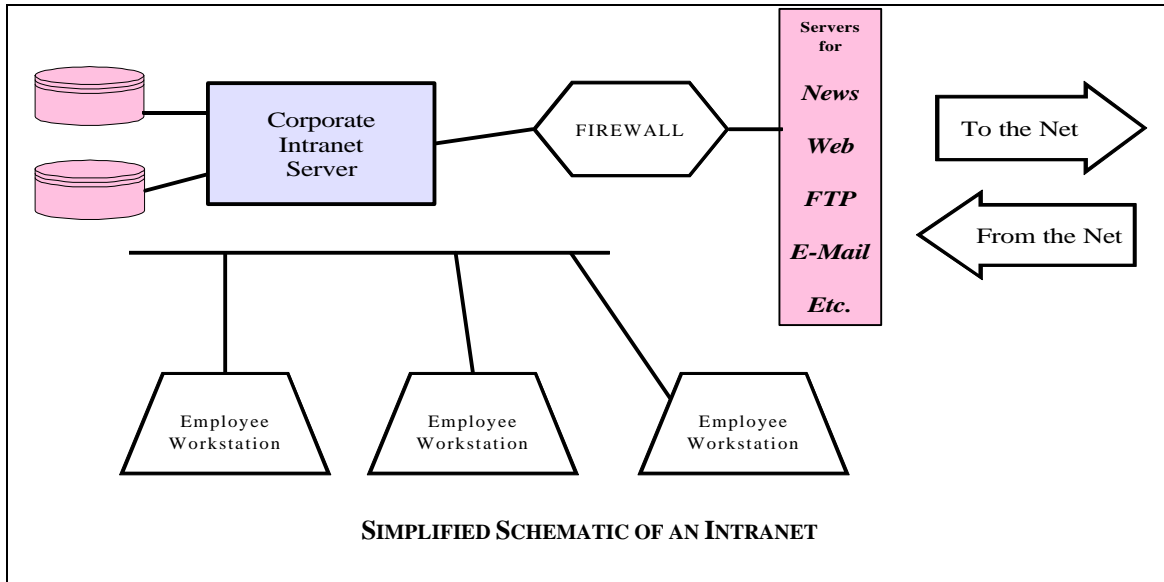


Standard software and protocols allow a seamless integration between internal and external sites.

**Figure 8**



This is a growth area, and one that can be adapted to use by any organization large enough to have its own internal network(s) and with a need to communicate with the Internet in either or both directions. Despite its current domination of the Internet browser market, much, if not most, of Netscape's business is in the corporate intranet market, and the company is refocusing its efforts to concentrate there.<sup>41</sup>

### **Pileups on the Information Superhighway**

All of the other issues discussed here become moot if access becomes so constipated as to render the Internet useless. Liken the experience to a traffic light that never turns green and allows no way around. If the traffic light is at the end of your driveway, driving ceases to be an option. (More accurately, the red light would likely be at the driveway to your cyberspace *destination* across the country or at an overcrowded interchange en route. The effect would be the same: you are not going anywhere.)

#### Sources of Congestion

- More hosts and more users.
- More high-bandwidth uses, especially sound and video.

<sup>41</sup> Robert E. Calem, "Netscape Unveils Its New Internet Suites," *New York Times* (online edition), October 16, 1996.

- Overworked routers and DNS servers.
- Growth in junk e-mail--commercial, advocacy, pranks, and chain letters.
- Lack of incentive to limit or set priorities on use, as access is often not metered and flat-rate services do not encourage conservation of bandwidth.

An indirectly related issue resulting from expansion of the Internet is a looming shortage of domain names and of IP addresses, the numerical addresses that uniquely identify each computer on the Internet, as a phone number uniquely identifies a particular customer's account. Steps are underway to alleviate these problems.<sup>42</sup>

### Are there Solutions?

Some aspects of the congestion problem can be solved, and some cannot. There has even been a vigorous debate over whether there *is* a bandwidth shortage (currently or just around the corner). One industry analyst predicted that Atlanta Olympics-related traffic on the Internet would cause online gridlock. The prediction proved false. Experience online nonetheless demonstrates that congestion is real and that it appears to be getting worse. At the same time, it is not nearly as serious as one would have expected from the phenomenal growth in Internet hosts, content, and users over the past two or three years.

It is critical to bear in mind that no matter how great the capacity of the Internet as a whole is, a popular site may be overwhelmed and inaccessible to most people trying to access it at a given time. *That is a reflection of limitations at that site*, not of the Internet as a whole. At the same time, however, even if specific sites are managing ok, if the total volume of traffic on the Net becomes large enough (millions of users accessing millions of hosts), bandwidth, routers, and DNS may be swamped. One person may be experiencing a system congestion problem while another is simply trying unsuccessfully to access one heavily used site. The results will look the same to the user, but the problems are fundamentally different.

Approaches to dealing with congestion cover a wide range, including purely technical data-handling methods, economics-oriented proposals for congestion pricing or priority tagging, and the building of alternative networks. As government increasingly makes use of the Internet to provide information and services, congestion increasingly is a matter of direct public concern.

---

<sup>42</sup> An even more distantly related, although not trivial, issue is the shortage of telephone numbers as more and more households acquire second phone lines for modem use. The growth in second lines for modems comes on top of increasing need for phone numbers for cellular phones, fax machines, and growing numbers of households and businesses.

