed the inclusion of the unique serial number for each computer as part of its expanded new Internet protocol address [New York Times Oct. 1999]. This number would be included within each packet sent from a computer, which could potentially strip away a measure of anonymity and security enjoyed by home computer users. Some privacy experts were appalled that IETF engineers would consider

[3] The Personal Information Protection and Electronic Documents Act received Royal Assent on April 13, 2000. The Act introduces measures to protect personal information in the private sector, creates an electronic alternative for doing business with the Canadian federal government, and clarifies how the courts assess the reliability of electronic records used as evidence.

the idea. They warned that commercial Internet sites could begin to correlate these numbers against a consumer's name, address and other personal details. It took four months, a grim debate, and thousands of mailing list messages, but the group that sets Internet standards decided not to support wiretapping. Under the organization's procedures, the draft statement is not yet final and members can offer changes. But a member of the drafting group said he anticipates no serious alterations [McCullagh, Feb. 3, 2000].

In November 1999, the public learned that RealNetworks' popular RealJukebox software for playing CDs on computers surreptitiously monitored the listening habits and certain other activities of people who use it and continually reported this information, along with the user's identity, to RealNetworks when they were connected to the Internet [Robinson 1999]. Company officials acknowledged this mistake and offered a software patch that prevents the software from transferring personal information back to the company. The company also agreed to cease data collection activities and undergo a comprehensive review of its policies [Luh 1999]. Jason Catlett, founder and president of the privacy watchdog organization Junkbusters, said: "Either they have been dazzlingly careless with their treatment of personally identifiable information or they are completely disingenuous. Which is worse? If they are not disclosing what they are doing, that is unconscionable" [Robinson 1999]. Will news like this shatter the public trust in Internet as an environment where they can remain anonymous?

In a similar scare, consumer and privacy advocates asked regulators at the FTC to force software makers to seal an email feature that they say enables companies to track the Web sites people visit [Srinivasan 1999]. The groups fear that companies could exploit the technology to match up people's email addresses and possibly other personal information with their Internet surfing habits.

Consumer privacy advocates and consumers themselves are concerned about privacy problems because of an outbreak of security issues. One such example is the case of Joel D. Newby vs. Amazon.com’s Alexa Internet. Newby

claims the software is sending his personal information to Amazon without his consent [Sandoval and Wolverton 2000]. Another example concerns Northwest Airlines users discovering a security breach in Northwest's web site exposing user's credit card and personal information. It occurred because a programmer forgot to enable the encryption software after he made changes. [*ibid.*] A more serious case is presented by ReverseAuction.com. The company made improper misrepresentations to eBay users. Besides gaining unauthorized access to eBay's web site and obtaining user identification numbers, it send a "spam" mailing to several hundred thousand users. The company finally settled with the FTC not to make misrepresentations in the future and destroyed any personal information it gathered from eBay customers [*ibid.*].

Privacy advocates are also concerned with corporate data collection, or the transfer of data to unknown third parties. Yahoo was sued for $4 billion by Universal Image for breach of contract in disclosing user information. The suit claims that since Broadcast.com was purchased by Yahoo, it stopped sending information about its users as promised by Yahoo's privacy policy. Dallas County Court Judge Leonard Hoffman issued a temporary restraining order that demands Yahoo cease implementing its privacy policy. He believes the policy is "fraudulent and deceptive to users because, among other things, it falsely indicates that users who registered at any time may block Universal's access to information" [Murphy Dec. 27,1999].

Another controversial issue that is surfacing is Internet privacy rights in the workplace. The courts believed that employers should be granted an exception to privacy rights to screen employees' Internet usage since the company furnished the technology to them. However, many people think that even if laws are passed to protect worker Internet privacy, companies can still bypass them by requiring employees to waive those rights as a condition of employment [Tsuruoka 1999].

On the positive side, Microsoft followed the lead of IBM in announcing that starting in 2000 it will advertise only on Web sites that post privacy policies [Sprenger and Glave 1999]. Some observers consider these announcements important as they come from the first and second largest Web advertisers.

Others see this announcement as only a small step in the right direction and find posted privacy policies very weak and falling short of the "Fair Use Policy." Privacy advocates say a better answer is legislation setting a basic standard for privacy that would apply across the Web [Kong 1999]. They observe that the "Privacy Policy" buttons at the bottom of Web pages seem to promise protection but in fact offer nothing of the kind, and that a "policy disclosure" should not be confused with actually safeguarding personal data. The privacy policies often tell visitors how much privacy they are losing.

On the flip side of the issue, the Clinton Administration developed a plan for an extensive computer monitoring system, overseen by the Federal Bureau of Investigation, to protect the nation's crucial data networks from intruders [Markoff July 28, 1999]. The draft calls for a sophisticated software system to monitor activities on various networks, including those used in banking, telecommunications, and transportation. The plan raised concerns from civil liberties groups, to say the least. Their concern is that the government will be able to intercept everybody's communication on the Internet, which may discourage its use for both business and private communication [McCullagh Feb. 1, 2000]. The system, to be implemented by the year 2003, is expected to become a major source of disagreement.

The Federal Communications Commission (FCC) drafted the privacy-invading rules permitting police surveillance. The Justice Department also supports the position that the Internet should be open for police eavesdropping, since such activities are related to continuous criminal investigation [McCullagh Jan. 2000]. However, civil liberties organizations disagree that law enforcement agencies should be allowed to order the telephone companies to intercept Internet transmissions without a warrant.

The FTC formed a group to discuss privacy practices and to issue a committee report on industry security practices and standards for granting users' access to their own information. The group, called the Advisory Committee on Online Access and Security, provides advice and recommendations on whether it is appropriate for companies to charge users a fee to view the personal data that

was gathered about them. The Committee should also provide directions for commercial Web sites to develop systems that will give people access to their personal information without companies incurring restrictive costs or compromising the security of that information [Clausing Dec. 1999].

Senator Robert Torricelli (D-N.J.) introduced the Internet Privacy Act. This act would mandate that sites obtain the approval of users before any personal information can be disclosed to others and would control the use of cookies [Curran 2000].

A newly established bipartisan Congressional Privacy Caucus took the first step in March 2000 toward its goal of establishing strict, national privacy protection standards. The Privacy Caucus held a public hearing featuring state attorneys general. The Caucus was founded on four basic principles. The first is that individuals must be informed when private companies or government agencies plan to collect and use personally identifiable information; they should also be informed of the intended recipient of such information. Second, the Caucus believes that individuals must be able to access and correct the information. Third, information should not be transferred without prior affirmative consent of the individuals. Finally, the states should be free to enact even greater protection than federal standards. Senator Richard Shelby, a member of the Caucus, said: "We believe the Congressional Privacy Caucus will help us bring these issues to the attention of members of Congress by holding Congressional briefings and by examining and recommending legislative proposals." [Brostoff 2000]

SECURE ENVIRONMENT FOR COMMERCE

Security of electronic commerce relates to protecting private data both during the transfer over the networks and while it is stored in databases connected to the networks. An early and highly influential document, "*A Framework For Global Electronic Commerce*" [Clinton and Gore 1997], states that: "If Internet users do not have confidence that their communications and data are safe from unauthorized access or modification, they will be unlikely to use the

Internet on a routine basis for commerce." The document defines the following four related requirements:

1. secure and reliable telecommunications networks,
2. effective means for protecting the information systems attached to those networks,
3. effective means for authenticating and ensuring confidentiality of electronic information to protect data from unauthorized use, and
4. well-trained Global Information Infrastructure (GII) users who understand how to protect their systems and data.

The document further suggests that accomplishing the goals of security and reliability requires an effective and consistent use of a range of technologies such as encryption, authentication, password controls, and firewalls, all supported globally by trustworthy key and security management infrastructures.

This goal may, at least in the near future, be impossible to achieve. Issues regarding the public key infrastructure (PKI) discussed later in this section illustrate problems with requirement 3 on the above list. Related to this issue is the unresolved conflict between several governments and business about restrictions in the global use of encryption technology. Requirement 4 is highly elusive, judging from the general lack of security protection. Even when the utmost attention is being paid to security, requirement 2 cannot be met. The following reports confirm this concern [National Infrastructure Protection Center 1999].

- A 1996 survey by the American Bar Association of 1,000 companies showed that 48% had experienced computer fraud in the last five years.
- A Study of 300 Australian companies by Deloitte Touche Tohmatsu found that over 37% of the companies experienced some form of security compromise in 1997, with the highest percentage of intrusions (57%) occurring in the banking and finance industry.

- A 1998 study by the Computer Security Institute shows that 64% of companies polled reported information system security breaches -- an increase of 16% over the previous year.
- The Federal Bureau of Investigation (FBI) also saw an increase in the number of pending investigations that involve the exploitation of technology that represents a threat to the public and private sectors. Both investigations and successful prosecutions increased significantly. Pending cases increased 115% from the beginning of 1997, from 260 to 559. In 1997, their data showed an increase of 110% in information and indictments (from 10 to 21), 950% in arrests (from 4 to 42), and 88% increase in convictions (from 16 to 30).
- In a 1999 research study published by British Telecom (BT), small and medium enterprises maintain even fewer security measures. According to the study, 26% of the respondents implemented the secure socket layer (SSL), while only 12% used public key infrastructure. Only 2% used firewall protection or cyber-liability insurance, digital certificates, and digital signatures. It seems that these companies know the security issues but do not understand (or cannot afford) the solutions available on the market [Dennis 1999].

It comes as no surprise that the U.S. government recognized the information infrastructure as one of the nation's critical infrastructures. The Clinton Administration issued Presidential Decision Directive 63 (PDD 63) [White House 1998], which sets the following goals:

- develop a reliable, interconnected, and secure information system infrastructure for the Federal Government by 2003
- significantly increase the security of Government systems by the year 2000 by
  - implementing a National Warning Center,
  - increasing protection capabilities, and
  - reducing threat exposure at the Agency level.

PDD 63 reflects the current thinking that places the "cyber-dimension" of emerging national security threats in three general categories.

1. Unstructured threat composed of insiders, recreational, and institutional hackers.
2. Structured (or organized) threats including organized crime, industrial espionage, and terrorists.
3. High-end or national security threats posed by the intelligence agencies of other states, or information warriors, operating under the direction of foreign governments.

PDD 63 also implies that it will take some time to reach the point when the information infrastructure, essential to the minimum operations of the economy and government, becomes reliable and secure.

Nonetheless, President Clinton asked the Congress for $91 million of a $2 billion proposal to find new technologies to deter cyber-terrorists. The proposal is set to maintain the security of the country's digitized infrastructure. Because the government is a heavy user of technology, it is extremely vulnerable to hackers and thieves. Cyber-terrorism is considered a top priority when it comes to threats facing America in the new century. The administration is in the process of creating a government-wide security network to watch suspicious and dangerous activities of hackers [Anonymous, Jan. 7, 2000].

Until such a network is established, media reports, such as the examples given in the sidebar that follows, can be expected to continue.[4]

[4] A computer virus carried by e-mail messages bearing the title "I Love You" quickly spread around the world Thursday, May 4, 2000, wiping out important computer files and forcing large corporations to shut down their e-mail systems [Pringle *et al.* 2000].

SIDEBAR: SECURITY INCIDENTS

- The Federal Bureau of Investigation was forced to take down its Internet site after hackers began an attack against it. It remained inaccessible for several days, along with the site for its National Infrastructure Protection Center, which helps investigate computer crimes [Reuters 2000].
- Takahashi [1999] reported that the "Worm.Explore.Zip" virus struck tens of thousands of computers in more than a dozen countries. Officials at the antivirus firm Network Associates Inc. estimated that 70% of its top 500 customers, representing thousands of computers, had been hit by the virus with varying amounts of damage. The impact was so severe that the Computer Emergency Response Team at Carnegie Mellon University issued a virus warning, the third time it has had to do so since March. The Federal Bureau of Investigation began a criminal investigation into the matter.
- While trying to secure his own servers, Greg Gonzales discovered an easy way to exploit a known hole in Microsoft's Internet Information Server (IIS) software in June 1999 [Sprenger July 20, 1999b]. The hole is so easy to exploit that people with even little Visual Basic programming experience would have no problem cracking an affected site. Gonzales said that at least 50 percent of the IIS sites he looked at are affected. Microsoft itself reported that some of the largest sites, such as Nasdaq and Compaq, are vulnerable. Similarly, Markoff and Robinson [1999] reported in late July that Microsoft and Compaq Computers acknowledged several significant software security flaws that could enable intruders to gain access to the computers of millions of customers and to damage their data via e-mail or through commands sent from a malicious Web site.
- There seems to be no end to such stories. Associated Press reported [Associated Press Aug. 6, 1999] that an embarrassing electronic assault against the AntiOnline site - a prominent Internet site devoted to computer security - occurred days after other hackers altered the Web site for Symantec Corp., whose software is used by millions of consumers to protect against viruses and electronic snoops. Another event, in which a group of scientists broke an international security code used to protect millions of daily Internet transactions, was also widely reported [Chicago Tribune Aug. 28, 1999]. They exposed a potentially serious security failure in electronic commerce. Using a Cray 900-16 supercomputer, 300 personal computers, and specially designed software, they broke the RSA-155 code, which is the backbone of encryption codes designed to protect e-mail messages and credit-card transactions. A distributed network of computers again cracked a 56-bit encryption key only weeks after a French company challenged hackers to break the algorithm. [Oaks 2000]
- A similar incident happened when a group of computer professionals created a program that can reveal secret keys kept inside the web servers that process credit card transactions. nCipher is a small British specialty hardware firm that claims to have the best encryption software. To discredit that claim, these professionals developed a program to obtain the secret keys and accessed credit card numbers and other private information. This attack is effective against the majority of operating systems that run Web servers like Microsoft Windows NT, Windows 2000, and Sun's Solaris. [Wayner 2000]
- RealNames Corp. reported that a hacker had succeeded in subverting its firewall, gained access to customer accounts, and may have stolen credit card data. [Andrews 2000]

Some computer scientists believe that in the rise of the Internet and the World Wide Web, society struck a Faustian bargain; gaining the potential of robotic software agents, which can flit from computer to computer to do their masters' bidding almost intelligently, but accepting as well the darker prospect of software infections that can spread the destruction of cybernetic plagues [Markoff June 14, 1999]. Online auctioneer eBay Inc. waived millions in listing fees after its worst service outage ever, but feels that the company may be hard-pressed to avoid some erosion of customer loyalty [Anders 1999]. Bidding on eBay was halted completely for almost 22 hours and left nearly 2.3 million auctions stranded in the middle of bids.

In December 1999, the online music store CD Universe learned that 300,000 credit cards were stolen from its Internet files. The extortionist requested $100,000 to destroy the files. The FBI is hunting for the blackmailer who calls himself Maxim and is believed to be located in Eastern Europe. He is believed to have hacked into other electronic commerce Web sites since 1997 [Markoff 2000].

These examples and those in the sidebar are just a small sample showing that the Internet can hardly be considered a secure and reliable environment for electronic commerce at this point of time. Adi Shamir, an encryption expert with Israel's Weizmann Institute of Science argues that "Secure systems do not exist; they will never exist. The key is, don't try to shoot for perfect security or you'll fail." [Associated Press, Jan. 17, 2000]

The February 2000 rash of denial of service attacks against major Web sites such as Yahoo! Inc. and E*Trade Group Inc. show that Internet architecture needs to be redesigned to prevent malicious tampering [Hamilton 2000]. Experts claim technical solutions to ward off such attacks would not be that hard to find but they also say that making the Internet more secure as a whole is much more difficult because there is no one governing body to enforce uniform standards. The IETF functions like a standards setting board but lacks authority to enforce what are, basically, only recommendations. The IETF claims that the IPv6 protocol would make it difficult for hackers to conduct denial of service attacks.

However, moving to IPv6 would be expensive for the industry and there is little support for doing so. The Internet will most likely remain an insecure place well into the future.

CONSUMER PROTECTION

FTC Chairman Robert Pitofsky remarked at the Workshop on Consumer Protection in The Global Electronic Market: 'The informal nature of the medium, the lack of personal contact between buyer and seller, and the geographic dispersion of sellers create new and unprecedented opportunities for consumer abuse through fraud and deception - opportunities so great that, if not effectively addressed, they can undermine the full development of global competition itself. How do we monitor the Internet, and deal with cross-border fraud? This is a daily challenge for this agency; we have brought over 80 cases involving Internet fraud to date" [Pitofsky 1999].

Consumer protection is most effective when businesses, government, and consumer groups all play a role [Harrington 1998]. Meaningful consumer protection takes:

(1) coordinated law enforcement against fraud and deception;

(2) private initiatives and public/private partnerships; and

(3) consumer education through the combined efforts of government, business, and consumer groups [FTC 1996].

Harrington also suggested that there is nothing new about most types of Internet fraud the FTC has seen so far. What is new -- and striking -- is the size of the potential market and the relative ease, low cost, and speed with which a scam can be perpetrated.

Matters are not yet resolved, as shown by horror stories, general disagreement on how to prevent fraud effectively and build public trust in electronic commerce, and a general failure to commit resources to combat fraud and deception. For example, Kawika Daguio, a consultant to the American Bankers Association found nine institutions that presented themselves on the Internet as banks but weren't banks. Most of them were shut down. One of the

institutions closed down was in the Caribbean, operated by several people who, according to both U.S. and the un-named Caribbean nation, were in the Russian Mafia. They encouraged depositors to make deposits into anonymous accounts and basically stole the money and ran away [Daguio 1999].

Harrington's report includes several examples of cases investigated by the FTC, including pyramid schemes, "spam" (unsolicited commercial e-mail), fraudulent online auctions, and schemes unique to the Internet. Fortuna Alliance allegedly promised consumers that for a payment of $250 they would receive profits of over $5,000 per month. In another case the FTC estimates that over 30,000 consumers who joined Credit Development International may have collectively lost $3 to $4 million in an alleged scam. Fraudulent business opportunity schemes are often cultivated by spam as a way to solicit millions of consumers for little cost. The FTC brought suit against Craig Lee Hare who advertised computers on several auction sites. Hare took as much as $1,450 each from "successful bidders" across the country but failed to send any computers or refunds.