Some methods that have been used or proposed follow:

- Data compression reduces the number of bits a message requires without losing necessary information, stretching available bandwidth. Some types of files can be compressed by a large factor (as much as 27:1 in the case of video, for example<sup>43</sup>). Compression can be accomplished in software and in hardware and at various levels in the system, including by modems that support data compression.<sup>44</sup>
- Installation of higher bandwidth backbones and of additional backbones.
- Use of faster routers and of high-speed switches.
- “Caching” of popular web sites on local servers (so that the data need not be retrieved again from the original source) and use of “mirror” sites that replicate often-used resources at alternative locations.
- Congestion pricing. Variations on this theme have been proposed or discussed by Jeffrey MacKie-Mason, Hal Varian, and others, but so far none appears to be practical to implement.<sup>45</sup> The question of congestion pricing encompasses complex questions of both economics and technology, and is beyond the scope of this paper. The central point, though, is that congestion would be reduced and bandwidth allocated more efficiently (from an economic point of view) if use of bandwidth were priced in proportion to congestion. Higher prices during congested periods would tend to change behavior so that low-value uses would be reduced or deferred in favor of high-value uses. Each user could, of course, determine what is of high or low value to him or her and when.
- Priority tagging of data packets. Cisco Systems has announced “Tag Switching technology,” a hardware-based means of differentiating among data packets on the basis of priorities. The technology is not in use yet, but appears to be part of Cisco’s strategic plans.<sup>46</sup>

Other technical developments promise increased bandwidth. These include asynchronous transfer mode (ATM), frame relay, Asynchronous Digital Subscriber Loop (ADSL), and Integrated Services Digital Network (ISDN). The *Cyber Dictionary* flatly asserts that

---

<sup>43</sup> Bill Gates, *The Road Ahead* (New York: Viking, 1995), p. 30.

<sup>44</sup> See Shnier, *Dictionary of PC Hardware and Data Communications Terms*, for definitions and brief explanations of many compression-related terms and techniques.

<sup>45</sup> See, for example, Jeffrey MacKie-Mason and Hal Varian, “Some Economics of the Internet,” paper prepared for the Tenth Michigan Public Utility Conference at Western Michigan University, March 25-27, 1993. Version posted on line dated February 17, 1994. Also, MacKie-Mason and Varian, “Pricing the Internet,” prepared for the conference “Public Access to the Internet,” JFK School of Government, May 26-27, 1993. Version posted on line dated February 10, 1994.

<sup>46</sup> See Cisco’s September 1996 white paper, “Scaling the Internet with Tag Switching,” posted at <http://www.cisco.com>.

ATM “will be the basis for most telecommunications by 1997.” It is an international standard designed from the ground up to carry data, voice, and video, to allow different types of system to communicate, and to serve networks of all sizes and scopes. Detailed discussion of these technologies is beyond the scope of this paper, but Kalakota and Whinston provide a summary.<sup>47</sup> The essential point is that the telecommunications technology underlying the Internet is evolving rapidly and dramatically in directions that could not have been predicted only a few years ago, driven by international commercial interests.

### **Is the Internet Boom Headed for Collapse?**

Cynics may suggest that the Internet is like citizens' band radio, a fad that shoots to prominence, peaks, then declines to a steady-state, obscure utility level. In a recent letter to *Time* magazine, one person summarized that view:

This whole computer/internet thing leaves me a bit mystified. Aside from a very few niche applications in business and certain of the sciences, of what practical use are computers or the Internet? The minor applications in business and research are valuable, but otherwise computers look to me like nothing more than expensive toys--Barbie dolls for spoiled and bored grownups--and the Internet browser programs look suspiciously like this year's dresses for Barbie.<sup>48</sup>

Given the explosive growth of the Internet, especially its Worldwide Web aspect, and given the large commercial enterprises with a stake in it, collapse of the Internet's popularity and growth looks unlikely now. But then, the collapse of the CB boom looked unlikely, too. What, then, might lead to a similar implosion for the Internet?

- Using it is too difficult and confusing for many potential users. Computers, even personal computers, can be cranky, confusing, and hard to use. To connect with the Internet, people not already used to a PC have to overcome the hurdles of using a PC in the first place *and* the hurdles of installing Internet access software and getting it to work. Even using a keyboard and mouse, not to mention navigating Windows, presents a challenge.
- Loss of novelty. Net surfing might simply become passé as it becomes more and more familiar to more and more people. But on the other hand, television is not novel yet remains a medium that, while changing, is entrenched and ubiquitous. The major commercial television *networks* may be losing market share, but that does not mean that the medium itself is going away. The question then is, is the Internet, as it is now established and developing, merely a novelty item with only transient entertainment value? Or does it involve much more than that, activities with more permanence? The

---

<sup>47</sup> *Frontiers of Electronic Commerce*, Chapter 19, “Broadband Communications.” This may be the best currently available summary.

<sup>48</sup> Marty Meltzer, Morton Grove, Illinois, letter to editor, *Time*, October 7, 1996, p. 4.

burgeoning numbers of sites and capabilities devoted to valuable information and services, communications, and commerce of all types suggest that the Internet is here to stay, even as the "market share" of its original applications shrinks.

- Using the Internet is too slow. The online experience can be tedious and therefore unrewarding. As a result, growth in the number of users could slow and eventually come to a halt.
- Regulatory strangulation. If Internet access providers, businesses online, backbone providers, and others involved in the system face excessive hurdles, growth could be slowed.
- Digital sabotage. Malicious hackers have repeatedly demonstrated that they can shut down Internet providers, delete thousands of posted messages with "cancelbots," and vandalize Web sites. If these sorts of activities become common, they could discourage and drive away users of the Internet at all levels, from individuals to corporations.
- High costs of access and use. Unless access becomes less costly (not requiring a \$1,500 to \$2,000 PC and not running up large monthly fees and possibly requiring a second phone line), the pool of people willing to pay for access will be exhausted.
- Unreliability for sensitive or critical applications. If the Internet simply cannot be made reliable for transactions requiring timeliness, security, and confidentiality, then its attractiveness will shrink.
- Failure of businesses to make a profit via the Internet. Many businesses have made money *from* the Internet (selling hardware, software, consulting services, access, and so on), but it is not clear that many have made money *on* the Internet. Ultimately, Web sites must be shown to contribute to business profitability. If that does not happen, the movement toward online commerce will come to a halt.
- Shortage of techno-nerds. Continuing growth in use of the Internet requires technicians at all levels. Small companies wishing to go online must either have in-house expertise or contract with a service to provide that expertise (setting up a Web site, for example). Companies, agencies, and individuals all need to get their hardware and software installed and running, even for simple access to the Internet for information and e-mail. At the rate Internet hosts and users have been increasing, technicians may be in short supply, at least for a time, slowing further growth.
- Too many choices. There may be a risk of consumers entering mental gridlock when faced with choices among Internet-access from cable companies, telcos, numerous local and regional ISPs, value-added proprietary providers, wireless systems, and others yet to be announced. The sensation may be not unlike that felt by the hapless