The whole theme of consumer trust was challenged in the New York Times [Caruso 1999]. Caruso suggested that dot-com companies' "increasingly questionable business practices are becoming public, casting long overdue doubt on the credibility of much of the commercial Internet." Web publishers did not adopt standards and practices that are assumed in traditional media. Neither tradition nor laws protect consumers. Amazon.com accepted money from publishers for its supposedly independent book reviews. Former U.S. Surgeon General Dr. C. Everett Koop was publicly embarrassed for taking commissions on products and services sold through his DrKoop.com site without disclosing such arrangements. Online newsletter *eMarketer* reported: "For instance, here is what comes up on a search for 'digital camera' on Lycos: A (paid) banner for digital cameras; a (paid) link to an online camera store; a (paid) link to an online bookstore offering books on cameras; the (unpaid) search result links" [eMarketer March 1999]. Caruso speculates that: "the use of the Net as a

commercial medium could drop precipitously as consumers realize they are being gamed."

Consumer trust is not established yet and it may never be. Some, perhaps most people will become selective and seek information and buy goods from sources they trust, such as, for example, britanica.com and bn.com, in which case only a few such trusted and established winners will take all. In other words, people will avoid sites they do not recognize, thereby establishing insurmountable barriers to entry for new small startups.

An illustration of general disagreements on means of protection and building trust is the position of the Electronic Messaging Association (EMA). EMA is a trade organization that represents the interests of almost 500 corporate users and providers of electronic messaging and commerce. EMA agrees with the FTC that we stand at a critical juncture in the development of electronic commerce, because fraud and deception may deter consumers from acquiring a greater confidence in the Internet as a place to transact business. At the same time, EMA recognizes that government regulations intended to protect against fraud can unreasonably and unnecessarily interfere with legitimate businesses if the government attempts to micro-manage online services or are vague in application of the law [Stackpole *et al.* 1998]. However, EMA also strongly opposes any finding that telemarketing rules encompass online communications. They also oppose any effort to extend telemarketing rules to electronic commerce via the "backdoor" of an expansive definition of "direct mail."

The FTC informally surveyed 200 Web sites in 18 countries to find out what types of disclosures and information online merchants give to consumers. Results suggest that most companies provided helpful general business information but do not provide important contract-related information such as refund policies, cancellation terms and warranty information [FTC 1999]. Only nine percent of the sites provided cancellation terms, 26 percent provided refund policies, and 38 percent of the sites disclosed the applicable currency. The FTC is still examining how to ensure effective consumer protection to participants in

international electronic commerce. It is probing what types of protections consumers need online, and how such protections can be secured.

Many electronic commerce retailers are not aware that they are subjected to the Mail Order Rule. This Rule includes regulations about shipping, informing customers in cases of unexpected shipping delays, and refunding customers' money. Violators may not only be sanctioned by the FTC but are exposed to class-action lawsuits [Caswell 1999]. The FTC suggests that online retailers review their legal obligations.

Harrington's report [Harrington, 1998] hints at the lack of resources committed to detect fraud. She reported that "The growing problem of 'spam' already threatens to outstrip our resources" and that "Fighting fraud over the Internet is clearly a formidable task for the FTC's limited available resources."

Spam may be a problem for the FCC if a bill introduced with bipartisan support in the U.S. House of Representatives becomes law. The legislation would direct the FCC to create a national list of people who don't want to receive spam and would penalize those who spam people on the list [Murphy Oct. 19, 1999]. The Unsolicited Electronic Mail Act of 1999 would allow users to post "No Trespassing" signs on their computers or choose to receive their e-mail through virtual gated communities where spamming is not allowed. The bill would also let Internet Service Providers (ISPs) decline to send spam and charge spammers for the costs. The bill would further provide for punishing spammers who lack valid return address or don't honor requests to be removed from the distribution list.[5] The bill is popular among antispam groups such as the Coalition Against Unsolicited Commercial Email. Some observers are concerned, however, that this duty may overwhelm the agency.[6]

---

[5] The House Commerce Committee passed the bill by voice vote. It now moves to the House floor [Murphy June 2000].

[6] The first state to enact legislation curbing spam has become the first state to have its law invalidated, when a Washington state judge ruled that the Unsolicited Electronic Mail Act violates the Interstate Commerce Clause of the U.S. Constitution [Computer & Online Industry Litigation Reporter Apr. 2000].

Robert Vastine, [Vastine 1999] president of the Coalition of Service Industries, in testifying before the Committee on Commerce at the U.S. House of Representatives proposed that the U.S. government support the position that a foreign consumer of an electronically delivered service supplied from the U.S. should, in general, be considered to have left his country virtually and traveled to the U.S. to buy the service. He suggested that were the law of the consumer's country to apply, the growth of transborder electronic commerce would be slowed to a funereal pace. Vastine expressed concern about the draft recommendations of the OECD that "… the law applicable to the electronic contract … should be that of the country in which the consumer resides when the contract is formed." He further proposed that advertising a service on an U.S. Web site should not be considered a direct advertisement in a foreign country and thus subjected to the laws of that country.

Vastine also recognized that governments cannot forego consumer protection for the sake of electronic commerce and proposed that this important issue be resolved by:

- Reaching bilateral or multilateral agreements mutually recognizing the validity of countries' consumer protection laws.
- Creating common standards of consumer protection for electronic transactions.
- Providing direct assistance to consumers in obtaining redress in foreign jurisdictions.
- Educating consumers about differences in consumer protection among countries.
- Encouraging voluntary certification programs for subscribing companies agreeing on consistent practices.

Just reading the above recommendations should lead to the conclusion that accomplishing these goals is extremely difficult. Educating the average person on the consumer protection policies of 150 nations is, frankly, unrealistic.

On the positive side, the Better Business Bureau issued a proposed Code of Online Business Practices for which it sought public comments [BBB 1999].

The new code, based on the experience of BBB*OnLine* and a review of 5,000 commercial sites, supports five basic principles:

1. Online businesses should clearly disclose accurate information about the business, goods and services, and online transactions.
2. They should not engage in deceptive or misleading trade practices.
3. They should adopt respectful information practices, post and adhere to a privacy policy, provide security and respect customers' preferences regarding unsolicited email.
4. They should make online shopping experience pleasant and seek to resolve disputes in a timely and responsive manner.
5. They should take special care to protect children under the age of 13.

This code is an effort to give consumers confidence and follows the creation of the BBB*OnLine* Reliability Seal and Privacy Seal Programs.

These goals are wonderful, but the news regarding consumer protection is not good. International online law enforcers warn that they are seriously behind in tackling Internet crime and believe cybercrime might prove a major threat to countries as well as businesses. No figures exist for Internet crime, but Brian Jenkins, formerly at the Rand Corporation and a consultant to the International Chamber of Commerce, believes online crime is growing faster than the Internet itself [Reuters, Dec. 7, 1999].

In some cases, inadequate business practices open the door wide to fraud. For example, an online bank, X.com, allowed its new customers to specify the account number from which funds would be transferred without checking whether the person creating the account was allowed to move the original funds. This policy enabled anyone who knew another person's account number and check routing numbers to transfer money from that account to the new X.com account and then withdraw it [Greenberg and Caswell 2000].

AUTHENTICATION AND CONFIDENTIALITY

Authentication technology is still imperfect. Only a few years ago public key encryption appeared to be the final solution to this problem. It called for the

establishment of a Public Key Infrastructure (PKI), a hierarchical structure of Certification Authorities (CA). The CAs keep public keys of individuals and organizations whom they authenticate. They guarantee that the owners of public keys are who they say they are. Each CA is in turn authenticated by the CA at a level up in the hierarchy with the exception of the CA at the top of the hierarchy, which must be a globally accepted trusted authority. It now appears that biometrics technology, such as voice recognition, has the potential to provide more robust authentication. It is not clear, however, whether the use of biometrics will also require legally established PKI. This state of affairs is another example supporting the concern that immediate regulation may be premature. Another worry among national regulators is that they may implement rules conflicting with international initiatives and thus isolate their country from global electronic commerce. Indeed, "One of the greatest risks posed by the current flurry of legislative interest in electronic signatures is that national legislation will actually *inhibit* the use of electronic signatures in international commerce." [Baker and Yeo 1999]

Progress in regulating electronic signatures is reported both in the U.S. and the UK. The House of Representatives voted overwhelmingly in November 1999 to approve the so-called E-SIGN bill, giving electronic contracts signed with digital signatures the legal validity of ink-signed paper contracts [Oxley 1999]. The Senate also passed digital signatures legislation, paving the way for a conference with the House to iron out any differences [Murphy Nov. 1999].[7] In the UK, the Electronic Communications Bill was published in November 1999 and is expected to pass easily when it is debated in Parliament early in the year 2000[8] [See 1999]. This bill, which also makes electronic signatures as legally

[7] In June 2000, Congress has passed this bill, overriding diverse state approaches. It now goes to President Clinton, who said he will sign it. If he does, electronically signed documents will be legal beginning Oct. 1. The use of electronic documents for record keeping will be possible beginning March 1 [Rosen 2000].

[8] As of June 15, 2000, this bill had received Royal Assent and the Act will be found on Her Majesty's Stationery Office site shortly [UK Parliament 2000].

binding as handwritten ones, is touted as the British government's commitment to helping turn the UK into one of the world's strongest Internet economies.

The essential component of public key infrastructure is encryption. The struggle between U.S. government security and protection agencies on one side, and the software industry and privacy protection groups on the other side went on for years. Agencies responsible for national security, for example, tried to establish policies that would enable them to decode the encrypted messages. This power was opposed by groups wanting to compete on an equal basis with foreign software developers offering stronger encryption technology and by privacy protection advocates who are afraid of extensive government control. Attorney General Janet Reno and FBI Director Louis Freeh, for example, told Congress that easing export controls on powerful data and voice-scrambling technology would hamper efforts to track down terrorists and other criminals [Associated Press July 13, 1999].

On September 16, 1999, everything changed. The new policy adopted by the Clinton administration permits the export, without a license, of any encryption software following a technical review. Exporting to the countries accused by the State Department of sponsoring terrorism remains prohibited. Beside this restriction, there is no limit on key lengths or key recovery schemes [Fry and Doscher 1999].

Levitt predicts that "Ultimately, PKI will become a commodity item. Certificate services will be widely available and applications will use PKI right out of the box." [Levitt 1999] He warns, though, that PKI is still a challenging application. Gartner Group analysts predict that by the year 2003 up to 80% of large companies will have tested one or more PKI solutions. Three years seems like a long time for testing, but PKI is a fairly complex software architecture and requires radical restructuring of security policies.

One of the promising developments in establishing PKI, however, at least for business-to-business electronic commerce, is the joint venture formed between VeriSign, Inc., a leading provider of Internet trust services, and Dun & Bradstreet. The two companies offer a number of services including digital

certificates with real-time business verification and certificate validation. This partnership is encouraging because Dun & Bradstreet maintains a global database of 57 million companies and can leverage VeriSign's expertise in digital certificate solutions [Dun & Bradstreet 1999].

ACCESS BLOCKING

The Presidential Directive on Electronic Commerce, issued July 1, 1997, contained the following order: "I direct the Secretary of Commerce to encourage the development and adoption within the next 12 months by industry of easy to use and effective rating systems and filtering technologies that empower parents, teachers, and other Internet users to block content that is inappropriate for children." [Clinton 1997] Two and a half years later, the matter is far from being settled.

Admittedly, some progress has been made. Software that blocks access to pre-selected sites and filters content is widely available and some family-friendly content is accessible on the Web. The third goal--to persuade foreign governments of the benefits of an approach, which empowers users, rather than governments, to control content--has not been achieved.

In the U.S., the concept of blocking or filtering access to "inappropriate" Web sites is understandably supported by concerned parents and others, and vigorously objected to by groups protecting free speech. For example, the American Library Association opposed the use of filters in libraries because it recognizes that it is the domain of parents, not librarians, the government, or faceless software companies, to oversee the use of the library by their children [IFEA 1998]. They believe that no filter can block all objectionable material while such software restricts access to valuable and constitutionally protected material. This position contrasts with that of Elizabeth Dole, then a candidate for the Republican presidential nomination, who said during her visit to a library in Bellevue, Washington: "Federal tax dollars should never be used to poison our children or provide free pornography for adults." [McCullagh June 1999]

Congress first attempted to regulate this area with the Communications Decency Act of 1996. The Supreme Court, however, held in June 1997 that it violates the First Amendment's guarantee of freedom of speech, and thus rejected censorship of the Internet.

On February 1, 1999, Judge Lowell Reed, an U.S. District Judge in Philadelphia, granted a preliminary injunction against the Child Online Protection Act (COPA). In granting the injunction, Judge Reed expressed his regret that the legitimate goal to protect our children from inappropriate material online would have, in this instance, a "chilling effect" upon constitutionally protected speech [Morrissey 1999]. "While the public certainly has an interest in protecting its minors, the public interest is not served by the enforcement of an unconstitutional law," the court's decision said. "Indeed, to the extent that other members of the public who are not parties to this lawsuit may be affected by this statute, the interest of the public is served by preservation of the status quo until such time that this Court may ultimately rule on the merits of plaintiffs' claims at trial" [SPLC 1999]. The preliminary injunction memorandum further comments that "perhaps we do the minors of this country harm if First Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection." COPA, passed as part of a spending measure in fall 1999, states that it is a criminal offense to publish material that is harmful to minors. Allowing unrestricting access to such material by minors is punishable by a $50,000 fine and civil fines with six months in jail [McCullagh Nov. 1999].

The Senate Commerce Committee approved the Children's Internet Protection Act on June 23, 1999. The legislation would mandate that schools and libraries receiving "E-Rate" universal service funds purchase and use Internet filtering software to regulate access by minors. The House of Representatives added a similar provision to the juvenile justice bill on June 17, 1999. The Internet Free Expression Alliance sent a joint letter to the Senate committee urging rejection of mandatory filtering [IFEA 1999].

In October 20, 1999, the FTC passed rules regarding parental consent [FTC 2000]. The ruling asks that parents must be given notice and consent for

release of child's information and its further usage especially for those organizations or sites that collect data from kids for internal use or with third parties. According to a March 1998 survey of 212 commercial children Web sites, 89% collect children's personal information but only 24% post privacy policies and 1% require parental consent. These organizations and sites had to comply by April 21, 2000 in order to avoid fines and penalties [Murphy Oct. 20, 1999].

The real battle will be fought over public places such as libraries and schools. Do these institutions have a right to install filtering software? Should they be required to do so? Both sides will continue to fight each other on these issues, and the courts will most likely have the final say [Rosoff 1999].

In June 1999, Australian political leaders passed one of the world's most far-reaching online content censorship programs. The rules, which took effect on Jan. 1, 2000, enable Australian government regulators to order domestic Internet service providers to remove indecent or offensive Web sites housed on their servers, and also require that they block access to certain domestic or overseas-based content [Taqqart 1999]. As one can expect, the opponents of online content restrictions will now shift to cyberspace itself. They believe the Internet simply will prove too large, too decentralized, and too fast-moving for regulators anywhere to successfully block access to any content for long.

In Ontario, Canada, the provincial government limits employee access to the Internet by installing a filtering device that prevents them from connecting to certain sites [Ditchburn 1999].

IV. ESTABLISHING GROUND RULES FOR THE DIGITAL MARKETPLACE

LEGAL FRAMEWORK

Perritt implies that nothing in our experience suggests that market forces will guarantee that the Internet will evolve in support of the best interests of society [Perritt 1999]. We should therefore not ask whether the law should stay

away from electronic commerce but rather how the law should engage it. Perritt suggested three alternatives.

1. There is no need to do anything new; the existing institutions will regulate the conduct on the Internet as they regulated the conduct before the Internet. This approach may not work because the Internet presents difficult jurisdictional problems. It is inherently global while all the existing legal institutions (including international ones) are premised on geographic boundaries. The solution in this case would be to target the intermediaries, the service providers. Although this could be done, targeting intermediaries would put in place private censorship, which will defeat the universality of the Internet.
2. The second option is some form of private self-regulation. Some remarkably promising alternatives could make self-regulation a reality in the context of privacy regulation. It is difficult to imagine, however, how this self-regulation model can be extended to all of the issues that one wants to deal with around the world.
3. Establishment of an international administrative agency to exercise jurisdiction over some kind of conduct over the Internet. Perritt believes that this alternative is not completely far fetched since the international community is able to act remarkably quickly. This solution, however, conflicts with three constitutional provisions that the U.S. Congress cannot delegate legislative power to make rules to anyone outside the Congress unless there is a sufficient guarantee of accountability.

It appears, then, that we don't even know which Internet and electronic commerce regulation strategy should be pursued.

The European Commission seems unwilling to wait for the answer to the dilemma. It decided to allow EU consumers to sue foreign providers of goods and services in the consumer's local court. This decision is an extension of existing law, known as the Brussels Convention, to the realm of electronic commerce. For it to apply, however, the defendant has to have solicited the plaintiff's business. The decision thus classifies a site on the Web as cross-border advertising.

Critics, even some members of the commission, say that this step undermines the legal basis for electronic commerce in the EU as it discourages small and medium-sized enterprises to invest in electronic commerce [Mitchener July 1999].

Although the U.S. government's approach discourages electronic commerce regulation, lawmakers have already passed a laundry list of bills that leave the federal government's fingerprints all over the Internet, and more are in the pipeline. A partial list of legislation the 106th Congress passed or is considering includes rules against cybersquatting, granting legal standing for digital contracts, proposing bans on Internet programming known as Webcasts, prohibiting online gambling and regulating spam, the junk mail of cyberspace. [Clausing Nov. 22, 1999]

A draft electronic commerce law received support from EU economics ministers. The directive on "legal aspects of electronic commerce in the [EU's] internal market" aims to establish legal guidelines for virtually every aspect of electronic services, including online newspapers, databases, financial services, professional services and entertainment such as video-on-demand [Mitchener Dec. 1999]. Issues addressed in the draft include the validity of electronic contracts, liability of Internet intermediaries, online dispute settlement, consumer protection, freedom of speech, advertising and sales promotions. The directive is particularly interesting because it would establish the principle of mutual recognition of the laws of other EU countries and just may be a possible model for global Internet regulation. The implications are significant. For example, Germany will likely be forced to review several controversial laws to bring them into line with those in other countries. The draft directive now faces a second reading in the European Parliament.[9]

[9] The EU approved the "framework directive," the hub of the EU's electronic commerce plans, on May 3, 2000. It establishes online standards across the 15 member states [De Bony 2000].

ACCEPTANCE OF ELECTRONIC TRANSACTIONS

Clarke [1999] suggests "Many of today's trading and settlement practices can be traced back to the heyday of the Venetian and even Phoenician economies, and most of the remainder to Victorian Britain." When one party involved in a business transaction breaches established trading practice, the other party can sue. To prove her case, the affected party needs to provide evidence that is acceptable to the court. One of the many possible reasons for disputes is a failure to comply with the terms of a long-term contract. Conventional regulation requires that such contracts are evidenced "in writing." The identities of both parties must be clear and may need to be authenticated by letterhead, signature, corporate seal, and/or the signature of a witness. These regulations also distinguish between the original document and its copies, relate to the modes of delivery of documents, and may require that the payments accompany certain documents.

This body of law must obviously be amended and adjusted to facilitate electronic commerce. In the U.S., nearly every state has sought to eliminate barriers caused by traditional writing and signature requirements by drafting legislation designed to permit the authentication of documents and signatures through electronic means [Morgan and Gidari 1999]. Forty states either considered or enacted electronic authentication and the count is growing. The important point in our context is that not one but a variety of authentication models were considered or enacted by the states. The legislative efforts focused primarily on limited electronic signature laws, such as transactions with the government or medical records, rather than on general laws. Nevertheless, seven states enacted general legislation, three using the so-called Utah model and four using the California model. At the same time, 36 limited laws were enacted out of the 48 proposed.

Late in 1999, what began as a seemingly simple attempt to stimulate electronic commerce by giving digital signatures the legal weight of their conventional counterparts erupted into a partisan political battle in Congress. Opponents fear that the proposed uniform federal law could wipe out some basic

consumer protections [Clausing Nov. 1, 1999]. One of the issues regards thousands of state and local laws that require institutions such as banks to notify customers by mail of certain situations such as mortgage foreclosures. Under the legislation pending in both the House and the Senate, such companies would be able to make those notifications electronically if the contracts were made online. Opponents fear that companies would be able to sidestep longstanding consumer notification laws. Of five bills meant to give digital signatures the legal weight of their ink-on-paper counterparts that were before the Congress, the House passed a bill that would authorize digital contracts and the Senate passed a narrower bill.[10]

Given the states within the United States differ in their approach to legislate contracting in cyberspace, we should not be surprised that there is no agreement internationally either. "Countries do not always agree on the required scope of electronic authentication legislation." [Baker and Yeo 1999] The good news is that several international initiatives are underway to unify national approaches. They include the draft EU Directive on electronic authentication, the work of the United Nations' Commission on International Trade Law (UNCITRAL) Experts Group in preparing Uniform Rules on electronic authentication, and a proposed international convention on electronic authentication [UNCITRAL 1998]. In September 1999, Asia-Pacific Economic Cooperation (APEC) ministers encouraged members to consider the UNCITRAL model law and agreed on a realistic implementation time frame. They will seek improved electronic access to markets for business and commit to a goal of paperless trading by 2005 for developed and 2010 for developing economies or as soon as possible thereafter [U.S. Department of State 1999]. By December 14, 1999, legislation based on the UNCITRAL Model Law on Electronic Commerce had been adopted in Colombia, the Republic of Korea, Singapore and in the state of Illinois [UN Office of Legal Affairs 1999].

---

[10] On June 16, 2000, Congress has passed this bill and President Clinton was expected to sign it within 15 days [Rosen 2000].

With the introduction of the Electronic Information and Documentation Act, Saskatchewan became the first Canadian province to try to define the ground rules for electronic commerce [Friedman Dec. 1999]. This law is based on model legislation proposed by the Uniform Law Conference of Canada, which is, in turn, based on the UNCITRAL Model Law. Other Canadian provinces are expected to follow Saskatchewan within months, making electronic commerce within Canada more attractive. If several other influential countries decide to put the Model Law on Electronic Commerce into operation, electronic signatures and contracts may become internationally accepted. It is not enough, however, that PKI becomes legally recognized--it also needs to be implemented.

TAXATION

The U.S. Congress passed the Internet Tax Freedom Act (ITFA) in October 1998. This Act placed a three-year moratorium on Internet taxation and established the Advisory Commission on Electronic Commerce to review Internet taxation issues. Controversy started even before the first meeting, though. The National Association of Counties threatened a lawsuit claiming that the Commission is unfairly biased against taxing Internet purchases [McCullagh Mar. 1999]. Members of the Commission, after several meetings, began to focus on a multiyear extension of the moratorium as one measure most members can agree on [Simpson 2000]. In the meantime, the states would be charged with simplifying their tax structures. The proposed compromise would likely include other recommendations gaining increasing support, including a permanent ban on taxing Internet access and removal of the federal excise tax on telecommunications. Other parts of the new proposal are contentious and a number of members doubt the proposal will be successful. There is no way to say how soon this issue can be resolved internationally.

The Commission, which held its first meeting in June 1999, is charged with considering the competing goals of promoting the economic potential of electronic commerce and addressing state and local revenue needs. As with any new industry, a complex tax burden can stifle the digital economy's development

and growth. Yet the revenue needs of states and localities also are undeniable. State and local governments fear they could lose some $17 billion annually in sales taxes by the year of 2002. They rely on sales taxes for 37% of their revenue [Wigfield 1999]. While this commission was working, Senator Ron Wyden (D. Ore) and Representative Christopher Cox (R. Cal) introduced bipartisan legislation in Congress to extend indefinitely the ban on new state or local taxes that single out the Internet. The bill would not, however, settle the question of how existing sales taxes should apply to electronic commerce [CNNFN 1999].

Because there are 5,000 separate state and local tax jurisdictions in the United States with tremendous variation in rates, product categories, exemptions, and administrative approaches, the complexity of tax collection may unconstitutionally burden interstate commerce. One possible solution is to employ technology such as "taxbots" that could seek out the taxes due. The Commission is to consider how taxes on electronic purchases can be imposed without sacrificing consumer privacy. The Commission, with eight members from industry, eight members from state and local government, and three from the federal government, will report its recommendations to Congress by April 2000. Any report must be approved by a two-thirds vote.[11]

Another concern is how other nations may tax electronic commerce and influence international trade and U.S. competitiveness. It is too soon to say how

[11] The Commission completed its work with its Report to Congress, which was delivered on April 12, 2000. A two-thirds majority vote supported the need to bridge the "Digital Divide," to protect consumer privacy, and to make a permanent standstill on international tariffs. A simple majority support included the repeal of the Federal three-percent tax on telephone services, the simplification of states' sales and use tax systems, permanent prohibition from taxing Internet access charges, extension of the current Internet tax moratorium on multiple and discriminatory taxation targeted at the Internet, and clarification of the nexus standards. The House of Representatives voted on May 10, 2000 to extend the existing moratorium on Internet taxation to 2006 [Murphy May 2000].

the Commission will resolve these and many other issues [Advisory Commission on Electronic Commerce 1999].[12]

TARIFFS

World Trade Organization (WTO) ministers agreed in May 1998 to continue the practice of not imposing customs duties on electronic transmissions for a year [Ferranti 1998]. Goods ordered electronically but delivered physically were not covered by this agreement. WTO's General Council adopted a Work Programme on Electronic Commerce in September 1998 to examine all trade-related issues regarding global electronic commerce, taking into consideration the economic, financial, and development needs of developing countries [WTO 1998]. The reports on the progress of the work program and related recommendations were supposed to be made at the Third WTO Ministerial Conference in Seattle on Nov. 30 - Dec. 3, 1999. The General Council established several subordinate entities to study a variety of issues and report to the General Council. One of them - Council for Trade and Services - was to examine and report on the treatment of customs duties among other issues.

The U.S. position is consistent. It was first presented by Clinton and Gore (1997) and concisely reiterated by Daley [Daley 1999a]: "But one thing that I think we must all agree on is that the Internet must be a duty-free zone. No ifs, ands, or buts."

Governments of many nations are looking for new sources of revenue, however, and may seek to levy tariffs on global electronic commerce. It appears that governments of developing countries would lose about three times more income by not charging customs duty than developed countries. The total amount of currently lost tariffs is virtually negligible and represents only 0.1 percent of all tariffs. However, with increased bandwidth, the international electronic transmission of digital products such as music and video material is

[12] With a draft law recently made public, the European Commission wants to place a value-added tax on non-European companies that sell and deliver products online. Such a tax is already imposed on European companies [Echikson 2000].

going to increase. Developing countries are wary of signing anything rapidly on cyberspace, arguing they need more time to study this new and complex area [Nando.net Online May 18, 1998]. They will import much more of such content than they will export, will thus end up with a net loss of income. It is likely that they will try to implement customs duty on electronic transfer of digital content.

Even Europe is not quite ready to ban tariffs on electronic commerce permanently, although businesses on both sides of the Atlantic say "hands off the Internet" [Dougherty 1999]. European governments could lose massive amounts of revenue if commerce began shifting to an Internet that was entirely duty free.

INTELLECTUAL PROPERTY PROTECTION

Legal issues regarding patents, trademarks, trade secrets and copyrights are collectively known as intellectual property issues. It used to be a fairly quiet legal domain but the Internet made it red-hot.

The World Intellectual Property Organization (WIPO), an arm of the United Nations, adopted two treaties dealing with copyright law in December 1996. Representatives from 160 countries attended this diplomatic conference [Eisenberg 1999]. The treaties were created to adjust current intellectual property protections to the digital age and expanded global electronic commerce. Before these treaties can come into force, 30 countries must ratify them.

On October 12, 1998, the U.S. Congress passed the Digital Millenium Copyright Act (DMCA), ending many months of turbulent negotiations regarding its provisions. Two weeks later President Clinton signed the Act into law. The Act implements the WIPO treaties signed in December 1996 and contains additional provisions. Although it promises less ambiguity, critical legal questions still plague intellectual property owners and online users [Oliva and Prabakar 1999]. One example is the implied license to copy. Posting a file on an FTP server implies permission to make a copy. So does posting on the Web site in the sense that in the act of browsing, the material will temporarily be stored on disk. Whether printing the material or saving it to disk intentionally for later use also

implies consent is an unanswered question. This issue will require further definition from the courts.

Another example of ambiguity is the fair use doctrine. Certain portions of a copyrighted work can in some situations be copied, adopted, or distributed without permission of the copyright owner. There are no hard and fast rules, though, to determine whether copying is "fair use" or not. Similarly, copying a small part of a work is allowed. However, if the copied section is qualitatively important to the work as a whole copying may still be infringing. Copyright issues online will continue to unfold over coming years.

Vendors are already marketing different incompatible combinations of technological features combining digital watermarking, copy protection, and encryption as solutions to the problem [Schull 1999]. The DMCA outlaws circumventing such devices or creating products and services to defeat them.

Conventional copyright law does not provide protection to data compilations where data is not creatively modified or summarized. The EU decided to create a new form of intellectual property protection for those who have made substantial investments in developing databases [Samuelson 1999]. In the U.S., the Collections of Information Antipiracy Act passed in the House of Representatives in 1998. There was much opposition, though, from the scientific and educational communities as well as the Department of Commerce and the Department of Justice. These issues will be on the legislative agenda during the 106th Congress.[13]

Although the DMCA clarified some concerns surrounding intellectual property protection, the reality is rather unsettled. A good example is the rapidly spreading MP3 technology enabling distribution of nearly CD quality audio recordings over the Internet. *WiredNews* reported over two years ago [Brown 1998]:

> "There are thousands of FTP sites around the Net, many maintained by high school or college students who use the freely available

[13] On June 2, 2000, the Bill was on the Union Calendar, Calendar No. 212.

MP3 (or MPEG-1 Layer 3 compression format) software to turn their CD collections into digital computer files. Those files, which at three megabytes are one-sixteenth the size of CD singles but retain their CD sound quality, are being traded around the Web, played on computers, and used to promote the MP3 format. But copying is illegal, and since the files can be easily burned into new CDs, the recording industry is wary about letting the practice continue."

This sounds like an understatement. The recording and distribution industries appear to be in a state of panic. The Recording Industry Association of America brought suit in October 1998 in an attempt to prevent Diamond Multimedia from releasing its portable MP3 player but an appeals court judge in California ruled that an MP3 player isn't subject to government restriction, clearing the way for more companies to market the devices [Sprenger June 1999].[14]

A more recent example of the unsettled marketplace is that of Lucasfilm Ltd. Its legal counsel sent letters to 700 Internet service providers alerting them that illegal copies of *Episode I - The Phantom Menace* might show up on the Web. The letters also asked them to be responsible for finding and blocking access to such content as instructed by the DMCA [Collett 1999]. Policing the Web sites is not the provider's responsibility under the act, though, as "safe harbors" qualify them for one of the several exceptions from liability.

Another issue in this category is patents and the Internet being their breeding ground. The issues arises from a ruling in July 1998 by the Federal Circuit U.S. Court of Appeals, which ruled that companies could patent business methods. The U.S. Patent and Trademark Office gave out more than 1,000 Internet and networking patents in 1998. The lawsuit that Priceline filed against Microsoft's Expedia, charging patent violation, is the first high-profile legal tangle involving the controversial practice of patenting Internet business processes

[14] Loosely grouped as "distributed file-sharing," about a dozen Napster-type programs have sprung to life in the last few months. All work off the same basic model--opening up millions of Net-connected hard drives for worldwide searches and user-to-user downloads [Bedell 2000].

[Murphy Oct. 14, 1999]. Open Market patented shopping carts, NetDelivery and InterMind patented push technology, CyberGold patented technology for compensating people for paying attention to online information. Netcentives won a patent for its idea of awarding frequent-flier miles to shoppers who buy online. Priceline patented a buyer-driven electronic commerce model where a buyer offers to buy an airline ticket for a suggested price and waits for the price to be accepted by an airline company. The proliferation of patents caused Tim Berners-Lee, inventor of the Web, to warn that patents are threatening the universality of the Internet. He urged the Internet community to help end the patent frenzy. In the meantime, the number of suits grew; DoubleClick filed one against L90 Inc., Cdnow and MusicMatch.com are litigating, Amazon's lawyers are suing barnesandnoble.com [Zelnick 1999] and U.S. District Judge Marsha J. Pechman granted an injunction against barnesandnoble.com [Anonymous Dec. 2, 1999]. Paul Goldstein, a Stanford University law professor, argues that this issue could bring e-commerce to a halt as does Paul Hagen from Forrester Research [Eisenberg 1999].

COMMERCIAL POLICY

The General Agreement on Trade in Services (GATS) is the basic instrument establishing the rights of service suppliers to compete freely in each others' markets. It applies to all services (except those supplied by governments) regardless of the means of delivery - whether by person, mail, telephone, Internet or other proprietary network. Thus a charge on the electronic export of a service by the importing country would not be permitted if that would violate a member's commitments under the GATS. While the GATS currently covers a broad range of services generally, including telecommunications and financial services, the Telecommunications Working Group of the Federal Trade Commission recommends that scope and substance of the commitments under the GATS agreement should be widened to cover as much of the services sector as possible [Coalition of Service Industries Electronic Commerce, Information Technology & Telecommunications Working Group 1999].

One of the more recent communications from EU to WTO expresses another basic disagreement: "The legal nature of 'digitised products' (music, films, software or 'books' material on the Internet) is still under discussion in the WTO. We argue that all electronic deliveries - including 'digitised products' - are services and therefore the GATS applies. This is also the view of most other WTO members and the WTO Secretariat. On the contrary, the U.S. and to a certain extent Japan argue that while the transmission of those 'products' is a service, the 'products' themselves are analogous to goods and therefore fall under the [General Agreement on Tariffs and Trade] GATT" [EU: Directorate General I 1999]. This issue and many others are currently being discussed within WTO. It is not clear how long is it going to take for WTO members to come to an agreement but issues are complex and it appears that the consensus is building only slowly and only on a few of many issues.

Another example of the difficulties in establishing commercial "rules of conduct" for electronic commerce is the U.S. FTC's attempt to adopt over 40 "Trade Rules" and "Guides" to the Internet and other electronic media. In May 1998, the FTC issued the Interpretation of Rules and Guides for Electronic Media, Request for Comment [Federal Register May 6, 1998], with the intention not to regulate but to solicit discussion and public comments on the issues that would be addressed in a future policy statement. As can be expected, the FTC's primary concern is consumer protection. The FTC believes that its proposed policy statement will provide guidance to encourage voluntary compliance by industry and promote industry self-regulation.

The FTC's rules addressed in this document prohibit specific unfair or deceptive acts or practices and may prescribe requirements to prevent such acts or practices. The policy statement would not create any new rights, duties, obligations, or defenses, but instead would clarify the rights, duties, obligations, or defenses that currently exist. When a change of rules would be necessary, the FTC will follow the required rulemaking procedures. Even though the intent of the proposed policy statement is to provide additional guidance and not to change

rules, comments the document solicited voice general disagreement with the FTC's intention.

The International Chamber of Commerce (ICC) is also involved in creating global trust in electronic trade transactions by defining best business practices for electronic commerce. ICC's Electronic Trade Practices Working Group is creating a set of foundation rules for electronic trade and settlement [ICC 1998]. The objective of this Group is to make trade more efficient by not only adapting rules to new technologies and media such as the Internet, but by taking advantage of these new tools to streamline trade transactions. Its focus is in adjusting the legal framework for conducting negotiations, making contracts, and arranging for finance, transport, or insurance electronically, recognizing that paper has inherent weaknesses as an information carrier. The group is finalizing a set of proposed rules in close coordination with ICC members in more than 130 countries.

PAYMENT SYSTEMS

Conventional payment systems, such as checks and credit cards, still dominate consumer payment services. Credit cards are the payment device of choice for retail Internet services as they offer a high level of consumer protection. The popularity of conventional payment devices, particularly in the Unites States, is one reason why innovative payment systems are not yet successful in this market. These new technologies include accounts in virtual banks, digital cash, digital checks, other "micropayment" technologies involving digital wallets, and smart cards. Although the need for inexpensive ways to process very small payments appears real, it is unclear when the market will endorse this technology.

The problems with the use of credit cards as the dominant payment device on the Internet may soon increase. Visa International Inc., for example, reported that half of Visa's transactions from online sales are disputed or full-fledged frauds [Nash and Harrison 1999]. An earlier report [Morgan Mar. 8, 1999a] suggests that credit card fraud is alive and well on the Web and that fraud rates

between 8% and 20% aren't unusual for new merchants [Morgan Mar. 8, 1999b]. The victims are the merchants rather than consumers. Card issuers and merchants cannot contest a cardholder's claim that a charge is unauthorized in a transaction in which the card was not available for inspection by the merchant, according to the current interpretation of Regulation Z, the regulation protecting the cardholders. Furthermore, under the rule of the credit card association, the card issuer is allowed to charge the transaction back to the merchant who presented it [Winn 1999].

Merchants will likely press for improved authentication technology or revisions to Regulation Z. In lieu of that, the merchants need to pay personal attention to each transaction or buy expensive but effective screening services and outsource the transaction check. Banks and credit-card processors use sophisticated systems to discover anomalies in a buyer's ordering process. Such systems use neural networks and other artificial intelligence techniques in addition to simple matching of delivery and cardholder's addresses. One company reduced the fraud rate to less than 1% by using antifraud software and elaborate screening systems [Morgan Mar. 8, 1999a]. Morgan also learned that when thieves are international, "You don't even know where to begin. Who's got jurisdiction?"