consumer surrounded by legions of car salesman at an auto mega-mall, a panic leading to flight.

The other side of all of these issues is that countless businesses, government agencies, educational institutions, organizations, and individuals have an interest in continuing the success and growth of the Internet. Some want to use it to provide information, some to sell goods and services online, and some to sell Internet equipment and software at all levels. The more it does succeed, the more incentive there will be to make access easier and more widespread and the more people there will be with the ability to do so.

In whose interest is it to ease access to the Net?

- Government agencies that want to put information and services online.
- Businesses looking for customers online.
- Educators who see that students benefit from information online.
- Publishers who want to benefit from paperless, inventoryless online systems.
- Tourist destinations (chambers of commerce, local attractions, hotels and motels, and so on) as they seek to reach travelers and vacationers.
- Travelers and tourists looking for help to choose destinations, arrange accommodations, and pick travel routes and methods.
- Librarians and library patrons making use of books, magazines, newspapers, and documents online.
- Environmentalists who see pollution reductions and resource savings made possible by online communications.
- Employers posting job notices, communicating with employees, and setting up telecommuting programs.
- Real estate agents advertising or looking for properties.
- Providers of Internet access services, who wish to have as large a clientele as possible.
- Producers of Internet-related hardware and software, who seek to enlarge their market.

In short, an enormous range of individuals and organizations share an interest in making Internet access widely and easily available. For that reason it seems improbable that

access could long remain too slow or too difficult. Too many people and institutions have incentives and abilities to fix the problems.

In other words, *market pressures and opportunities will work to make access to the Internet widely and inexpensively available.*

In the future, everyone will have a Web site

Well, maybe not everyone--but perhaps as many people and organizations as now have telephone listings, advertisements in newspapers and magazines, and listings in professional society rosters and "who's who" lists. As e-mail becomes an increasingly common way to reach people, and as the Internet becomes increasingly common as a way of finding information, personal Web pages will become increasingly accepted as a way of making available that information people wish to be public, including hobbies and interests, résumés, organizational memberships, and business information. This *could* require a lengthy transition--a generation or more--but could also happen much more rapidly, at least among a large part of the U.S. population.

In time, e-mail will become as common as today's physical, paper mail services, called "snail mail," by Internet users, and will develop comparable alternative delivery systems. It is not difficult to envision a chain of "E-Mail Boxes, Etc." stores for those who want privacy, prefer not to clutter their home or business e-mail boxes with some kinds of correspondence, are on the road, or otherwise need an alternative or an extra e-mail account.

Little by little, communications via the Internet, or whatever a successor system may be called, will become as routine as the telephone, television, and fax machine are today--and all of those were new and unknown technologies not very long ago.

-----

This chapter has outlined what the Internet is and where it came from, how it works, the kinds of information it encompasses, how the Internet relates to the telephone system, and changing methods of access. The next chapter looks at commerce on the Internet and some of the issues related to Internet-based business.





## CHAPTER 2: COMMERCE ON THE INTERNET

“Within a few years, the digital document, complete with authenticatable digital signatures, will be the original, and paper printouts will be secondary.” (Bill Gates, *The Road Ahead*, 1995.)

“It will take at least a half a century for customer use of electronic money and banking to become commonplace, the chairman of Citicorp said Thursday [September 19, 1996].” (Reuter Information Service report, September 20, 1996.)

Commerce is now the driving force behind the Internet’s continuing growth, especially its Worldwide Web aspect. Everything except physical goods can be delivered across communications lines in the form of digital information. Much commerce is just the exchange of information, which makes the Internet an ideal means for conducting business. Although physical goods cannot be sent over the wires, information vital to design, production, selection, sale, purchase, and delivery of such goods certainly can be. You cannot send groceries over the Internet, but at least in Manhattan and in Los Angeles you can order them online for next-day delivery.<sup>49</sup>

Businesses of many types are already on the Web, sometimes selling directly and sometimes just providing information on products that may be purchased by other means. Advertising appears on increasing numbers of sites, and hyperlinks quickly bring Web users to vendors’ own Web pages. While the Web has reportedly not yet proven profitable to many companies, the technology is still in its infancy as a means of doing business.

During the 1996 Summer Olympics, Web addresses appeared in small print on many televised advertisements, in contrast to none whatsoever in any previous Olympics. This is a harbinger of things to come, where advertising is integrated across the spectrum, from print to broadcast to Internet. Once TV broadcasts are themselves coordinated with the Internet and viewers may navigate on screen to an advertiser’s site, the integration of the technologies will become complete: *The sprinters perform. Reebok (or Nike, or whoever) runs a spot promoting its running shoes and other athletic gear. The viewer clicks on an icon to visit a virtual sales floor for the promoted merchandise, examines the choices, and enters an order on the spot. The order is transmitted instantly to the local dealer, who in turn delivers the merchandise to the purchaser’s door or has it ready for pickup at a nearby store.*

The Internet, and especially its Web component, is beginning to have a significant impact on the conduct of some types of business. For example, the ability to post real estate information on the Web is offering some competition to the Multiple Listing Service, a

---

<sup>49</sup> Katherine Cavanaugh, “Grocery Shopping Online in Manhattan,” *New York Times* (online edition), September 4, 1996. In Los Angeles, Kroger’s has an online grocery shopping site, with a link from the *Los Angeles Times*’s Web site as of mid-September 1996.

system to which only fee-paying Realtors<sup>50</sup> have access. Real estate companies are posting their own Web pages and individual home owners can post information that is then freely available to anyone with Web access. (Real estate mega-firm Coldwell Banker has a Web site that it advertises on the radio.) It is only reasonable to expect Web-based businesses to spring up specifically to facilitate listing of properties online and to act as a central directory of many property listings, even to facilitate "by-owner" sales. Similar enterprise may be expected in other areas where the Internet may be used to get buyers and sellers together outside of previously established methods and institutions.

In evaluating the commercial potential of the Internet, one group of researchers concluded:

The Internet, especially that portion known as the World Wide Web, has the potential to radically change the way businesses interact with their customers. The Web frees customers from their traditionally passive role as receivers of marketing communications, gives them much greater control over the information search and acquisition process, and allows them to become active participants in the marketing process.<sup>51</sup>

The opportunities offered by these changing roles can be expected to multiply as use of Internet grows in number of participants and in the types of transactions in which those participants engage. So far, consumers have been reluctant to make purchases online, but this can be expected to change as payment methods become easier and more secure, as consumers become more familiar and comfortable with the technology, and as more consumers have Internet access.

At this time, there is little indication of the Internet yet proving profitable to online businesses. David C. Churbuck, writing in *Forbes*, asked, "where is the flood of spending money this great phenomenon [the Internet] was supposed to unleash?" He adds, "as a way to move merchandise, it has not proven itself and probably won't for a long time."<sup>52</sup> That article appeared two years ago, though, and much has happened since then, both in terms of increasing numbers of Internet users and in terms of mechanisms for merchandising online. The potential for profitability may be growing faster than the author expected. More recent reports, however, are not wildly encouraging, at least for the near term:

Thousands of companies have set up electronic storefronts on the World Wide Web with hopes of luring customers from around the globe. But precious few have produced a profit, while the vast majority of Web sites

---

<sup>50</sup> "Realtor" is a trademark for a member of the National Association of Realtors, and is not synonymous with the generic term "real estate agent."

<sup>51</sup> Donna L. Hoffman, Thomas P. Novak, and Patrali Chatterjee, "Commercial Scenarios for the Web: Opportunities and Challenges," *JCMC*, Vol. 1, No. 3 (posted at <http://shum.huji.ac.il/jcmc/vol1/issue3/-hoffman.html>, downloaded October 10, 1996), p. 17.

<sup>52</sup> "Where's the Money?" *Forbes*, January 30, 1995 (as posted on line).

are still spilling red ink. Most of these efforts lack the financial resources of Microsoft [which is reported to be ready to lose substantial sums of money on its Internet activities, following losses already running into the hundreds of millions of dollars].<sup>53</sup>

The issues surrounding online commerce are of concern not only to business, but also to government, as government increasingly conducts business online. The California Department of Information Technology (DOIT) briefly addressed electronic commerce in its July 1996 *Interim Annual Report*:

The ability to provide information, benefits, and services electronically, without direct, personal contact has revolutionary implications not only for business, but perhaps to an even greater extent [for] government. Virtually any government activity that involves filling out a form, registering, paying, receiving benefits, or supplying information can be done effectively, and significantly more inexpensively, through electronic means. As a result, the DOIT is working with several agencies to aggressively pursue electronic government opportunities.

Currently, hundreds of thousands of individuals and organizations receive paper checks/warrants, benefit coupons, etc., each day from the state. As a result, in conjunction with the Treasurer's Office and the Office of the State Controller, the DOIT is preparing to initiate a pilot in early FY 96-97 to transform this process into an electronic one, substituting electronic payment for the paper-based system.

The DOIT anticipates that this procedure will become ubiquitous, as electronic benefits transfer, electronic data interchange, and other forms of electronic commerce begin to predominate in state government, saving millions of taxpayer dollars.<sup>54</sup>

It seems reasonable to expect that the State of California and local governments in California will begin to purchase supplies and services online as the techniques and opportunities for doing so progress and as online purchasing becomes an efficient and reliable option. However, several issues must be faced before online purchasing becomes the norm.

---

<sup>53</sup> Jared Sandberg, "Microsoft Plans to Spend Big on the Internet," *Wall Street Journal*, November 15, 1996, p. B9.

<sup>54</sup> California Department of Information Technology, *Interim Annual Report: Reforming the State of California's Use and Management of Information Technology* (Sacramento: the Department, July 1996), p. 27.

## General Requirements of Electronic Commerce

There are several requirements for online commerce, applicable to all kinds of transactions, not just those directly involving payment, and not just pertinent to the Internet. These include authenticity, integrity, nonrepudiation, writing and signature, and confidentiality.<sup>55</sup>

*Authenticity* has been defined as being “. . . concerned with the source or origin of a communication. Who is the message from? Is it genuine or a forgery?” Authenticity is necessary for the conduct of business. The Internet does not change that fact, but does create new ways in which authenticity might be compromised or require proof. Knowledgeable computer users can and do send messages that purport to be from another party, a process called “spoofing.”

*Integrity*, too, is vital to business, and “is concerned with the accuracy and completeness of the communication. Is the communication the recipient received the same as the communication that the sender sent? Is it complete? Has the communication been altered either in transmission or in storage?” Electronic methods introduce possibilities for alteration of messages that differ from those previously known. A communication on paper can be altered, but is likely to show some marks of having been altered, such as erasure marks. A purely digital message, however, may be altered with no indication of the change having been made. Use of the Internet expands the potential threats to communications integrity, as insecure systems may be hacked by outsiders and data files altered blatantly or subtly.