V. ENHANCING INFORMATION INFRASTRUCTURE

DEVELOPMENT OF INFORMATION INFRASTRUCTURE

The existing Internet technology was developed many Internet years ago and scaled up extremely well. However, it shows its age and its many limitations. Among them are:

- limited point-to-point throughput,
- scarcity of IP addresses, and
- a very basic, primitive protocol.

The National Science Foundation (NSF) recognized these limitations and in 1993 initiated several separate but coordinated projects to develop a faster and more reliable communications medium [NSF 1999].

One of the NSF sponsored projects is the creation of the very High performance Backbone Network Service (vBNS) through its partnership with MCI WorldCom. The vBNS was created in 1995 and links two supercomputer sites and 150 research institutions with high performance network connections operating at OC-12 (622 Mbps) speed. One section linking Los Angeles and San Francisco was upgraded to OC-48 (2.4 Gbps) in 1999. The rest of the vBNS will be also gradually upgraded to OC-48. In addition to high speed, vBNS also offers new functionality and supports IPv6, Quality of Service, multicast, and other features[15]. IPv6 is an abbreviation for Internet Protocol version 6, which is capable of handling reasonable scenarios of future growth. Quality of Service enhancements provide a reserved bandwidth service and differentiation between applications that need bandwidth reservation and those that can operate with a best-effort service. The multicast function enables a source to send a packet to a group of interested end stations, where the group membership and topology information can be adjusted dynamically.

President Clinton and Vice President Gore announced an initiative called the Next Generation Internet (NGI) in October 1996. The president pledged funding to connect research universities and laboratories with high-performance networks. About 100 organizations should be provided with speeds of 100 times today's Internet and additional 20 sites with connections at speeds of 1,000 times today's Internet. The key players in this initiative are again the NSF and the Department of Defense, Department of Energy, NASA, the National Institutes of Health, and the National Institute for Standards and Technology. The maximum measured end-to-end performance is about 80 Mbps but it is expected that the performance will be significantly improved in the future [President's Information Technology Advisory Committee 1999]. On October 28, 1998, President Clinton

[15] vBNS transitioned on April 1, 2000 to vBNS+. The typical link is OC-48 (2.488 Gbps) while a couple of OC-12 (622 Mbps) connected routers remain. vBNS engineers have driven an OC-48 circuit terminated by Jniper M40s to over 2 Gbps data rate, which was sustained for many days. It offers advanced features, such as performance based IPv4, Quality of Service, IP multicasting, Native IPv6, etc. It offers access to the commodity Internet and is available to anybody in 48 continuous states in the U.S. allowing access at speeds ranging from T-1 to OC-12 [vBNS 2000].

signed into law the NGI Research Act, a bill designed to keep the U.S. on the cutting edge of Internet technology development.

More than 150 of the nation's institutions of higher education launched an independent project called the Internet2. They are researching and developing a new generation of applications to take advantage of advanced networks. Internet2 also involves additional functionality such as IPv6, scalable Quality of Service, and multicasting. Many of these institutions received support from NSF to connect to vBNS or to "Abilene," a network developed by the University Corporation for Advanced Internet Development, a home for the Internet2 institutions and their committees. Abilene is an advanced backbone network that connects regional network aggregation points, called gigaPoPs, to support the work of Internet2 universities as they develop advanced Internet applications. The Abilene Project complements other high-performance research networks, such as those in Canada and Scandinavia.

As we can see, researchers and developers are involved in several Internet initiatives in the U.S. and globally. While various initiatives within the U.S. are well coordinated by the Large Scale Networking Working Group, coordination does not seem to be the case internationally. Development and testing of these improvements will take several years. For example, the Time Line Summary of the NGI Implementation Plan [National Coordination Office for Computing, Information, and Communications 1998] suggests that terabit-per-second packet switching technology will be demonstrated in 2002 and that more than 10 advanced applications will be in the testing stage over the ultrahigh performance test bed by that year as well. Thus, commercial use of the next generation Internet is at least several years away.

The development of Internet2 appears to run on about the same timeline as NGI. Technology transfer is a major goal of the project. While the timeline is not published, corporate partners collaborating with Internet2 universities are expected to begin integrating the results into their commercial products at the end of 2000 [Wood 1999]. The first results are expected in the areas of multicasting, Quality of Service, digital video, and distributed storage.

In response to a move by AT&T to build a cable TV system that will provide voice telephony and high-speed data connections, SBC Communications Inc. plans to spend $6 billion to upgrade its local phone networks so they can deliver ultra-high-speed Internet connections. SBC's plan is to provide high-speed data connections to about 80 percent of its customers in 2002 [Van Oct. 1999]. These, and competing wireless projects such as Teledesic's global broadband "Internet-in-the-Sky," promise to solve the "last kilometer" problem in a few years. That is, we can expect broadband connections and next generation Internet service to our offices and homes in a time frame of several years, at least in the developed areas of the world if not globally.

INTERNET GOVERNANCE

The Department of Commerce entered into an agreement with a new organization named the Internet Corporation for Assigned Names and Numbers (ICANN) on November 25, 1998. ICANN was designed to initiate an implementation plan under which the private sector undertakes the management of the domain name system functions. The U.S. Government intended to transition technical management functions to the private sector gradually by September 2000. The Board of ICANN is composed of nineteen Directors: nine At-Large Directors, nine selected by ICANN's three supporting organizations, and the President/CEO (*ex officio*). The nine current At-Large Directors are ICANN's initial Directors and will be succeeded by At-Large Directors. They are telecommunications executives and academics from the U.S., Europe, Asia, Australia, and Latin America. Esther Dyson, an analyst, publisher and entrepreneur, chairs the interim board. The lack of information about how the interim board was created has fostered a conspiracy theory about the board's hidden agenda [Clausing June 7, 1999].[16]

ICANN is currently run by 10 directors appointed by a small group of Internet insiders and has been criticized for ignoring the public in favor of the

[16] Later this year, five At-Large Directors will be selected by ICANN's At-Large Members in a worldwide online election [ICANN 2000]. Another four will be elected in 2001.

richer large corporations and special interest groups [Clausing Nov. 5, 1999]. Critics such as Iperdome, Inc. [Fenello 1998] complained that ICANN is working behind the scenes with powerful international corporate and government interests to create a top-down hierarchy that flies in the face of the free-wheeling, consensus-based spirit that built the Internet. Some observed that the Internet is now in less stable hands, which increases the risk that angry factions may secede from the network, splitting it into several disconnected networks. Other observers reasoned that if the interim board pushes too far and loses support among key constituencies, ICANN itself could be undercut, which would lead to a situation with nobody in control.

Responding to this criticism, the Commerce Department recommended that ICANN:

- eliminate a $1 fee on Internet address registrations,
- open its board meetings to the public immediately, and
- draft clear restrictions on the boundaries of its authority [Clausing July 1999].

In response, ICANN eliminated the fee and made its board meetings public.

One of the ICANN's first assignments was to break up the monopoly of Network Solutions, Inc. in assigning the most popular domain names ending with .com, .net, and .org. It succeeded, to an extent, as Network Solutions reached a settlement in late September 1999 to open up the domain name registration to competition. After several months of negotiations, Network Solutions became an accredited registrar or retailer through 2004, with the right to renew indefinitely. It will also operate the central database of names for which the competitors pay $6 per name annually [Loftus 1999]. This agreement will allow more than 80 companies to compete in the registration of Internet domains and give consumers and businesses around the world lower prices, better service, and other options in registering Internet addresses [Clausing Nov. 5, 1999].

Network Solutions formally recognized ICANN as the body overseeing domain-name registration and agreed to operate its registry in accordance with ICANN's provisions. This settlement has been approved by ICANN at its November 2-4, 1999 meeting in Los Angeles, California [Clausing Nov. 5, 1999].

INTERCONNECTIVITY AND TECHNOLOGICAL CONVERGENCE

Open access to the Internet is often taken for granted, at least in the U.S. However, a 1999 court ruling illustrates that this issue is not settled yet. The U.S. District Court in Portland, Oregon ruled on June 4 that AT&T must allow competing Internet service providers access to its cable system in Portland [Richtel 1999]. AT&T planned to keep exclusive control of its new high-speed network. The ruling does not bind AT&T or other cable operators elsewhere. According to this report, Mark Rosenblum, vice president for law at AT&T, called the decision "inexplicable," arguing that Portland and the county are beyond their legal authority in requiring open competition. A spokeswoman for a coalition of Internet companies that pursued open access praised the ruling and suggested that it will likely spark more action by local authorities.

Soon after this court ruling FCC Chairman William Kennard said a national policy is needed to govern high-speed access to the Internet via cable-television lines [Chen 1999]. He suggested that there would be chaos if local regulators all pile in with their own rules for broadband connections and that a national broadband policy is in the national interest. AT&T, which committed $120 billion to buying cable companies, said these investments won't be worthwhile if it must open its cable lines to competitors. In the meantime, the local authority in Broward County, Florida, also imposed requirements to carry competing Internet service providers on its approval of the transfer of TCI's local cable franchise to AT&T.

In July 1999, the National Association of Counties approved a resolution backing the right of local governments to require open access and urged the FCC and Congress to adopt such policies. Mr. Kennard, however, reiterated his opposition to regulation of Internet on cable. He said that FCC would back

AT&T's appeal of a federal court ruling in Portland [Wired News Online, July 21, 1999]. Later in July, the Board of Supervisors in San Francisco voted to grant a transfer of TCI's cable TV franchise to AT&T without requiring that AT&T pledge to offer America Online Inc.'s (AOL) Internet access service on its cable system [Van July 1999]. In mid-August, the FCC asked a federal appeals court to stop Portland from forcing AT&T to open its cable lines [Gruley 1999]. Mr. Kennard said he wants to ensure a national no-regulation policy for the Internet, rather than let local governments impose rules that could differ from community to community.

In the hope of avoiding regulations that might set terms and conditions AT&T would rather avoid, the telephone giant in early October 1999 suddenly decided to offer open access within a few years. AT&T is trying to find concrete ways to demonstrate that commitment [Schiesel Oct. 1999]. It cannot move quickly because of a contract that obligates it to give exclusive cable access until 2002 to the Excite@Home Corporation. This position was reiterated in a later announcement [Schiesel Dec. 1999].[17]

AOL was one of the most vocal lobbyists for open access to the cable networks until it announced its merger with Time Warner. Observers expected that AOL would change its position, which indeed happened [Wired News Online, Feb. 14, 2000]. AOL officials confirmed they have ended their lobbying push in various states for legislation requiring cable firms to share high-speed Internet lines with competitors but stressed they still favor an end to cable's exclusive Internet service deals. AOL is now working with Time Warner to craft a set of voluntary principles allowing multiple Internet providers on cable systems.

This struggle for open Internet access using cable is happening in the U.S., arguably the most open telecommunications market in the world. We can speculate that much more intense and lasting effort will be needed to open the access and provide interconnectivity worldwide.

---

[17] Reversing a lower court, the United States Court of Appeals for the Ninth Circuit ruled on June 22, 2000 that a local government could not force a cable company that offered Internet access to share its telecommunication lines with rival providers of cable modems [Richtel 2000].

INTERNET TECHNICAL STANDARDS

Some observers argue that the smooth standards setting operation of the Internet Engineering Task Force (IETF) has become burdened by the extensive financial implications of their decisions on technology vendors and business Internet users in general. The size of this organization's workload is becoming an issue. IETF now involves 117 active working groups, many with profound implications for service providers' multiservice architecture plans and for the future direction of the Internet itself [Caron 1999]. Two IETF efforts of particular interest to service providers are:

- Multiprotocol label switching (MPLS), a critical routing improvement enabling the Quality of Service, and
- IP multicasting, also seen as nothing less than a savior of the Internet infrastructure.

IETF uncharacteristically struggled with MPLS and IP multicasting for years and multicasting is still under construction. The controversy surrounding MPLS illustrates IETF's problems. Cisco and Nortel differ about how to implement it, so it became a big money, high-stakes issue. As a result, IETF could not adopt either technology. The conflict remains unresolved, leaving it up to vendors and service providers to decide which approach to take or to support both.

Despite such frustrating experiences, Internet standards are generally evolving, but some Internet related technologies are not. For example, a dispute between AOL and Microsoft and others erupted in late July 1999 about instant messaging services. Microsoft and Yahoo had reverse engineered AOL's instant messaging technology. Their accomplishment angered AOL, which would like to control the messaging market.[18]

In another case, IBM and Compaq are pushing for new Net standards on micropayments. This software enables businesses to sell merchandise over the

[18] On June 15, 2000, a week after federal antitrust enforcers began investigating AOL's instant-messaging policies, it made its first gesture toward allowing open access to its wildly popular messaging system [Angwin 2000].

Internet in small amounts, that is, any amount too small for a credit card. The tool will accept all micropayments under $1 with a mouse click. Currently, most sites keep track of small items and roll them into a monthly credit card transaction. According to Russ Jones, business manager of Compaq's MilliCent micropayment technology, "Standardized pricing markup will do for Internet content what the Universal Bar Code standard did for retail merchants" [Hershman 1999].

The PC industry's dream of leaping into the living room is far from reality, perplexed by a lack of agreement on standards between computer companies and consumer electronics manufacturers. "It's a big morass… Nobody's talking to anybody else" believes Kevin Fong, general partner at the Mayfield Fund [Stroud 1999]. PCs are not compatible with consumer appliances and home LANs are still far too complicated for widespread use.

Another unresolved domain for standards is that of wireless Internet access technology. Although negotiators from around the world settled on a wideband code division multiple access (CDMA) for the so-called third generation cellular telephony, carriers in the U.S. are still fighting over standards. In Japan, trials are already underway on an advanced wideband wireless transmission technology. Japan may drive the global standard and become a leader in the next generation of mobile phones [WuDunn 1999]. In Europe, cellular phone carriers from Scandinavia through Germany and down to Italy plan to start text-only wireless Web sites for mobile phones [Andrews 1999]. European governments, too, are setting the stage for third generation wireless networks. In the U.S., AT&T and others are pushing a third generation technology called EDGE while other big players such as Sprint and Bell Atlantic are pushing wideband CDMA. Conflicting standards slowed advances considerably.

Some news is good, though. The International Telecommunications Union (ITU) wrapped up a full set of standards for asymmetric digital subscriber line (ADSL), the technology for high-speed transfer of data over standard copper phone lines [Oakes July 1999]. The UN standards body approved the standard in July 1999. This development changes the projection for the number of wide

bandwidth connections to more than 10 million by 2001 from prior projection of only 2 million users.

ENSURING ADEQUATE BANDWITH AND ACCESS

It may come as a surprise that adequate bandwidth and access is not available both across the globe and also within the U.S. In a 1999 report the iAdvance coalition, an organization of public interest groups and telecommunications and technology companies, found telecommunications regulations slowed the development of high-speed Internet backbones [Olbeter and Robinson 1999]. The report lists a dozen states at highest risk of being left behind because too few backbone hubs are being built outside population and financial centers. The states accessing the Internet through the digital equivalent of dirt roads are Arkansas, Alabama, Idaho, Iowa, Maine, Montana, New Hampshire, North Dakota, Oklahoma, South Dakota, West Virginia, and Wyoming.

The U.S. Department of Commerce's National Telecommunications and Information Administration noted other aspects of Internet access inequalities. The third report in a series "Americans in the Information Age Falling Through the Net" [NTIA 1999] provides evidence that the "digital divide" between certain demographic groups and regions in the U.S. continues to persist and in many cases is widening significantly. Minorities, low-income persons, the less educated, and children of single-parent households, particularly when they reside in rural areas or central cities, are among the groups that lack access to information resources. The authors claim that: "Whites are more likely to have access to the Internet from home than Blacks or Hispanics have from *any* location" and that "[I]t is reasonable to expect that many people are going to lag behind in absolute numbers for a long time." Education and income appear to be among the leading elements driving the digital divide today. Because these factors vary along racial and ethnic lines, minorities will continue to face a greater digital divide as we move into the 21st century. The researchers suggest: "[W]e need to encourage the buildout of broadband networks to rural and other

underserved areas of our nation, so that all Americans can take full advantage of new information technologies and services" but concede that: "It is highly unlikely that, in the foreseeable future, prices will fall to the point where most homes will have computers and Internet access."

The initiatives are encouraging, however. In an effort to bridge the widening "digital divide," the Clinton administration proposed a $50 million plan to link low-income families to the Internet [Jacobus 2000]. The proposal would help about 9 million households that are currently on the U.S. food stamps program. In a separate plan, President Clinton called for $2 billion in tax incentives over 10 years to encourage the private sector to donate computers, train workers and sponsor technology centers to connect schools to the Internet.

A totally different hurdle was introduced by AOL, which has been promptly hit with a class-action lawsuit claiming that the latest version of its software prevents customers from using rival ISP accounts [Wired News Online Feb. 2, 2000]. Lawyers representing the plaintiffs argue that users are paying a monthly access fee, but AOL does not allow them to use their ISP. They request damages of $8 billion, or $1,000 for each of the 8 million AOL customers who have upgraded the AOL's software to version 5.0.

Switching to a global perspective brings up similar intentional constraints imposed by governments as another factor limiting access to the Internet. In the Middle East and North Africa, for example, governments adopted various means to restrict the flow of information and thus commerce online [Human Rights Watch 1999]. Saudi Arabia, Yemen, and the United Arab Emirates impose censorship using proxy servers, which block specified content. Tunisia enacted detailed Internet-specific legislation to control online speech. Internet users in Bahrain and Tunisia suspect that the right of privacy is being violated by government surveillance of e-mail. Taxation and telecommunications costs keep the Internet out of reach of all but the most affluent in many countries.

A French media organization, Reporters Sans Frontières, similarly reported that twenty nations all but bar the Internet from their borders [Reporters Sans Frontières 1999]. They also found that additional 25 countries severely

restrict the Internet by forcing users to filter content, subscribe to a state-operated ISP, or register with authorities. The list includes the countries of Central Asia and the Caucasus, including Azerbaijan, Kazakhstan, Kirghizia, Tajikistan, Turkmenistan, and Uzbekistan. Also on the list are Belarus, Burma, China, Cuba, Iran, Iraq, Libya, North Korea, Saudi Arabia, Sierra Leone, Sudan, Syria, Tunisia, and Vietnam. People in Iraq, North Korea and Libya don't have the right to use the Internet at all. The countries listed represent over 28% of the world population.

On the positive side, some developments suggest that one of the technical issues - the throughput - will be resolved rather soon. At the Telecom conference in Geneva Nortel showed that it could send data with a speed of 80 gigabits per second over a single optical fiber along a 480 km long loop on equipment we may be able to use by 2001. Using a conservative application of dense wave division multiplexing to multiply that capacity, Nortel claimed a bandwidth of 6.4 terabit per second [Nortel Networks 1999]. Lucent Technologies similarly reported that its new switching technology product using microscopic mirrors can switch 10 times the amount of data carried by the entire Internet [Schiesel Nov. 1999]. This kind of innovation suggests that backbone throughput is a short-term concern.

FURTHERING COMPETITION

The U.S. Government, the OECD and other influential international institutions consistently call for increased competition in all electronic commerce technologies, but such competition cannot be taken for granted. Those who remember the war for market dominance in the Web browser technology recall that it was anything but open competition.

Furthering competition focuses in most discussions on telecommunications services that used to be government monopolies all around the world. In February 1998, the WTO Telecommunications Services Agreement went into force and 70 countries began implementing commitments to provide market access and a pro-competitive regulatory environment for basic

telecommunications services. It is extremely difficult to accomplish these goals. A monopoly in leased telephone lines worldwide still exists in over two thirds of the countries although the U.S. government provides technical assistance to telecommunications regulators to help them implement this agreement [WTO 1999].

To establish and foster successful competition, a government appoints an independent regulatory body and establishes a pro-competitive interconnection policy. The presence of clear interconnection rules provides new entrants with the ability to compete on a level playing field with the former monopoly. The effectiveness of such rules can only be guaranteed by a telecommunications regulatory body that is guided by pro-competitive, consumer-oriented principles, is shielded from political influence, and engages in open and transparent decision making [*ibid*.].

While privatization is the most important short-term item on the agenda for transforming the telecommunication sector in many developing countries, opening markets to competition will almost certainly be more significant and profound in the long run. Being aware of this, more and more countries are beginning to wrestle with the complicated developments that are set in motion when a government pursues a policy of both privatizing and opening the market to the entry of new carriers [*ibid*.].

Regulatory expertise is developed only gradually. Although development of telecommunications is essential to the overall development of a national economy, the political system, the legal framework and the availability of human resources largely affect what can be done in practice. Major factors cited by developing countries as influencing the implementation of telecommunication reform are private-sector participation, shortage of sufficient government funds for infrastructure development, ineffective termination of the monopoly, and creation of an enabling environment for investment in the telecommunication sector. A regulatory body independent from any supplier of telecommunication services ensures that telecommunication services will be provided in the best interest of the public. Regulators are best able to be impartial if they do not have

a personal or financial interest in the entities, which they regulate or oversee [*ibid.*]. Many governments find the enactment of needed changes extremely difficult and elusive, and possibly, in some cases, undesirable.

Competition within the United States has been constantly in the minds of FCC administrators since 1984. The United States Internet Service Providers Alliance (USISPA) put a new twist to this issue in 1999. It accused the Baby Bells of behaving in an anti-competitive fashion that keeps the ISPs from serving their customers [Murphy Oct. 13, 1999]. USISPA members plan to lobby Congress and the FCC to stop local phone monopolies and to make ISPs able to provide advanced telecommunications services on the same terms.

VI. MAXIMIZING BENEFITS

UNDERSTANDING THE DIGITAL ECONOMY

The final report from the 1998 Ottawa conference [WGEC 1998] recognizes that electronic commerce will extend markets and create new businesses. These changes will create new and skilled jobs, but will also eliminate other jobs. Electronic commerce will thus impact business, the economy and society. Representatives of trade unions and consumer organizations at that conference stressed the need for broad interrelation between society and technology. Representatives outlined several areas of current and future work, which they considered as critical to achieve the full social and economic potential of electronic commerce. These included access, skills and digital literacy; privacy, trust and content; and social impact, and costs and benefits. In the context of the last concern, representatives recognized that electronic commerce spatially extends the markets and creates new businesses. To cope with social impacts, to avoid or to reduce risks and to ensure a broad distribution of benefits in favor of social equity and the quality of life, these representatives of trade unions and consumer organizations stressed the need to consider the broad interrelation between society and technology.

The conference agreed on a seven-point near-term program. One of these points calls on the OECD to extend analysis of the economic and social impacts of electronic commerce.

A number of economic and social implications of electronic commerce are apparent, but are not yet well understood [OECD 1998c]. Some of them are:

- new channels of knowledge diffusion and human interactivity in the workplace will be opened,
- new relationships will be created among businesses and between business and consumers,
- traditional intermediary functions will be replaced,
- more flexibility and adaptability will be needed,
- workers' functions and skills will be redefined and higher-skilled workers will be needed,
- regulations will be reformed,
- economic and geographical boundaries will erode,
- consumers' expectation of openness will cause transformations for better (increased transparency, competition) or for worse (invasion of privacy),
- the importance of time will be reduced, which will change business structures and social activities.

These and other changes require a re-examination of business frameworks, governmental policies and commercial practices and policies, most of which were formed with a much different image of commerce in mind. It is thus necessary to understand the economic and social implications of electronic commerce.

The U.S. Government Working Group on Electronic Commerce acknowledged in its First Annual Report [WGEC 1998] "The economic and social influence of electronic commerce and information technology is complex, broad, and likely to expand in the future. But the full economic and social implications are presently not well understood." The Group added these implications to the set of important unresolved issues. The same Group reported some progress a year later, but nevertheless repeated that: "The emerging digital

economy presents difficult methodological and resource allocation problems for statistics collection and analysis, and poses challenging questions about long-term social and economic implications. The digitization of the economy is difficult to assess because it is so pervasive and is reflected in a series of interrelated phenomena – new infrastructure, processes, and transactions. However, there is growing recognition that better information about the digital economy is needed, whether for private investment decisions or for developing sound public policy." [WGEC 1999]

J. Bradford De Long [De Long 1999] posed six questions he considers essential to any analytic overview of the emerging digital economy. Some of these questions do not presently have any clear answers—an indication of the uncertain and confused state of our knowledge at this point—but together they do convey how the digital economy is different, in some ways startlingly so, from the market economy of orthodox economics. His questions are:

- Will the economies of scale unleashed by the interconnection and interoperability of digital networks compel convergence towards a single, uniform framework of governance and regulation and substantially curtail institutional variation and experimentation?
- Why is fashioning governance and regulatory structures for the digital economy so different and difficult?
- What should the new legal and regulatory framework be?
- Are organizations and persons now achieving greater mobility and, if so, will this substantially delimit the institutional and regulatory options open to policy makers?
- What will be the dominant form of political and economic organization in the coming era?
- How can we ensure that the policies pursued by nation-states in fostering and adjusting to the digital economy will produce positive-sum games, rather than the zero or negative-sum games that are all too common in the world of international affairs?

He concludes by reiterating "Neither of these questions points to clear answers at this early stage in the development of the global and digital economies. Yet we had better keep them in mind as we face the inevitable challenges and strains of political economic change."

MEASURING ELECTRONIC COMMERCE

Measuring electronic commerce is being discussed internationally so that simple and understandable measures can be developed. The measures need to be globally standard to enable meaningful comparisons. At an OECD Workshop on defining and measuring electronic commerce, Elmer [1999] proposed a measuring framework and stressed that two very different definitions of electronic commerce and methodologies for measuring are needed:

- end-use, which relates to the business to consumer and business to business delivery of products and services,
- business to business cooperation during the process of design and development of products and services.

The latter is more difficult to define and measure.

Also at this workshop, Kaplan proposed a number of specific variables, some unique to the French environment such as the use of Minitel, along with assessments of the ease of gathering and quality of available data [Kaplan 1999]. Little data is available and some of the available data is of rather low quality or incomplete.

It may take several years to organize the gathering of data from the four relevant categories [Elmer 1999]. They are:

- supply-side offerings, measured for example by Web seller surveys,
- demand-side behavior, measured by household and corporate buyer surveys,
- macro environment, measuring total market sizes by sector, industry, and geography,

- technological environment, measuring Internet penetration, such as PC base and ISP subscription, and payment methods, such as credit card holders, and transaction value.

Electronic commerce measurement is not very advanced in the U.S. either. Commerce Secretary Daley showed great interest in the topic in June 1999 when he said: "We were discussing ways to include e-commerce in government statistics. The fact is that people in the private sector are making billions of dollars in decisions about e-commerce -- without a reliable base of information" [Daley 1999a].[19]

It is clear that tracking Internet business, especially in a timely way, requires new economic measures and measurement techniques. The Economics and Statistics Administration and the Census Bureau and its Bureau of Economic Analysis are taking steps on this path. The Census Bureau, for example, plans to measure the dollar value of e-commerce sales for the next *Annual Survey of Retail Trade*.[20] Thus, some pieces of the measurement framework will be gradually put in place over the next few years as new data gathering instruments are implemented. At present, the numbers reported as indicators of a certain aspect of electronic commerce vary widely. The only common characteristic of all such observations is that they keep increasing over time.

GLOBAL PARTICIPATION, SEAMLESS GLOBAL MARKETPLACE

Kalin [Kalin 1999] presented a rather thorough analysis of the worldwide commercial use of the Internet. According to the International Telecommunications Union (ITU), more than one half of world households do not have a telephone, let alone a personal computer. The number of telephone lines per 100 inhabitants in Africa, for example, is only 2.15. Somalia has 0.15 lines

[19] In a foreword to the third annual report published in June 2000 [DOC 2000a], Secretary Daley suggests that "Hard questions of definition and measurement will still have to be resolved [...] before we can understand the full impact of these changes on our economy."

[20] In March 2000, the Census Bureau released the first official measure of an important subset of B2C electronic commerce, "e-tail." Online sales by retail establishments totaled $5.3 billion, or 0.64 percent of all retail sales [DOC 2000a].

per 100 people, Chad 0.12, and the Democratic Republic of Congo only 0.04. ITU estimates that only about 2.5 percent of the world population can access the Internet. The level of Internet access varies widely even within industrialized nations and depends on the cost, penetration of personal computers and infrastructure. Connectivity limitations around the world are certainly restraining global participation in a seamless global "marketspace."

Forrester Research found almost two thirds of the U.S. companies that have global presence had no plans to support languages other than English on their Web sites [Kalin 1999] and 85 percent of U.S. retailers surveyed could not ship products internationally [Cottrill 2000]. Organizational and content management problems thus represent a second obstacle for electronic commerce globalization. Kalin suggests that understanding country-to-country variability can help a business prioritize its efforts. *Forbes*' analysts gave similar advice regarding Internet investments in EU countries [Meland 1999]. In other words, the ideal of a seamless global marketspace just doesn't seem realistic, at least within the next 15 years or more.

Great Britain was ranked the highest among the EU member countries with an A-. Yet, Sprenger [July 20, 1999a] described the situation in Great Britain as troublesome. He quoted Thomas Power, chairman of the electronic commerce education forum The Ecademy as saying: "It's quite disappointing how ignorant both the government and the opposition are on the subject of e-commerce." Power criticizes the government for not seeing electronic commerce as a creator of wealth and jobs. Small start-up companies claim that their investments in electronic commerce threaten established large corporations. The general mood at a last year's meeting of British electronic commerce companies was described as a disgruntlement toward both traditional businesses and the government. If this is the state of the highest ranked EU country, one wonders how much worse the problems may be in lower ranked countries, not to even mention less developed environments.

The other obstacle to global electronic commerce is consumer protection-related jurisdiction. As Commerce Secretary Dailey stated: "These jurisdictional

issues are complicated -- just as they are for copyrights and a host of related issues. And they are complicated on an international basis, too. No doubt, this will take years to sort out and resolve. There is no silver bullet. But I think we have to come to a consensus on jurisdictional issues." [Daley 1999a]

Another dimension of seamless globalization is whether the Internet works as an equalizer and allows small enterprises to compete with the international giants or provides an accelerating advantage to a few big players. A study by two Xerox Corporation researchers offers statistical support to the notion that on the Internet the rich are getting richer. The top five percent of the sites in their sample received 75 percent of all Web traffic. This finding is consistent with the results of a similar study by a group of IBM's researchers from Almaden Research Center in San Jose, California. Both teams of researchers said that once a Web site catches on, its popularity tends to increase rapidly [Markoff June 21, 1999].

The finding of a growing gap between the richest and least-developed countries is also supported by the Human Development Report, the UN Development Program's annual global overview. The report recognizes that the global inequalities in income and living standards have reached "grotesque" proportions and that the Internet, rather than reducing the disparity, is increasing it [Longworth 1999]. The report also points out that inequalities in consumption are extreme. Globally, the 20% of the world’s people in the highest-income countries account for 86% of total private consumption expenditures—the poorest 20% only 1.3% [UN Development Program 1999].

SMALL AND MEDIUM SIZE BUSINESSES AND THE INTERNET

The U.S. Government Working Group on Electronic Commerce reported [WGEC 1998] that many small businesses do not take advantage of the opportunities that the Internet presents. These businesses lack an understanding of the Internet’s potential benefits, of how to develop electronic commerce profitably or how to cope with the complexity of rules affecting electronic commerce. In addition, many lack the technical personnel that could assist them

in implementing a business model for electronic commerce. To overcome these hurdles, the Secretary of Commerce and the Small Business Administration developed an electronic commerce small business strategy. The initiatives include training of government employees who have contacts with small businesses, moving government products and forms to the Internet to serve small businesses better, developing better measures of the economic impact, developing an outreach program jointly with the private sector to inform small businesses on how to profit from electronic commerce, highlighting successful cases, and establishing Internet-based program to match exporters with export finance providers and to allow instant exchange of relevant information.

To help small businesses market themselves internationally, the Department of Commerce has developed Virtual Trade Shows, or E-ExpoUSA. In January 2000, E-ExpoUSA featured 630 exhibitors from over 50 industry sectors [DOC 2000b]. The Small Business Administration (SBA) created a number of online services for small businesses including electronic commerce courses for its Small Business Classroom on the Web, an online resource for training and informing entrepreneurs [SBA 2000a]. The SBA has also developed several Internet based systems for providing information to small businesses. Some of them are the U.S. Business Advisor, built to provide businesses access to federal government information, services, and transactions [SBA 2000b]; PRO-NET, an electronic gateway of procurement information for and about small businesses [SBA 2000c]; *SCORE Online*, offering e-mail assistance and counseling help for small firms [SCORE 2000]; *Tech-Net*, providing technology information and resources for and about small high tech businesses [SBA 2000d]; ACE-Net, a link to potential SBA-sponsored investors [SBA 2000e]; and several others. Yet, the Yankee Group found that although 28 percent of companies with less than 20 employees and 54 percent of companies with between 20 and 99 employees have Internet presence, they use it primarily as online brochures. Only a small percentage (less than one-third of those with a Web site) is using Internet to sell products, provide customer support, or reduce operating costs [WGEC 1999].

A report by OECD's Working Party on Small and Medium-Sized Enterprises (SME), distributed just two months before the report by the U.S. Government Working Group, highlighted similar findings [OECD 1998b]. A survey of the member countries identified the following obstacles for SMEs to engage in electronic commerce:

- lack of awareness and understanding of electronic commerce by SMEs,
- lack of governments' understanding of electronic commerce for SMEs,
- business-friendly information is not being delivered,
- training and access to skills is not available,
- evaluation of effectiveness of policies for SMEs and electronic commerce has not been performed.

The report suggests that electronic commerce is still immature in terms of its diffusion into the economy and use as a tool for electronic transactions. The survey responses suggest that detailed studies of how and why electronic commerce is or is not implemented are lacking. The survey further shows a lack of understanding of key reasons for SMEs to implement electronic commerce and a lack of evaluation mechanisms. Furthermore, countries are at different levels of experience and focused on different aspects of electronic commerce.

Based on these findings, the Working Party recommended a number of policies including the international definition of electronic commerce, promotion of the awareness and understanding of electronic commerce for SMEs, delivering business-friendly information, and improving the knowledge of benefits, opportunities and barriers to electronic commerce for SMEs.

In summary, small businesses would likely be able to benefit from the implementation of electronic commerce to broaden their markets and lower transaction costs. Technology diffusion will not be rapid and easy, though. Small businesses are often lacking the expertise and technology, but some governments are organizing to provide training and assistance. Acceptance of electronic commerce by small businesses will likely be slow and uneven among countries, and will also depend on the industry and on company size.

VII. SUMMARY

The previous four sections of this report describe many details demonstrating the electronic commerce paradox presented in the Introduction. We are observing the rapid growth of electronic commerce and sweeping changes in our economic and social environments, but we also recognize that this network or digital economy is built on an unstable, unsettled foundation.

This foundation involves four themes discussed in Section II through VI:

- building trust for users and consumers,
- establishing ground rules for the digital marketplace,
- enhancing the information infrastructure, and
- maximizing benefits.

Each of these four themes contains a number of critical issues, none of which is fully resolved yet. Can they be resolved? and if so, how? and when?

BUILDING TRUST FOR USERS

Building trust for users and consumers involves:

- privacy protection,
- security,
- consumer protection,
- authentication and confidentiality, and
- access blocking.

Privacy protection is a highly controversial issue within the U.S. and internationally. The U.S. Department of Commerce and the EU are moving closer to an agreement on data privacy, but a few stumbling blocks remain. Negotiations involve a fundamental difference in perception of what the people in Europe and in U.S. find as acceptable. While the U.S. government supports industry self-regulation, the EU regulated the issue.[21] Some states in the U.S. and other countries are also not willing to wait. Various discoveries and announcements, such as those related to RealJukebox, IETF, and the Clinton

[21] This dispute was resolved in March 2000 [Smith 2000 and DOC 2000c].

Administration itself were strongly attacked by the privacy protection groups. On the other hand, industry self-regulation is slowly influencing corporate policies. Some major Web advertisers, including IBM and Microsoft, decided to abandon sites that do not post privacy policies.

Providing a secure environment for electronic commerce will likely be resolved technically in a matter of years to the point where most businesses would find security risks low and acceptable. Encryption technology is powerful and is now widely available, although several cases of flaws and successful breaking of RSA encryption have been reported. Storage and protection of private keys can perhaps be resolved by the use of hardware identification devices, smart cards with PINs or biometrics. The necessary public key infrastructure (PKI), however, will not be easily established, at least globally. It may take a few years to agree on it and put it into operation in the developed part of the world and much longer elsewhere. We should not expect a solution in the near future for secure global commerce between parties without pre-established relationships or contracts.