*Nonrepudiation* is intimately related to authenticity and integrity. It “is concerned with holding the sender to his or her communication. The sender should not be able to deny having sent the communication if he or she did, in fact, send it, or to claim that the contents of the communication as received are not the same as what the sender sent if, in fact, they are what was sent.”

The law may require that transactions be *in writing and signed*. For example, “federal, state, and local governments . . . require that certain transactions [such as contracts] be signed and in writing . . . before the government will consider itself bound.” But in the world of digital communications, what constitutes a written, signed document?

Finally, *confidentiality* “is concerned with controlling the disclosure of information.” Although sometimes confidentiality is not an issue, other times it is critical. Confidentiality is somewhat separate from the other issues, as a non-confidential communication (one that has been intercepted and read by a third party) might still meet standards of authenticity, integrity, nonrepudiation, and writing-and-signature. Likewise, a commu-

---

<sup>55</sup> This list follows Thomas J. Smedinghoff, editor, *Online Law: The SPA's Legal Guide to Doing Business on the Internet* (Reading, Massachusetts: Addison-Wesley, 1996), Chapter 3.1. Quoted passages in this section, if not otherwise identified, are from *Online Law*, Chapter 3.1.

nication might be kept confidential, but nonetheless be inauthentic or of compromised integrity, subject to repudiation, or lacking verified and accepted signature.

If the problems of authenticity and integrity are solved, and if an accepted method is devised for treating digital documents as written and signed, then the nonrepudiation issue would seem to be solved as well, or at least as well as for comparably secure paper documents. The question then becomes, *how may digital documents be proven authentic, assured of integrity, and affixed with the digital equivalent of a signature?* For the sake of discussion, let us assume that settling those three matters also settles the matter of the communication being “in writing.” A more detailed analysis of that specific point is beyond the scope of this paper.

## Digital Signatures

A “digital signature” is *not* a digital representation of a handwritten signature. Nor is a digital signature the same from one document to another even if issued by the same individual. Rather, a digital signature is based on the specific document *and* on a unique key assigned to the individual. That is, the digital signature is tied to the particular person and the particular document. Any change in the document invalidates the signature and requires that a new one be generated for the revised document, but again one reflecting the individual’s unique key.

The concept is summarized in *Online Law*:

Before a sender can digitally sign an electronic communication, the sender must first create a public-private key pair. The private key is kept confidential by the sender and is used for the purpose of creating digital signatures. The public key is disclosed generally by posting the key in online databases, repositories, or anywhere else the recipient of the digitally signed communication can access it.

To digitally sign an electronic communication, the sender runs a computer program that creates a message digest (or hash value) of that communication. The program then encrypts the resulting message digest using the sender’s private key. The encrypted message digest is the digital signature. The sender then attaches the digital signature to the communication and sends both to the intended recipient.<sup>56</sup>

A “message digest” is a string of characters generated (maybe “calculated” is a better term for the process) by the digital signature software. The string of characters appears meaningless, but the software can evaluate the string and compare it to the message and

---

<sup>56</sup> Smedinghoff, *Online Law*, p. 45. Also see Ravi Kalakota and Andrew B. Whinston, *Frontiers of Electronic Commerce* (Reading, Massachusetts: Addison-Wesley, 1996), pp. 202-3, and Benjamin Wright, *The Law of Electronic Commerce*, Second Edition (Boston: Little, Brown, 1996), §16.7.3.

the public key to determine whether the message has been altered since the digital signature was generated.

The system works because the sender's public key (and *only* the sender's public key) can decrypt a digital signature that has been encrypted with the sender's private key.<sup>57</sup> The sender's private key remains private. The sender cannot repudiate a secure, digitally signed document.<sup>58</sup>

Wyoming, California, and Utah have digital signature laws, and a committee of the American Bar Association has drafted guidelines for digital signatures. The Wyoming law authorizes the Secretary of State to accept electronically signed documents, but leaves the selection of methods up to that office.<sup>59</sup> The California law (Chapter 594, Statutes of 1995, AB 1577, Bowen) defines a digital signature, authorizes their use in communications with public entities, and requires the Secretary of State to adopt regulations not later than January 1, 1997. The Utah law "is more specific, more ambitious, and much more complex . . . [as it] singled out a particular electronic technology, and said that if the technology were used in limited and particular ways, then certain legal results [pertaining to all types of electronic messages] would follow." In addition, "Utah chose to regulate use of the technology, even use that has no direct relevance to the administration of state government."<sup>60</sup>

## Online Payment Systems

A key problem in online commerce is *means of payment*. There must be a way to assure that the payment is valid (authentication), to prevent fraud by merchants or their staffs, and to secure financial information, such as credit card numbers, from unauthorized access. This has been, and will continue to be, an area of vast and varied activity, with many players involved in developing and implementing payment systems. This section will only attempt an overview of some mechanisms now in use or under development and of the sorts of issues that must be addressed.

Government agencies charge for some information and collect fees for some services (for example, park reservations). Once the technical obstacles and security concerns are overcome, tax returns could be filed via the Internet and amounts due collected or refunds provided through electronic fund transfers. (Tax returns can now be filed electronically, a service that many tax-preparers provide, but the filing is not done via the Internet.) Even if government is not involved in the creation of online payment methods and establishment of other standards for commerce, it does have an interest in the efficiency and security of those methods (and in understanding how they may be used) in order to conduct its own affairs in an increasingly Internet-dependent world.

---

<sup>57</sup> For an explanation of encryption, see Daniel C. Lynch and Leslie Lundquist, *Digital Money* (N.Y.: John Wiley and Sons, 1996), especially Chapter 3.