Protecting consumers is difficult because of the nature of the Internet. It will not be enough to act against fraudulent behavior in just one part of the world. Can a global community of nations agree on consistent measures and when? While the U.S. government supports industry self-regulation, the Canadian government did not want to wait and unveiled a set of guidelines for fair Internet business practices for Canadian businesses called Principles for Consumer Protection in Electronic Commerce. They cover consumer protection, dispute resolution, privacy and unsolicited email, and have a high moral force because of the broad range of organizations that helped draft them [Friedman Nov. 1999].

Public key encryption technology appeared only a few years ago as the final solution enabling authentication and confidentiality. Although emerging biometrics technology may be even more promising, both may require legal establishment of PKI or an equivalent structure in the case of biometrics. Although some predict that PKI will ultimately become a commodity item, this will

not happen soon. Gartner Group predicts that by the year 2003 up to 80% of large companies will have tested this complex technology [Levitt 1999].

Access blocking to protect Internet users, particularly children, from inappropriate content is also highly controversial. Free speech advocates argue against filtering requirements while concerned parents and some politicians want to protect the public from what they consider to be harmful content. Several domestic attempts to regulate this issue and enforce filtering Internet content were defeated in the courts. Internationally, some countries and regional governments regulate Internet access. However, the Internet may be too large, too decentralized and too dynamic for effective access blocking. In the U.S., the Commission on Child Online Protection is examining the issue.

THE DIGITAL MARKET

The ground rules for a digital marketplace include:

- a legal framework,
- acceptance of electronic transactions,
- taxation,
- tariffs,
- intellectual property,
- commercial policy, and
- payment systems.

A legal framework is far from established. In fact, we don't even know which of the possible alternatives should be pursued. The global reach of the Internet calls for an unprecedented universal international agreement. Even if such a global administrative agency could be established, three constitutional provisions of the U.S. prohibit the delegation of the legislative power to anyone outside the Congress unless there is a sufficient guarantee of accountability. Yet, once again, the EU is rushing ahead and is establishing legal guidelines for virtually every aspect of electronic services within the EU. This directive

establishes the principle of mutual recognition of the laws of other EU countries and may be a possible model for global Internet regulation.[22]

The Model Law on Electronic Commerce, developed by the United Nation's Commission on International Trade Law [UNCITRAL 1998], addresses electronic signatures and contracts. It is gradually gaining international acceptance. Several countries, including the U.S., the United Kingdom, Canada, and some others, either expressed their support for or introduced legislature compatible with the Model Law. Unfortunately, the EU's Electronic Signatures Directive, now in the final stages of consideration by the EU Parliament, follows a model involving a greater degree of government regulation. Under that model, a government creates a preference for one or more particular types of electronic authentication by establishing specific technical requirements for electronic signatures [Pincus 1999].

The collapse of the 3rd WTO Ministerial Conference in Seattle in 1999 may negatively impact international agreements on taxation and tariffs. Electronic commerce issues were supposed to receive serious attention and the Clinton Administration's agenda included extending the moratorium on Internet tariffs and ensuring that existing trade rules remain in effect in the era of online commerce [Murphy Dec. 1, 1999]. In the U.S., Congress passed a three-year moratorium on Internet taxation in October 1998 and established an advisory commission, which plans to report to Congress by April 2000.[23] Members of this commission are in disagreement since state and local governments fear losing a substantial portion of their income.

Developing countries will be importing much more of the digital content than they will be exporting. Not collecting tariffs would result in a net loss of

---

[22] At its plenary session on May 4, 2000 in Brussels, the European Parliament threw its weight behind the Council of Ministers' common position on the proposal for a Directive on certain legal aspects of electronic commerce in the internal market. Pursuant to the co-decision procedure, the Directive is considered as definitively approved, since the Parliament introduced no amendment. The Member States now have 18 months to transpose the new provision into their national law [Anonymous May 2000].

[23] The Advisory Commission on Electronic Commerce submitted the 140-page report to Republican congressional leaders on April 12, 2000. The future of Internet taxation is now in the

income and they will likely try to implement customs duty on electronic transfer of digital content. Even Europe is not ready to permanently ban tariffs on electronic commerce.

Intellectual property issues concern patents, trademarks, trade secrets and copyrights. The World Intellectual Property Organization (WIPO) adjusted the intellectual property protection to the digital age with two treaties in December 1996. President Clinton signed into law the Digital Millenium Copyright Act in the fall of 1998. This Act implements the WIPO treaties, but critical legal questions still plague intellectual property owners and online users. The 1998 ruling by the Federal Circuit U.S. Court of Appeals, which ruled that companies could patent business methods, is highly controversial and triggered a number of lawsuits. The recording and distribution industries are looking for ways to protect digital content from illegal copying in a rather disorganized way, since they are threatened by technologies such as MP3, Napster and Gnutella.

The disputes on commercial policy are also not yet resolved. While many WTO members consider all electronic deliveries, including those comprising digital content, to be services, the U.S. and to a certain extent Japan argue that the deliveries are indeed services, but that digital products themselves are goods falling under GATT agreement rather than GATS. The issue is still being discussed within the WTO.

Although the need for micropayment technologies appears real, the popularity of conventional payment devices such as credit cards, particularly in the U.S., prevents the implementation of innovative payment systems. This situation may change if the reports about credit card-related fraud and security breaches keep scaring consumers and even more so the merchants. The problem with credit card fraud is particularly threatening in cases of international commerce.

---

hands of Congress. Key issues that polarized commission members now shift to an even more politically charged setting [McGregor 2000].

INFRASTRUCTURE

The needed enhancements of the information infrastructure include:

- Internet infrastructure and governance,
- interconnectivity and technical convergence,
- technical standards,
- bandwidth and accessibility, and
- furthering competition.

Internet limitations, such as inadequate point-to-point throughput, scarcity of IP addresses, and a rather primitive protocol are generally recognized. Several projects in the U.S., such as the very High performance Backbone Network Service, the Next Generation Internet and Internet2, and similar developments in Canada and Scandinavia, promise to significantly increase the speed of the backbone and implement IPv6, Quality of Service, and multicasting, within the foreseeable future. The penetration of Digital Subscriber Line (DSL) technology, Internet service over cable TV and anticipated speed increase of wireless Internet access promise to resolve the "last kilometer" bottleneck in about the same time frame. If all evolves as expected, the issue of infrastructure development may be discarded from the list of electronic commerce obstacles in a few years, but the migration to the IPv6 will probably take much longer.

Significant progress has been made in transitioning Internet governance from U.S. Government control to the private sector. Although the Internet Corporation for Assigned Names and Numbers (ICANN) is not fully staffed yet by elected board members, the monopoly of Network Solutions, Inc. in assigning the domain names was broken. Network Solutions recognized ICANN as the body overseeing the domain name registration. Critics such as Iperdome, Inc. [Fenello 1998] and a group representing small businesses argue that ICANN's policies circumvent the need for the bottom-up, consensus-building tradition in Internet governance and favor large corporate trademark holders.

Interconnectivity, often taken for granted, is not guaranteed or resolved in all cases. For example, will cable systems owned by AT&T and the proposed AOL Time Warner become open to competitive content providers? If this question is unresolved in the U.S., much more intense and lasting effort will be needed to open the access and provide interconnectivity worldwide.

Some observers [Caron 1999] argue that Internet technical standards setting by the IETF is burdened by the extensive financial implications on vendors and business users. The problem is illustrated by two major technology providers, Nortel and Cisco, who have different views on how to implement multi-protocol label switching. The developments of other technologies, such as messaging services, a standard between computer companies and consumer electronics manufacturers, and wireless Internet access also remain unresolved.

Nortel's claim of a transfer rate of 6.4 terabit per second over a single optical fiber, and Lucent Technologies announcement that its new switching technology using microscopic mirrors can switch 10 tmes the amount of data carried by the entire Internet suggest that backbone throughput is a short-term concern. However, these developments do not ensure adequate global bandwidth and access. The reported digital divide in the U.S. speaks for itself, but an even wider divide exists internationally. It may be imposed by restrictive governments or be a consequence of inadequate telecommunication infrastructure. A French media organization [Reporters Sans Frontières 1999] reported that 28 percent of the world population does not have unrestricted access to the Internet due to governmental interventions.

Furthering competition is primarily about the global opening of telecommunications markets to foreign competition. The WTO Telecommunications Services Agreement in 1998 forced 70 countries to begin implementing commitments to provide market access and regulations supporting competition [Bhatnagar 1999]. The monopoly in basic telecommunication services, however, still persist in over two thirds of the world's countries. Interconnectivity and privatization are difficult hurdles to overcome and may require adjustments in national economies, political systems, legal frameworks

and the availability of related and scarce expertise. Once again, this transition will be accomplished in a few years in the developed part of the world and will take much longer elsewhere.

MAXIMIZING BENEFITS OF ELECTRONIC COMMERCE

The benefits of electronic commerce require understanding of the digital economy, its measurement, seamless globalization and involvement of small businesses. Many social and economic implications of electronic commerce are not well understood. Some concerns that we are able to recognize include:

- new channels of knowledge diffusion,
- creation of new relationships among businesses and between businesses and consumers,
- dis-intermediation and new intermediation,
- requirement for a higher-skilled workforce,
- need for reformed regulations, and
- erosion of geographical boundaries.

We are becoming aware of such issues but not necessarily of their social and economic impact. Several governmental and international initiatives to research the implications and increase our understanding are underway.

Commerce Secretary Daley said in June 1999 [Daley 1999a] that the private sector is making billions of dollars worth of decisions about electronic commerce without a reliable base of information. Clear tracking requires new economic measures and techniques, which will be gradually put in place over the next few years. The issue is again complicated because consistent and simple measures need to be implemented globally. In addition to measuring the business-to-business and business-to-consumer deliveries, a much more difficult measurements of business-to-business cooperation in product design and development is also needed.

According to several reports [Kalin 1999, Cottrill 2000, Markoff June 21, 1999, Longworth 1999], the global participation and seamless global electronic marketplace will remain elusive. The first obstacle is the telecommunications

infrastructure. Over one half of world households do not have telephones. If the "Internet in the sky" cannot deliver an affordable opportunity to leapfrog the connectivity constraint to underdeveloped countries, this issue will not be resolved for many years. Other obstacles are the predominance of English on the Internet, lack of government support, and unsettled international legislation on consumer-protection, to name a few. Making matters worse, the rich appear to be getting richer on the Internet and the disparity between the rich and the poor parts of the world is increasing.

Electronic commerce provides an interesting opportunity to small and medium size businesses, but many are not able to take advantage of it. They may lack the understanding of complex market space or may lack technical expertise. This issue is being addressed by different governmental initiatives in the U.S. Researchers at the OECD's Working Party on Small and Medium Enterprises (SME) came to similar conclusions [OECD 1998b]. They observed a lack of awareness and understanding; a lack of governments' understanding of electronic commerce for SME; a lack of business-friendly information, training and access to skills; and deficiency of evaluations of SME policies on electronic commerce. Based on these findings, a number of recommendations have been proposed. Technology diffusion will be slow and uneven both geographically and among industries.

V. CONCLUSIONS

All 22 issues described in Table 1 (Section II) that are critical for seamless global electronic commerce, remained unresolved in February 2000, the time this article was prepared. The issues can be aggregated into several big questions defining the future of Internet-based electronic commerce.

1. *Will the world community be able to define and agree on the rules governing cyberspace?*

Such rules have to include jurisdiction, commercial practices involving tariffs, consumer protection and many other issues, standardization, open access etc. The answer at this time has to be "no" and the discussion in this article

provides ample support for this lack of optimism. We conjecture that some countries will, for a variety of reasons, not catch the ride and suffer substantial and lasting economic consequences. Shushil Baguant, Mauritius' chairman of National Computer Board, shares this concern [Leopold 2000]: "If you don't do the right thing and address it at this moment, you are going to accentuate the gap."

The United Nations is finally recognizing the importance of this issue. Secretary-General Kofi Annan set up a panel on electronic commerce as part of his preparation for a Millennium summit in September 2000, at which time he proposed that the United Nations take a lead in transferring information technologies to poor nations. The panel suggested at its initial news conference that the world body had not taken the leadership among its members and that it needs a major initiative, such as those on AIDS or sustainable development [Leopold 2000].

Reports of Internet vulnerability, such as massive denial-of-service attacks, misuse of medical records, posting of thousands stolen credit card numbers, and consumer profiling, lead to the question:

2. Will consumer trust in the Internet as a valid business environment be gradually lost?

The U.S. government is serious in its attempts to prevent the loss of consumer trust. However, it is reasonable to at least speculate that the way the Internet was designed, its openness and accessibility make it impossible to control. We read that fraud on the Internet is increasing and so are security breaches, delayed shipments, cases of compromised privacy, and number of hacked sites.

3. Should governments regulate electronic commerce, or will its commercial users be able to agree and self-regulate?

The U.S. Government's argument is that electronic commerce is in its early stage of evolution, is not well defined yet, and should not be regulated because regulation may stifle its full expansion. Some consumer groups counter that the government should protect people against fraud and loss of privacy, for

example, and are urging it to regulate the Internet. A balanced approach to regulation may gain majority support within a country, but we question whether regulation of electronic commerce can be established internationally, at least in the near future.

The paradox is, indeed, obvious. While electronic commerce is experiencing “explosive” growth, the environment is not quite ready to support it. However, the factors driving electronic commerce are strong and cannot be ignored. Electronic commerce offers opportunities to expand markets, speed up business cycles, decrease the costs of doing business, expand the line of products and services, and improve convenience and the number of choices. We know that electronic commerce works; just look at Cisco, Dell, eBay, E*TRADE, and other successful pioneers.

Are we observing a powerful landslide, which easily overcomes the obstacles described in this paper? The "Internet Economy" has grown more rapidly than anyone could have envisioned, opening up new vistas of communication, collaboration and coordination between consumers, businesses and trading partners [Internet Indicators 2000]. One group of media reports therefore suggests that the world is wired and all we need now do is click, sell, shop and eliminate virtually all inventory and friction along the supply chains. Another set of reports, however, contains occasional warnings. As the analysis in this article suggests, many serious issues are unresolved, and as stated at the end of the Introduction: "A corrective is, we feel, needed, to focus attention on what still needs to be done before the dreams of global electronic commerce can be realized. Thus the tone of warning, of caution. We have far to go, many obstacles to overcome, and tough work ahead."

Editor’s Note: This article was received on February 23, 2000. It was with the author approximately five weeks for two revisions. It was published on June 28, 2000

REFERENCES

EDITOR’S NOTE: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word

processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.
2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.
4. the author(s) of this article, not CAIS, is (are) responsible for the accuracy of the URL and version information.

Advisory Commission on Electronic Commerce (1999) "First Meeting of the E-Commerce Commission," Press Kit, online: www.ecommercecommission.org/packet.htm, retrieved June 25, 1999.

Anders, G. (1999) "eBay to Refund Millions in Listing Fees As Outage Halts Bids for About 22 Hours," *WSJ Interactive Edition*, June 14.

Andrews, E. L. (1999) "As Europe Zooms Ahead, U.S. Fiddles With Formats," *The New York Times*, July 27, pp. C1, C8; online: www.nytimes.com/library/tech/99/07/biztech/articles/27euro.html, retrieved July 27, 1999.

Andrews, W. (2000) "RealNames Says Hacker May Have Stolen Credit Card Data," *Internet World News*, Feb. 11.

Angwin, J. (2000) "America Online Submits Plan Allowing Rivals Open Access to Instant Messaging," *WSJ Interactive Edition*, June 16.

Anonymous (1998a) Cover page, *Fortune*, (138)11 (Dec. 7, 1998).

Anonymous (June 1999) "Report Quantifies Economic Impact Of U.S. Internet-Related Companies," *WSJ Interactive Edition*, June 10.

Anonymous (Dec. 2, 1999) "Federal Judge Grants Injunction Against Barnesandnoble.com," *WSJ Interactive Edition*.

Associated Press (July 13, 1999) "Congress hears encryption debate," *USA Today*, Tech Report, online: www.usatoday.com/life/cyber/tech/ctf588.htm, retrieved May 28, 2000.

Associated Press (Aug. 6, 1999) "Hacker vandalizes security-related site," *Chicago Tribune*, sctn. 3, pp. 2.

Associated Press (Jan. 17, 2000) "Net conference focuses on privacy," *USA Today*, online: www.usatoday.com/life/cyber/tech/cth162.htm, retrieved Jan. 28, 2000.

Baker, S. and Yeo, M. (1999) "Survey of International Electronic and Digital Signature Initiatives," online: www.ilpf.org/digsig/survey.htm, version Apr. 14, 1999, retrieved May 26, 1999.

BBB (1999) "Better Business Bureau System Posts Draft of New Code of Online Business practices and Solicits Public Comment," online: www.bbb.org/alerts/newcodepr.html, Nov. 22, 1999, retrieved Dec. 7, 1999.

Bedell D. (2000) "Online Copyright Crisis Moves Beyond Music," *The Dallas Morning News* , June 22, 2000.

Bhatnagar, P. (1999) "Telecom Reforms in Developing Countries and the Outlook for Electronic Commerce," *Journal of World Trade*, (33)4, Aug. 1999, pp. 143-158.

Brostoff, S. (2000) "Congress revisits GLB privacy provisions," *National Underwriter*, (104)13, page 38.

Brown, J. (1998) "Heat Turned Up on Digital Music Pirates," *WiredNews* , online: www.wired.com/news/news/culture/story/10234.html, Feb. 12, 1998, retrieved June 7, 1999.

Caron, J. (1999) "On Top Of Technology," Telecom99 News Service, online: www.telecom99news.itu.int/story/DCM19990930S0014, retrieved Nov. 4, 1999.

Caruso, D. (1999) "Digital Commerce," *The New York Times*, Nov. 8, 1999, p. C4.

Caswell, S. (1999) "E-tail Failures Could Trigger Federal Legal Action," *E-Commerce Times*, online: www.ecommercetimes.com/news/articles/991229-1.shtml, Dec. 29, 1999, retrieved Jan. 28, 2000.

Chen, K. (1999) "FCC Chairman Calls for National Policy On High-Speed Internet Access Via Cable," *WSJ Interactive Edition*, June 16, 1999.

Chicago Tribune (Aug. 28, 1999) "Researchers say they cracked Internet's global security system," *Chicago Tribune*, sctn. 1, pp. 9.

Clarke, R. (1999) "Might Slow Adaptation of the Law Impede E-Commerce?" Online: www.anu.edu.au/people/Roger.Clarke/EC/BCA99.html, version Mar. 8, 1999, retrieved May 26, 1999.