<sup>58</sup> Kalakota and Whinston, p. 202.

<sup>59</sup> Wright, §16.7.3.

<sup>60</sup> Wright, §16.7.3.

Some concepts important to online payment systems are secure protocols, digital cash, and smart cards.

### Secure Protocols

Packets sent on the Internet may be intercepted, and therefore are not secure without special precautions. Concern over theft of credit card numbers and other confidential information sent over the internet has led to a variety of methods to prevent snooping. One relatively low-tech method is for the customer to establish an account with the vendor by mail or over the telephone and then to place orders online with the understanding that the merchandise will be charged to the previously-established account. This addresses the problem of credit card security, but does nothing to prevent snooping into other aspects of the transaction.

One fully online approach is the “secure sockets layer” (SSL), a data security protocol proposed by Netscape Communications. SSL encrypts data going both directions and provides other security measures. The software on both ends of the transaction handles the encryption and decryption. (That is, the Netscape browser program itself does some of the work.) In short, “SSL provides encryption that creates a secure channel to prevent third parties on the network from being able to tamper with and read messages being exchanged between the client and server and authentication that uses a digital signature to verify the legitimacy of the server.”<sup>61</sup> A site may have *both* a secure and an insecure server, so a user can browse a catalog via the insecure server and then go to the secure server to place an order.

Another method is the Secure Hypertext Transfer Protocol, S-HTTP. (HTTP is the Internet protocol used to transfer documents on the Web.) S-HTTP’s approach is to encrypt specific documents transmitted on the Web, while SSL instead encrypts the entire session. SSL and S-HTTP “address different pieces of the security puzzle,” but are not incompatible.<sup>62</sup>

Netscape Navigator users may sometimes notice a small key icon in the lower left corner of the screen. A broken key indicates an insecure server, which is the normal case. When the browser has contacted a secure server, the broken key is replaced by a whole one, indicating a secure protocol. The browser then stops issuing warnings about possible interception of communications when the user completes a form and clicks on the “submit” button.

---

<sup>61</sup> Kalakota and Whinston, p. 247. Section 6.5 of this book (pp. 243-50) addresses security on the Web.

<sup>62</sup> Kalakota and Whinston, p. 249.

## Digital Money

Digital money may take two basic forms.<sup>63</sup> One is a computer data file that holds a store of value. That value may be spent, and as a portion is spent, it is deducted from the total value of the file. I will refer to that system as “digital cash” here for convenience. The other basic form is a “smart card,” a wallet-size card encoded with the value it holds, and used in a manner somewhat comparable to an automated teller machine card. Pre-paid phone cards are a special-purpose smart card.

Daniel Lynch and Leslie Lundquist summarize the “guiding principles of digital money” this way:<sup>64</sup>

- It must be independent from any single physical location
- It must be secure--not reusable
- It must be private--that is, untraceable, just like coins and Federal Reserve Notes
- It must be usable off line as well as online
- It must be transferable to others
- It must be divisible into smaller amounts, so that the whole amount need not be spent in one transaction

Many companies are involved in the field of digital money and other online payment systems. (Some deal in debit systems that draw funds from a bank account, not in “digital money” as defined here.) Not all of them meet all of the listed requirements, and each emphasizes particular features or benefits. These companies include Checkfree, Cyber-Cash, DigiCash, First Virtual, NetBill, Netscape, and Open Market, Inc. (OMI).<sup>65</sup>

It is difficult to draw a clear line between smart cards and digital cash, especially as smart card readers connected to PCs or set-top boxes will allow them to be used for online payment. Both types of digital money will serve the same purpose, to allow payment without the use of credit cards, checks, or checking accounts. At this time, it is not possible to predict which company or companies--or even which systems--will prevail in the market. It does seem likely that ultimately some combination of systems, provided by many companies, will find a niche, just as many kinds and vendors of credit cards and charge cards, checks, check cards, ATM cards, and merchant scrip, not to mention cash, all have a place today.

---

<sup>63</sup> See the “Electronic Payment Schemes” page, <http://www.w3.org/pub/WWW/Payments/roadmap.html>, for extensive information and links to those involved in this industry.

<sup>64</sup> This list is adapted and partly quoted from Lynch and Lundquist, pp. 109-110.

<sup>65</sup> Lynch and Lundquist, p. 37, Table 2.2. For a concise summary of each of these companies, see *ibid.*, especially at pp. 36-39



One of the potential benefits of digital money, especially when used on the Internet, is that it may help to avoid the complexities of currency exchange and to minimize the costs of conversions. Digital money could certainly make international purchases and sales easier and faster. While this prospect is promising to some, it may be threatening to others challenged by increased competition made easier by a borderless Internet.

The State will be directly affected by these technologies in many ways, as both purchaser and vendor of goods and services, and therefore has an interest in their costs, security, and functionality.

### **Taxation and the Internet**

The Internet raises only one tax issue directly: the taxation of Internet access service itself. It does complicate others, however, and may have significant indirect impacts.<sup>66</sup>

The U.S. Department of the Treasury has summarized its view of tax policy and administration issues arising from new information and communication technologies, including electronic money:

These new technologies . . . have effectively eliminated national borders on the information highway. As a result, cross-border transactions may run the risk that countries will claim inconsistent taxing jurisdictions, and that taxpayers will be subject to quixotic taxation. If these technologies are to achieve their maximum potential, rules that provide certainty and prevent double taxation are required.

In order to ensure that these new technologies not be impeded, *the development of substantive tax policy and administration in this area should be guided by the principle of neutrality. Neutrality rejects the imposition of new or additional taxes on electronic transactions and instead simply requires that the tax system treat similar income equally, regardless of whether it is earned through electronic means or through existing channels of commerce.* [Emphasis added.]