Clausing, J. (June 1, 1999) "Unclear Future for Trans-Atlantic E-Commerce," *The New York Times on the Web*, online: www.nytimes.com/library/tech/99/mo/cyber/articles/01capital.html, retrieved June 1, 1999.

Clausing, J. (June 7, 1999) "Casting Too Wide a Net?" *The New York Times*, pp. C1, C2.

Clausing, J. (July 1999) "U.S. Moves to Tighten Reins On New Internet Regulator," *The New York Times on the Web*, July 10.

Clausing, J. (Nov. 1, 1999) "Signatures on Cyberspace's Dotted Line," *The New York Times*, pp. C2.

Clausing, J. (Nov. 5, 1999) "Internet Group Approves Domain Registration Rules," *The New York Times*, p. C2.

Clausing, J. (Nov. 22, 1999) "Internet Makes an Easy Target For Lobbyists and Lawmakers," *The New York Times*, pp. C1, C5.

Clausing, J. (Dec. 1999) "New Committee to Address privacy and Security Online," *The New York Times on the Web*, Dec. 28.

Clinton, W. J. (1997) "Electronic Commerce," The White House, Office of the Press Secretary, online: www.fas.org/irp/offdocs/pdd-nec-ec.htm, posted July 1, 1997, retrieved July 1, 1999.

Clinton, W. J. and Gore, A. Jr. (1997) "A Framework For Global Electronic Commerce," online: www.iitf.nist.gov/eleccomm/ecomm.htm, retrieved June 1, 1999.

CNNFN (1999) "Wyden, Cox Push For Ban ON Internet Tariffs," interview, online: cnnfn.com/news/technology/newsbytes/137097.html, retrieved Sep. 30, 1999.

Coalition of Service Industries Electronic Commerce, Information Technology & Telecommunications Working Group (1999) "Recommendations on Electronic Commerce," online: www.ftc.gov/bcp/icpw/comments/csi.htm, retrieved July 2, 1999.

Collett, S. (1999) "Lucas Empire Strikes First," *Computerworld*, pp. 16. Also online: www.computerworld.com/home/print.nsf/all/990510A51E, May 10, 1999, retrieved June 7, 1999.

Computer & Online Industry Litigation Reporter (Apr. 2000) "Judge Strikes Down Washington State Anti-Spam Law," *Computer & Online Industry Litigation Reporter*, (17)13, Apr. 10., p. 14.

Cottrill, K. (2000) "Global Limits," *Traffic World*, 261(4837), Jan. 10, 2000, online: www.trafficworld.com/reg/news/logistics/l011000.html, retrieved June 7, 2000.

Culnan, M. J. (1999) "Georgetown Internet Privacy Policy Survey," online: www.msb.edu/faculty/culnanm/gippshome.html, May 17, 1999, retrieved June 1, 1999.

Curran, J. (2000) "New Jersey senator pitches Internet privacy legislation," *The Associated Press State & Local Wire*, Mar. 10, 2000.

Daguio, K. (1999) "Mr. Kawika Daguio on Regulation," excerpt from a video clip, online: www.ecomm.dal.ca/mpg/regulatr.html, Mar. 18, 1999, retrieved June 14, 1999.

Daley, W.M. (1999a) "Remarks at the Industrial Sector Advisory Committees Opening Plenary Session," Washington, DC, online: 204.193.246.62/public.nsf/docs/990616-committees-opening-plenary-session-dc, June 16, 1999, retrieved June 22, 1999.

Daley, W. M. (1999b), foreword in Henry, D. *et al*. "The Emerging Digital Economy II," U.S. Department of Commerce, online: www.ecommerce.gov/ede/ede2.pdf, retrieved June 24, 1999.

De Bony, E. (2000) "EU Approves E-Commerce Legislation," *The Standard*, online: www.thestandard.com/article/display/1,1151,14788,00.html, May 4, retrieved June 22, 2000.

De Long, J.B. (1999) "Analytic Overview at the Conference of the University of California E-conomy™ Project," Washington, D.C., online: e-conomy.berkeley.edu/events/deip/summary.html, May 27, 1999, retrieved June 7, 2000.

Dennis, S. (1999) "Online Security Still A Mystery - British Telecom," *Newsbytes*, online: www.newsbytes.com/pubNews/99/141338.html, Dec. 29, 1999, retrieved Jan. 3, 2000.

Ditchburn, J. (1999) "Canadian Furor Over Net Filters," *WiredNews*, online: www.wired.com/news/news/politics/story/20391.html, June 24, 1999, retrieved July 1, 1999.

DOC (2000a) "Digital Economy 2000," U.S. Department of Commerce, online: www.ecommerce.gov/de2000.pdf, June 2000, retrieved June 6, 2000.

DOC (2000b) "E-ExpoUSA," online: e-expousa.doc.gov/ExpoWeb2.nsf/pages/PressFrameset, retrieved June 15, 2000.

DOC (2000c) "EU-U.S. Summit Statement on Data Privacy," May 31, 2000, online: www.ecommerce.gov/ecomnews/doc060200.html, retrieved June 23, 2000.

Dougherty, C. (1999) "A Taxing Dilemma for the EU," *WiredNews*, online: www.wired.com/news/business/0,1367,32217,00.html, Nov. 1, 1999, retrieved Nov. 1, 1999.

Dun & Bradstreet (1999) "VeriSign and eccelerate.com, a Dun & Bradstreet Company, To Enable Trusted Online Business-to-Business Transactions," press release, Nov. 2, 1999, online: www.dnb.com/newsview/1199news2.htm, retrieved Jan. 28, 2000.

Echikson, W. (2000) "This Tax Could Tangle the Global Net," *Business Week*, 3687, June 26, 2000, p. 194, online: www.businessweek.com/2000/00_26/b3687148.htm, retrieved June 22, 2000.

Economist (Dec. 18, 1999) "Living in the Global Goldfish Bowl," *The Economist*, (353)8150, p. 49.

Eisenberg, A. (1999) "Copyright, legal issues in stars for celestial jukebox," *Chicago Tribune*, Dec. 27, 1999, section 4, p. 6.

Elmer, S. (1999) "Electronic Commerce - IDC Definitions & Methodologies," OECD Workshop on Defining and Measuring Electronic Commerce, Paris, online: www.oecd.org//dsti/sti/it/ec/pdf/Elmer.pdf, Apr. 21, 1999, retrieved Aug. 19, 1999.

eMarketer (Mar. 1999) "Kicking the Line," *eMarketer*, online: www.emarketer.com/enews/030899_theline.html, retrieved Nov. 12, 1999.

EU: Directorate General I (1999) "Digital Products: The Case for Services," online: europa.eu.int/comm/dg01/ecom6.htm, Mar. 26, 1999, retrieved Aug. 6, 1999.

European Report (May 2000) "Information Society: MEPS Approve Directive on Electronic Commerce,", May 10.

Federal Register (May 6, 1998) "Interpretation of Rules and Guides for Electronic Media; Request for Comment," *Federal Register*, (63)87, also online: www.ftc.gov/os/1998/9805/63fr24996.pdf, retrieved July 6, 1999.

Ferranti, M. (1998) "WTO reaches no-tariff pact on Internet transmissions," *InfoWorld.com*, online: www.infoworld.com/cgi-bin/displayStory.pl?980521.wiwto.htm, May 21, 1998, retrieved Aug. 4, 1999.

Fenello, J. (1998) "Testimony before the Committee on Commerce," online: www.iperdome.com/responses/testimony.htm, June 10, 1998, retrieved June 17, 2000.

Friedman, M. (Oct. 1999) "Canada House OKs Privacy," *WiredNews*, online: www.wired.com/news/politics/0,1283,32120,00.html, retrieved Oct. 28, 1999.

Friedman, M. (Nov. 1999) "Canada's E-Commerce Edge," *WiredNews*, online: www.wired.com/news/print/0,1294,32447,00.html, retrieved Nov. 11, 1999.

Friedman, M. (Dec. 1999) "Making E-Contracts Count," *WiredNews*, online: www.wired.com/news/politics/0,1283,33149,00.html, retrieved June 20, 2000.

Fry, J. and Doscher, M. (1999) "Just Like That, the War's Over On the Encryption Battlefield," *WSJ Interactive Edition*, Sep. 17, 1999.

FTC (1996) *Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace,* Bureau of Consumer Protection, pp. iii.

FTC (1998) "Online Privacy," online: www.ftc.gov/reports/privacy3, version June 9, 1998, retrieved June 1, 1999.

FTC (1999) "FTC Staff Releases Results of International Web Survey," online: www.ftc.gov/opa/1999/9906/interweb.htm, June 8, 1999, retrieved June 22, 1999.

FTC (2000) "New Rule to Protect Children's Online Privacy Takes Effect April 21, 2000," online: www.ftc.gov/opa/2000/04/coppa1.htm, Apr. 20, 2000, retrieved May 28, 2000.

GBDe (1999) "Unprecedented Global Business Dialogue launched to establish framework for e-commerce," online: www.gbde.org/library/press1.htm, retrieved Aug. 5, 1999.

Greenberg, P. A. and Caswell, S. (2000) "Online Banking Fraud Raises More Security Concerns," *E-Commerce Times*, online: www.ecommercetimes.com/news/articles2000/000201-2.shtml, Feb. 1, 2000, retrieved Feb. 5, 2000.

Gruley, B. (1999) "FCC Asks Court to Stop Portland, Ore., From Making AT&T Open Cable Lines," *WSJ Interactive Edition*, Aug. 16, 1999.

Hamilton, D. P. (2000) "Redesigning the Internet: Can it Be Made Less Vulnerable?" *The Wall Street Journal*, Feb. 11, p. B1.

Harrington (1998) Prepared Statement of the Federal Trade Commission on "Consumer Protection in Cyberspace: Combating Fraud on the Internet," before the Telecommunications, Trade, and Consumer Protection Subcommittee of the House Committee on Commerce, U.S. House of Representatives, online: www.ftc.gov/os/1998/9806/test.623.htm, June 25, 1998, retrieved June 15, 1999.

Hershman, T. (1999) "Toward a Click-and-Pay Standard," *WiredNews*, online: www.wired.com/news/technology/0,1282,32092,00.html, Nov. 3, 1999, retrieved Feb. 18, 2000.

Human Rights Watch (1999) "The Internet in the Mideast and North Africa: Free Expression and Censorship," online: www.hrw.org/advocacy/internet/mena/summary.htm, June 8, 1999, retrieved June 8, 1999.

ICANN (2000) "Call for Recommendations and Expressions of Interest," ICANN Nominating Committee, online: www.icann.org/nomcom/call.htm, May 22, 2000, retrieved June 4, 2000.

ICC (1998) "The ICC Electronic Commerce Project (ECP)," online: www.iccwbo.org/home/electronic_commerce/electronic_commerce_project.asp, retrieved June 13, 2000.

IFEA (1998) "Joint Statement for the Record on 'Kids and the Internet: The Promise and the Perils'," online: www.eff.org/pub/Censorship/Academic_edu/Library_filtering/HTML/19981214_ifea_nclis_statement.html, Dec. 14, 1998, retrieved June 29, 1999.

IFEA (1999) "Letter to Senate Commerce Committee Concerning the Children's Internet Protection Act (S.97)," online: www.ifea.net/s97_letter.html, June 23, 1999, retrieved July 1, 1999.

Internet Indicators (2000) "The Internet Economy Indicators," *Indicators Report*, online: www.internetindicators.com/, June 15, retrieved June 19, 2000.

Jacobus, P. (2000) "Clinton wants $50 million to close digital divide," CNET News.com, online: news.cnet.com/news/0-1005-200-1540155.html, Feb. 2, 2000, retrieved Feb. 5, 2000.

Kalin, S. (1998) "Reading Between The Lines," *CIO Web Business Magazine*, online: www.cio.com/archive/webbusiness/040198_money.html, Apr. 1, 1998, retrieved June 11, 1999.

Kalin, S. (1999) "The Worldlier Wider Web," *CIO Web Business Magazine*, online: www.cio.com/archive/webbusiness/030199_axes.html, Mar. 1, 1999, retrieved June 11, 1999.

Kaplan D. (1999) "The 'Lorentz' EC Task Force and the Measurement of Electronic Commerce," OECD Workshop on Defining and Measuring Electronic Commerce, Paris, online: www.oecd.org//dsti/sti/it/ec/pdf/kaplan.pdf, Apr. 21, 1999, retrieved Aug. 19, 1999.

Keto, A. (1999) "Clinton Announces Electronic Medical Record Privacy Rules," *Dow Jones Newswires*, Oct. 29, 1999.

Kling, R. (1996) "Hopes and Horrors: Technological Utopianism and Anti-Utopianism in Narratives of Computerization," in *Computerization and Controversy: Value Conflicts and Social Choices*, (2nd Ed.) San Diego: Academic Press, online: www.slis.indiana.edu/kling/cc/2-HOPE4.html, retrieved April 4, 2000.

Kong, D. (1999) "Privacy policies may offer few protections, experts say," *Chicago Tribune*, July 19, 1999, section 4, pp. 6.

Larsen, A. K. (1999) "Virtual Cash Gets Real," *InformationWeek Online*, online: www.informationweek.com/736/cash.htm, May 31, 1999, retrieved June 24, 1999.

Leibovich, M., Smart, T. and Dugan, I.J. (1999) "Internet's E-conomy Gets Real," *The Washington Post*, p. A1; online: www.washingtonpost.com/wp-srv/business/daily/june99/internet20.htm, June 20, 1999, retrieved June 22, 1999.

Leopold E. (2000) "Experts Tell UN It Doesn't Understand Internet Age," *Yahoo!.news* , online: dailynews.yahoo.com/htx/nm/20000420/tc/internet_un_1.html, April 20, 2000, retrieved April 24, 2000.

Levitt, J. (1999) "In Keys We Trust," *InformationWeek*, pp. 75-86. Also online: www.informationweek.com/738/pki.htm, June 14, 1999, retrieved June 16, 1999.

Loftus, P. (1999) "Network Solutions Reaches Settlement on Domain Names," *The Wall Street Journal Interactive Edition*, online: interactive.wsj.com/articles/SB938532200438475792.htm, Sep. 28, 1999, retrieved Sep. 29, 1999.

Longworth, R. C. (1999) "A 'grotesque' gap," *Chicago Tribune*, July 12, 1999, pp. 1, 8.

Luh, J.C. (1999) "Real Apologizes, Promises Patch To Thwart Jukebox Spying," *Internet World News* , Nov. 1, 1999.

MacMillan, R. (1999) "Commerce Dept. Offers EU Privacy Directive Help," *Newsbytes*, online: www.cnnfn.com/digitaljam/newsbytes/129481.html, Apr. 1, 1999, retrieved June 1, 1999.

Markoff, J. (June 14, 1999) "Illness Becomes Apt Metaphor For Computers," *The New York Times*, pp. A1, A18.

Markoff, J. (June 21, 1999) "Not a Great Equalizer After All? On the Web, as Elsewhere, Popularity Is Self-Reinforcing," *The New York Times*, pp. C4.

Markoff, J. (July 28, 1999) "U.S. Drawing Plan that will Monitor Computer Systems," *The New York Times*, pp. A1, A16.

Markoff, J. (2000) "An Online Extortion Plot Results In Release of Credit Card Data," *The New York Times*, Jan. 10, pp. A1, A16.

Markoff, J. and Robinson, S. (1999) "Security Flaws In Software Are Reported," *The New York Times*, July 31, 1999, pp. B1, B14.

McCullagh, D. (Mar. 1999) "Counties Demand Net Taxes," *WiredNews*, online: http://www.wired.com/news/news/politics/story/18203.html, retrieved June 25, 1999.

McCullagh, D. (June 1999) "Liddy: Put a Lid on Libraries," *WiredNews*, online: www.wired.com/news/news/politics/story/20464.html, retrieved June 29, 1999.

McCullagh, D. (July 1999) "Feds Tackle Online Privacy," *WiredNews*, online: www.wired.com/news/news/politics/story/20832.html, retrieved July 21, 1999.

McCullagh, D. (Nov. 1999) "COPA Goes Before the Bench," *WiredNews*, online: www.wired.com/news/politics/0,1283,32313,00.html, retrieved Feb. 15, 2000.

McCullagh, D. (Dec. 1999) "Defending Privacy Snooping," *WiredNews*, online: www.wired.com/news/politics/0,1283,32826,00.html, retrieved Dec. 2, 1999.

McCullagh, D. (Jan. 2000) "Wiretapping Unwarranted?" *WiredNews*, online: www.wired.com/news/politics/0,1283,33810,00.html, retrieved Jan. 28, 1999.

McCullagh, D. (Feb. 1, 2000) "Cyber Safe or Gov't Surveillance?" *WiredNews*, online: www.wired.com/news/politics/0,1283,34027,00.html, retrieved Feb. 5, 2000.

McCullagh, D. (Feb. 3, 2000) "Thumbs Down on Net Wiretaps," *WiredNews*, online: www.wired.com/news/politics/0,1283,34055,00.html, retrieved May 23, 2000.

McGregor, M. (2000) "Virginia Governor Submits Report on Internet Taxation," *Richmond Times*, April 13.

Meland, M. (1999) "Europe: The next frontier: How does Europe stack up on the Internet? A country by country ranking," *Forbes DigitalTool*, online: www.forbes.com/tool/html/99/mar/0329/feat.htm, Apr. 2, 1999, retrieved Apr. 12, 1999.

Mitchener, B. (July 1999) "EU Commission Is Criticized On Electronic-Commerce Law," *WSJ Interactive Edition*, July 15, 1999.

Mitchener, B. (Dec. 1999) "EU Economic Ministers Approve Draft Law to Ease E-Commerce," *WSJ Interactive Edition*, online: interactive.wsj.com/articles/SB944592061873399168.htm, retrieved Dec. 8, 1999.

Morgan, C. (Mar. 8, 1999a) "Web Merchants Stung by Fraud," *Computerworld*, online: www.computerworld.com/home/print.nsf/all/9903089532, retrieved May 25, 1999.

Morgan, C. (Mar. 8, 1999b) "Protecting Your Web Site Against Credit-Card Fraud," *Computerworld*, online: www.computerworld.com/home/print.nsf/all/99030894B2, retrieved May 25, 1999.

Morgan, J. P. and Gidari, A. (1999) "Survey of State Electronic & Digital Signature Legislative Initiatives," online: www.ilpf.org/digsig/digrep.htm, Apr. 29, 1999, retrieved May 26, 1999.

Morrissey, C. M. (1999) "The Child Online Protection Act: Decency and the Internet Revisited," Law Library Resource Xchange, LLC. Online: www.llrx.com/congress/011599.htm, Feb. 15, 1999, retrieved June 29, 1999.

Murphy, K. (Oct. 13, 1999) "ISPs Say Baby Bells Act Anti-Competitively," *Internet World News*.

Murphy, K. (Oct. 14, 1999) "Priceline Suit Could Be First of Many Patent Fights," *Internet World News*.

Murphy, K. (Oct. 19, 1999) "New Bill Would Make FCC Into Spam Cop," *Internet World News*.

Murphy, K. (Oct. 20, 1999) "FTC Tells Sites How To Handle Kids' Data," *Internet World News*.

Murphy, K. (Nov. 1999) "Cybersquatting Bill Expected To Become Law," *Internet World News*.

Murphy, K. (Dec. 1, 1999) "U.S. Focuses on E-Commerce in Trade Talks," *Internet World News*.

Murphy, K. (Dec. 27, 1999) "$4B Sought from Yahoo for Not Sharing Customer Data," *Internet World News*.

Murphy, K. (May 2000) "House Approves 5-Year Ban on Net Taxes," *Internet World News*, May 10, 2000.

Murphy, K. (June 2000) "Commerce Committee Approves Antispam Measures," *Internet World News* , June 14, 2000.

Nando.net, online (May 18, 1998) "Pact on duty-free electronic commerce still elusive," www.techserver.com/newsroom/ntn/info/051898/info1_26697_noframes.html, retrieved August 5, 1999.

Nash, K. S. and Harrison, A. (1999) "Feds Make Bust in $45M Net Scam," *Computerworld*, May 10, 1999, pp. 1, 16, online: www.computerworld.com/home/print.nsf/all/990510A51A, retrieved May 25, 1999.

National Coordination Office for Computing, Information, and Communications (1998) "NGI Implementation Plan," online: www.ccic.gov/ngi/implementation/, Feb. 1998, retrieved Aug. 18, 1999.

National Infrastructure Protection Center (1999) "Frequently Asked Questions," online: www.fbi.gov/nipc/nipcfaq.htm, retrieved June 17, 1999.

New York Times (Oct. 1999) "Internet Plan Spurs Privacy Fear," *The New York Times on the Web*. Oct. 12.

Nortel Networks (1999) "Nortel Networks Breaks Own 'Land Speed Record' using Light -- Redefines Speed of Internet & Networking," News Release, online: www.nortelnetworks.com/corporate/news/newsreleases/, retrieved Oct. 20, 1999.

NSF (1999) "Fact Sheet," Office of Legislative and Public Affairs, online: www.nsf.gov/od/lpa/news/media/fs325.htm, April 1999, retrieved June 18, 1999.

NTIA (1999) *Falling Through the Net: Defining the Digital Divide*, U.S. Department of Commerce, online: www.ntia.doc.gov/ntiahome/digitaldivide/index.html, July 8, 1999, retrieved Aug. 10, 1999.

Oakes, C. (June 1999) "Tackling E-Privacy in New York," *WiredNews*, online: www.wired.com/news/news/politics/story/19991.html, retrieved June 3, 1999.

Oakes, C. (July 1999) "Fast Net Standards in Place," *WiredNews* , online: www.wired.com/news/news/technology/story/20585.html, retrieved July 7, 1999.

Oakes, C. (2000) "Online Security Remains Elusive," *WiredNews*, online: www.wired.com/news/politics/0,1283,33569,00.html, retrieved Jan. 1, 2000.

OECD (1998a) "A Borderless World: Realising the Potential of Global Electronic Commerce," online: www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final, retrieved June 4, 1999.

OECD (1998b) "SMEs and Electronic Commerce," Working Party on Small and Medium-Sized Enterprises, Report DSTI/IND/PME(98)18/REV1, online: www.oecd.org/dsti/sti/it/ec/prod/sme18e.pdf, Sep. 18, 1998, retrieved July 29, 1999.

OECD (1998c) *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda*, online: www.oecd.org/subject/e_commerce/summary.htm, retrieved September 22, 1999.

Olbeter, E. R. and Robinson, M. (1999) "Breaking the Backbone: The Impact of Regulation on Internet Infrastructure Deployment," online: www.iadvance.org/background/, July 27, 1999, retrieved July 28, 1999.

Oliva, R. A. and Prabakar, S. (1999) "Copyright perils can lurk on the business Web," *Marketing Management*, (8)1 (Spring 1999), pp. 54-57.

Oxley, M. G. (1999) "House Passes E-SIGN Legislation," online: www.house.gov/oxley/n9911e.htm, Nov. 9, 1999, retrieved Dec. 8, 1999.

Perritt, H. H., Jr. (1999) From his presentation at Regul@tion$.gov: Coming to Terms With On-Line Commerce, Washington College of Law, American University, Mar. 26, 1999. Videotapes of the conference are available from the organizer.

Pincus A. J. (1999) "Statement of Andrew J. Pincus, General Counsel, U.S. Department of Commerce," online: www.house.gov/judiciary/pinc0930.htm, retrieved Jan. 11, 2000.

Pitofsky, R. (1999) "FTC Chairman Robert Pitofsky's Opening Remarks at Workshop on Consumer Protection in The Global Electronic Market," online: www.ftc.gov/opa/1999/9906/globalpitof.htm, June 8, 1999, retrieved June 22, 1999.

President's Information Technology Advisory Committee (1999) "PITAC Review of the Next Generation Internet Program and Related Issues," online: www.ngi.gov/pitac_ngi_review.html, Apr. 28, 1999, retrieved June 18, 1999.

Pringle, D., Borzo, J. and Eden, S. (2000) "'I Love You' E-Mail Virus Attacks Computer Systems World-Wide," *WSJ.com*, May 4.

Reporters Sans Frontières (1999) "The twenty enemies of the Internet," online: www.rsf.fr/uk/alaune/ennemisweb.html, Aug. 9, 1999, retrieved Aug. 19, 1999.

Reuters (Jan. 7, 2000) "Clinton Will Ask for Funding To Prevent Cyber-Terrorism," *WSJ Interactive Edition*.

Reuters (2000) "The Hijacking of Web.net," Jun. 1, 2000.

Richtel, M. (1999) "Judge Says Local Officials Can Force AT&T to Share Cable Lines," *The New York Times*, June 5, 1999, pp. B1, B4.

Richtel, M. (2000) "Both Sides Talk of Victory in Cable Ruling," *The New York Times*, June 23, 2000, pp. C2.

Robinson, S. (1999) "CD Software Said to Gather Data on Users," *The New York Times*, Nov. 1, 1999, pp. C1, C10.

Rosen, C. (2000) "Electronic-Signature Bill Awaits Clinton's Paper Signature," *InformationWeek Daily*, June 15, 2000.

Rosoff, M. (1999) "Threat From the Net," *CNET*, online: home.cnet.com/category/0-3805-7-292506.html, July 7, 1999, retrieved July 8, 1999.

Sandoval, G and Wolverton, T. (2000) "Security, privacy issues make Net users uneasy," *CNET*, online: news.cnet.com/news/0-1007-200-1518321.html, Jan. 7, 2000, retrieved May 23, 2000.

Samuelson, P. (1999) "Good News and Bad News on the Intellectual Property Front," *Communications of the ACM*, (42)3 (Mar. 1999), pp. 19-24.

SBA (2000a) "About the Small Business Classroom," online: classroom.sba.gov/about.htm, retrieved June 15, 2000.

SBA (2000b) "May We Assist You?" online: www.business.gov/busadv/index.cfm, retrieved June 15, 2000.

SBA (2000c) "What is PRO-*Net*?" online: pro-net.sba.gov/index2.html, retrieved June 15, 2000.

SBA (2000d) SBA Technology Resources *Network* home page, online: tech-net.sba.gov, retrieved June 16, 2000.

SBA (2000e) SBA, Office of Advocacy, ACE-*Net* home page, online: www.sba.gov/advo/acenet.html, retrieved June 16, 2000.

Schiesel, S. (Oct. 1999) "Another Giant Seeks to Deflect Cable TV Criticism," *The New York Times*, Oct. 6, p. C1.

Schiesel, S. (Nov. 1999) "Lucent Says it has New Switching Technology," *The New York Times*, Nov. 10, p. C4.

Schiesel, S. (Dec. 1999) "AT&T Revamps to Pursue Local Phone, Internet Markets," *The New York Times*, Dec. 7, p. C15.

Schull, J. (1999) "Infonomics 101: A map of the information economy," *Inform*, (13)2 (Feb. 1999), pp. 28-31.

SCORE (2000) Counselors to America's Small Business home page, online: www.score.org, retrieved June 16, 2000.

See, D. (1999) "UK Net Bill Passes Hurdle," *WiredNews*, online: www.wired.com/news/politics/0,1283,32675,00.html, Nov. 22, 1999, retrieved Dec. 8, 1999.

Simpson, G. R. (2000) "Internet-Tax Panel Will Focus On Extending Ban for Years," *WSJ Interactive Edition*, Feb. 2, 2000.

Smith, M. (2000) "EU and US Agree on Data Protection: Personal Information Breakthrough Aims to End Displute," *Financial Times*, Mar. 15, 2000, pp. 13.

Sprenger, P. (June 1999) "Rio Rolls Over RIAA," *WiredNews*, online: www.wired.com/news/news/politics/story/20235.html, retrieved June 16, 1999.

Sprenger, P. (July 20, 1999a) "UK E-Commerce: Mind the Gap," *WiredNews*, online: www.wired.com/news/news/politics/story/20812.html, retrieved July 21, 1999.

Sprenger, P. (July 20, 1999b) "Server Bug Places Sites at Risk," *WiredNews*, online: www.wired.com/news/technology/0,1282,20836,00.html, retrieved July 22, 1999.

Sprenger, P. and Glave, J. (1999) 'MS Backs Privacy with Ad Bucks," *WiredNews*, online: www.wired.com/news/news/business/story/20377.html, retrieved June 25, 1999.

Srinivasan, K. (1999) "Consumer Advocates File Petition Alleging Privacy Danger in E-Mail," *WSJ Interactive Edition*, online: interactive.wsj.com/articles/SB944261086973664340.htm, Dec. 3, 1999, retrieved Dec. 6, 1999.

Stackpole, K, Bruce J.T., Baker, W.B. and Margie, R.P. (1998) "Before the Federal Trade Commission: Comments of the Electronic Messaging Association," by Wiley, Rein & Fielding for EMA, online: www.ema.org/html/at_work/ftc.htm, July 7, 1998, retrieved May 23, 2000.

Stroud, M. (1999) "Digital's Long, Winding Road," *WiredNews*, online: www.wired.com/news/news/culture/story/20334.html, June 21, 1999, retrieved June 22, 1999.

SPLC (1999) "Judge halts enforcement of new federal Internet censorship law," online: www.splc.org/newsflashes/020599copa.html, Feb. 5, retrieved June 29, 1999.

Takahashi, D. (1999) "'Worm' Strikes Tens of Thousands Of Computers Across the Globe," *WSJ Interactive Edition*, June 14.

Tapscott, D. (1999) "Introduction," in *Creating Value in the Network Economy*, Tapscott, D. (ed), Boston: Harvard Business Review Press, 1999, p. xxvi.

Taqqart, S. (1999) "Australian Net Censor Law Passes," *WiredNews*, online: www.wired.com/news/news/politics/story/20499.html, June 30, 1999, retrieved July 1, 1999.

Tsuruoka, D. (1999) "Will Employee Privacy Be the Internet Issue of '00s?" *Investor's Business Daily*, Dec. 29, 1999, p. A6.

UK Parliament (2000) "Public Bills before Parliament," online: www.parliament.the-stationery-office.co.uk, retrieved June 15, 2000.

UN Development Program (1999) "Human Development Report 1998," online: www.undp.org/hdro/98.htm, retrieved July 13, 1999.

UN Office of Legal Affairs (1999) "Status of Conventions and Model Laws," online: www.uncitral.org/english/status/status.pdf, retrieved Jan. 11, 1999.

UNCITRAL (1998) "UNCITRAL Model Law on Electronic Commerce," online: www.uncitral.org/english/texts/electcom/ml-ec.htm, retrieved June 17, 2000.

U.S. Department of State (1999) "Sept. 10 APEC Ministerial Meeting Joint Statement," International Information Programs, online: usinfo.state.gov/regional/ea/apec/min99.htm, retrieved Oct. 20, 1999.

Van, J. (July 1999) "AT&T puts its name on TCI cable," *Chicago Tribune*, section 3, pp. 1, 4.

Van, J. (Oct. 1999) "Net access upgrade to cost SBC $6 billion," *Chicago Tribune*, Oct. 19, 1999, section 3, pp. 1, 6.

Vastine, R. (1999) "Expanding Global Services Trade Through Electronic Commerce," statement before the Committee on Commerce, House of Representatives, online: www.uscsi.org/expanding_global_servicest.htm, retrieved Aug. 6, 1999.

vBNS (2000), very High performance Backbone Network Service, FAQ, online: www.vbns.net, retrieved June 2, 2000.

Wayner, P. (2000) "Attacks on Encryption Code Raise Questions About Computer Vulnerability," *The New York Times*, Jan. 5, 2000, p. C2.

WGEC (1998) "First Annual Report," online: www.doc.gov/ecommerce/E-comm.pdf, retrieved June 4, 1999.

WGEC (1999), "Towards Digital eQuality," 2nd Annual Report, online: www.ecommerce.gov/annrpt.htm, retrieved June 7, 2000.

White House (1998b) "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," white paper, online: docs.whitehouse.gov/WH/EOP/NSC/html/documents/NSCDoc3.html, May 1998, retrieved June 17, 1999.

Wigfield, M. (1999) "Panel to Begin Work Sorting Out Contentious Internet-Tax Issues," *WSJ Interactive Edition*, June 18, 1999.

Winn, J. K. (1999) "Clash of the Titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems," online: www.smu.edu/~jwinn/clashoftitans.htm, retrieved May 25, 1999.

WiredNews, online (July 21, 1999) "FCC to Fight Open Cable Access," *WiredNews* , online: www.wired.com/news/news/business/story/20857.html, retrieved July 22, 1999.

WiredNews, online (Dec. 7, 1999) "'Locusts' Infesting E-Commerce," *WiredNews* , online: www.wired.com/news/reuters/0,1349,32960,00.html, retrieved Dec. 8, 1999.

WiredNews, online (Feb. 2, 2000) "Class-Action Suit Calls on AOL," *WiredNews* , online: www.wired.com/news/politics/0,1283,34063,00.html, retrieved Feb. 5, 2000.

WiredNews, online (Feb. 14, 2000) "AOL Gives Up Fast-Access Fight,": www.wired.com/news/politics/0,1283,34334,00.html, retrieved Feb. 15, 2000.

Wood, G. (1999) Personal communication with Mr. Wood, Director of Communications, Internet2, June 19, 1999.

WTO (1998) "Work Programme on Electronic Commerce," online: www.wto.org/wto/ecom/e_274.doc, Sep. 30, 1998, retrieved Aug. 4, 1999.

WTO (1999) "Seminar on Electronic Commerce and Development," WT/COMTD/18, online: www.wto.org/ddf/ep/D1/D1171e.doc, Mar. 23, 1999, retrieved June 20, 2000.

WuDunn, S. (1999) "Forced to Compete, Japan Becomes a Global Power," *The New York Times*, July 27, 1999, pp. C1, C8.

Zelnick, N. (1999) "Another Lawsuit Filed as Patent Wars Escalate," *Internet World News* , Nov. 18, 1999.

LIST OF ACRONYMS

ACLU - American Civil Liberties Union

ADSL - asymmetric digital subscriber line

AIDS - acquired immunodeficiency syndrome

AOL - America Online Inc.

APEC - Asia-Pacific Economic Cooperation

B2C - business to consumer

bps - bits per second

BT - British Telecom

CA - Certification Authority

CD - Compact Disk

CDMA - code division multiple access

CEO - Chief Executive Officer

CNNFN - Cable News Network Financial

COPA - Child Online Protection Act

DMCA - Digital Millenium Copyright Act

D-N.J. - Democrat, New Jersey

DOC - U.S. Department of Commerce

D. Ore - Democrat, Oregon

EMA - Electronic Messaging Association

EU - European Union

FBI - U.S. Federal Bureau of Investigation

FCC - U.S. Federal Communications Commission

FTC - U.S. Federal Trade Commission

FTP - File Transfer Protocol

GATS - General Agreement on Trade in Services

GATT - General Agreement on Tariffs and Trade

GBDe - Global Business Dialogue on Electronic Commerce

GII - Global Information Infrastructure

IBM - International Business Machines Corporation

ICANN - Internet Corporation for Assigned Names and Numbers

ICC - International Chamber of Commerce

IETF - Internet Engineering Task Force

IFEA - Internet Free Expression Alliance

IIS - Internet Information Server

IP - Internet Protocol

IPv6 - Internet Protocol version 6

ISP - Internet Service Providers

ITFA - Internet Tax Freedom Act

ITU - International Telecommunications Union

LAN - local area network

MP3 - MPEG-1 Layer 3

MPEG - Moving Picture Expert Group

MPLS - Multiprotocol label switching

NASA - National Aeronautics & Space Administration

NGI - Next Generation Internet

NSF - National Science Foundation

OC-12 - optical carrier 622 Mbps

OC-48 - optical carrier 2.488 Gbps

OECD - Organisation for Economic Co-operation and Development

PC - personal computer

PDD 63 - Presidential Decision Directive 63

PIN - personal identification number

PKI - public key infrastructure

R. Cal - Republican, California

SBA - U.S. Small Business Administration

SME - Small and Medium-Sized Enterprises

SPLC - Student Press Law Center

SSL - secure socket layer

TV - television

UCLA - University of California Los Angeles

UNCITRAL - United Nations' Commission on International Trade Law

USISPA - United States Internet Service Providers Alliance

vBNS - very High performance Backbone Network Service

WGEC - U.S. Government Working Group on Electronic Commerce

WIPO - World Intellectual Property Organization

WTO - World Trade Organization

ABOUT THE AUTHOR

Sasa Dekleva is Associate Professor of Information Systems and the MIS Program Administrator at the Kellstadt Graduate School of Business at DePaul University in Chicago, Illinois. He earned his Ph.D. in information systems from University of Belgrade. Before coming to DePaul University, he spent ten years in the industry at various system engineering and management positions and taught at the Universities of Ljubljana, Maribor, and Iowa. His articles have appeared in *Communications of the ACM*, *MIS Quarterly*, *Information Systems Research*, and many other journals. His current research interests include electronic commerce and IT management.

Communications of the Association for Information Systems