A major substantive issue raised by these new technologies is identifying the country or countries which have the jurisdiction to tax such income. It is necessary to clarify how existing concepts apply to persons

---

<sup>66</sup> On November 21, 1996, the U.S. Treasury Department announced “a draft report . . . that outlines the Clinton administration’s opposition to new federal taxes on the Internet but underscores its determination that the global computer network not become a haven for tax evaders . . . the report would advocate an ‘overarching goal of neutrality [treating transactions similarly whether they take place on or off the Internet],’ at least on the federal level . . . .” (“U.S. Trying to Figure Out How to Tax Internet,” *San Francisco Chronicle*, November 21, 1996, p. D1.) The draft has been posted for comment (see below), but came too late for review and analysis in this paper.

engaged in electronic commerce. In addition, transactions in cyberspace will likely accelerate the current trend to de-emphasize traditional concepts of source-based taxation, increasing the importance of residence-based taxation.

Another major category of issues involve the classification of income arising from transactions in digitized information, such as computer programs, books, music, or images. The distinction between royalty, sale of goods, and services income must be refined in light of the ease of transmitting and reproducing digitized information.

In the area of tax administration and compliance, electronic commerce may create new variations on old issues as well as new categories of issues. The major compliance issue posed by electronic commerce is the extent to which electronic money is analogous to cash and thus creates the potential for anonymous and untraceable transactions. Another significant category of issues involves identifying parties to communications and transactions utilizing these new technologies and verifying records when transactions are conducted electronically. However, developments in the science of encryption and related technologies may lead to systems that verify the identity of persons online and ensure the veracity of electronic documents.<sup>67</sup>

The key policy perspective in the report appears to be the support of neutrality between online (electronic) and other forms of commerce.

### Taxes on Internet Access Services

As Internet access services grow, they are seen as a possible source of revenue by local governments, raising questions of who could tax what, how, and where, and with what effects.

The most-reported case of a tax on ISPs was in Tacoma, Washington.<sup>68</sup> Tacoma imposed a six percent tax on ISPs' service charges and sought a \$72 annual city business license. These fees were to apply to all ISPs with customers in the city, not just those located in Tacoma. Within two months, the Tacoma City Council, under pressure from ISPs and local citizens, repealed the telecommunications tax as it applied to ISPs and agreed to refund taxes already paid. (The fate of the business license has not been reported in press stories about the tax and its repeal, but it appears unlikely that the city could enforce a license requirement or fee on providers not actually having a business location in Tacoma because it has no means by which to do so.)

---

<sup>67</sup> U.S. Department of the Treasury, Office of Tax Policy, *Selected Tax Policy Implications of Global Electronic Commerce*, November 1996 (posted at <http://www.ustreas.gov>), Executive Summary, pp. 2-3.

<sup>68</sup> Reports on this issue have cited similar taxes in Texas, Tennessee, Pennsylvania, Connecticut, the District of Columbia, and Florida.

The simplest approach to an Internet access tax, an approach proposed in Florida, is a statewide excise tax on computer network subscription fees and usage charges. The proposed Florida rate is 7 percent. Florida would also tax gross receipts of Internet service providers at a rate of 2.5 percent “if the business is classified as a taxable telecommunications service.”<sup>69</sup> The Florida Chamber of Commerce is campaigning against the proposed Internet taxes, arguing that telephone service is already taxed and that the proposed measure “sends a very negative signal to business seeking to expand in Florida . . . .”<sup>70</sup> A Chamber spokesman also reported concern over double taxation of the services and over the administrative burden imposed by the complexity of dealing with taxes on these services.<sup>71</sup>

The *practical* difficulty raised by a tax on Internet access services is that a state without such a tax could become a haven for ISPs that provide national access via POPs in other states. A spokesman for the Florida Chamber of Commerce stated that this exact issue had been raised in discussions of the proposed Florida taxes on ISPs.<sup>72</sup>

Final resolution of controversies in this area might require a Supreme Court decision as to the conditions under which states may tax Internet access services provided by out-of-state ISPs *or* federal legislation clarifying the entire subject and possibly preempting the right of states and localities to tax Internet access services.

The *political* difficulty raised by taxes on Internet access services is that Internet users can quickly communicate their opposition and mount an attack via the Internet on those who propose such taxes, as has happened in the cases of the city of Tacoma and the states of Florida and Texas.<sup>73</sup> That possibility, however, has not stopped several states from taxing Internet access services. Such taxes are reportedly imposed by Ohio,<sup>74</sup> Pennsylvania,<sup>75</sup>

---

<sup>69</sup> Reported by Associated Press, February 17, 1996: “Florida to tax Internet service providers?”, as posted at [http://www.jbit.com/bow/bow\\_tax1.htm](http://www.jbit.com/bow/bow_tax1.htm) (downloaded October 28, 1996).

<sup>70</sup> Quoted from press release posted at <http://www.flchamb.com/tsx.html>.

<sup>71</sup> John Bussey, Florida Chamber of Commerce, personal communication, October 28, 1996.

<sup>72</sup> *Ibid.*

<sup>73</sup> As of February of 1996, a controversy had arisen in Texas as to “whether Texas Internet Service Providers are required to pay a direct tax assessment for the Telecommunications Infrastructure Fund. As it stands right now, almost every ISP in the state owes tax for 1995 plus 10% penalty.” Source: “More TIF Tax Trouble for ISP and BBS,” *Texas Telecommunications Journal*, February 29, 1996, as posted at <http://www.telecommute.org/ttj>.

<sup>74</sup> Ohio applies sales tax to internet access services used for business purposes, but not for personal use. A spokesman for the Tax Analysis section of Ohio Taxation Department stated that data on the amount raised by this tax is unavailable, but the amount is probably not large. (David M. Elzemeyer, personal communication, January 14, 1997.)

<sup>75</sup> Pennsylvania expanded its sales tax coverage to include all “computer services” (except those for banking, such as computerized account inquiries) in 1991; that category includes Internet access services (for both business and personal use) along with many other types of computer service. Because Internet access services are included in a broader category, specific figures for revenue raised by the sales tax on Internet access services are not available. (Joe Breen, Pennsylvania Revenue Department, personal communication, January 14, 1997.)

Connecticut,<sup>76</sup> Massachusetts, and the District of Columbia, in addition to the previously mentioned Florida and Texas.<sup>77</sup> New York has decided to exempt Internet access service fees from sales tax.<sup>78</sup>

Currently in California, Internet access services and other online services, such as those provided by Netcom or Internet Unlimited (Internet access) and America Online (value-added network services plus Internet access), are not subject to sales tax, nor is taxation of such services currently proposed or known to be under consideration by staff of the Board of Equalization.<sup>79</sup> The State could, however, extend the sales tax specifically to Internet access charges or impose an excise tax on those services, either directing the proceeds to the General Fund or earmarking them for specific purposes, such as support of information resources for underserved populations or State government use of the Internet as a medium for providing information and services to the public.

#### Sales Tax Liability: Where is a Business on the Web *Doing* Business?

Before the Worldwide Web, a business either had offices, sales floors, representatives, and so on in a state or it did not. If it did, then its sales to residents of the state were subject to state sales taxes (in states with a sales tax). Companies that only mailed catalogs into other states and took orders by mail or phone but that did not have a physical presence in the state argued that they were exempt from any obligation to collect sales taxes and remit them to the states whose residents bought merchandise. The states, however, argued that they were in fact entitled to sales tax revenues on such sales.

The “Quill Decision” (*Quill Corporation v. North Dakota*, 112 S. Ct. 1904 [1992]) addressed the issue of mail order sales:

In *Quill*, the Supreme Court held that an out of state mail order seller that has no physical presence in the state and who merely mails catalogs into the state and fills orders by U.S. mail or common carrier is protected by the Commerce Clause from use tax collection obligations in the destination

---

<sup>76</sup> Internet access services are subject to sales tax in Connecticut under the broader category of computer services. No specific information is available on revenue raised by the tax as applied to Internet access services. (Susan Sherman, Connecticut Revenue and Services Department, personal communication, January 14, 1997.)

<sup>77</sup> Elizabeth Wise, “Nation’s Tax Collectors Eye Internet,” *San Jose Mercury News*, April 12, 1996, p. 1C, citing Scot Greirson, “a California lawyer specializing in on-line taxation.” The report also, but incorrectly, cites New York as imposing sales tax on Internet access services.

<sup>78</sup> A January 12, 1997, article in the *New York Times* (online edition) reported that Internet access service fees are not currently taxed and are to be explicitly exempted from sales tax, after “a yearlong study by the state Department of Taxation and Finance.” (Shannon McCaffrey, “New York Governor Declares Tax Exemption for Net Access.”)

<sup>79</sup> Dennis Fox, California State Board of Equalization, personal communication, October 28, 1996.

state. The court reaffirmed the holding of *National Bellas Hess, Inc. v. Illinois Dept. of Revenue*, 386 U.S. 753 (1967).<sup>80</sup>

But how should the “virtual sales floor” or the “virtual office” now made possible by the Worldwide Web be viewed? When anyone anywhere can connect to a company’s Web site and conduct business online, *where is* that business located? Does accessibility via a Web site constitute a connection between the taxpayer and the taxing jurisdiction (“nexus”)? Is a Web site the functional equivalent of physical presence in every state? Or is it only the functional equivalent of mailing catalogs into every state? These questions, sooner or later, may have to be settled by the Supreme Court, as the Quill decision predated the Worldwide Web as a business medium and does not explicitly address the questions raised by Web-based catalog shopping.

U.S. Senator Dale Bumpers introduced the “Consumer and Mainstreet Protection Act of 1995,” S. 545, to address this issue by mandating payment of sales and use taxes under specified circumstances. Those circumstances would have applied to large national catalog retailers that now, under the Supreme Court’s Quill decision, do not pay such taxes except in states where they have a physical presence. The bill languished in the Senate Finance Committee, never reaching a vote.<sup>81</sup>

The potential stakes in the sales tax battle are large, both for businesses and for taxing jurisdictions. One analysis suggested that in 1994 California lost nearly a half-billion dollars of sales taxes on mail order sales (out of a national total of about 3.3 billion dollars of taxes lost on such sales).<sup>82</sup> The analysis notes that “These two trends, more out-of-state sales [due in part to the Internet] and a greater dependence by local governments on sales taxes, are now on a collision course.”<sup>83</sup> The author concludes:

The reality is that the rise of national and global commerce calls for national and even global solutions, regulations and revenue sources. While much rhetoric around the new technologies hearkens to images of small firms and decentralization, the reality is of rising billion-dollar and soon-to-be trillion dollar corporations straddling the globe. To expect local governments to devise fair and efficient systems of taxation with such a disparity in power is senseless.<sup>84</sup>

---

<sup>80</sup> “1992 Bellsouth Tax Conference, State Tax Update,” Charles R. Beaudrot, Jr., Morris, Manning & Martin. Posted at <http://www.com/mmm/mmmStateTax.html>.

<sup>81</sup> Bill Summary and Status Report, S. 545, via <http://thomas.loc.gov>, September 25, 1996.

<sup>82</sup> This is about 2.8 percent of the approximately \$17 billion in sales and use taxes collected in California that year.

<sup>83</sup> Nathan Newman, “Prop 13 Meets the Internet: How State and Local Government Finances are Becoming Road Kill on the Information Superhighway” (Berkeley: Center for Community Economic Research, UC Berkeley, August 1995; posted on line at the Software Industry site), p. 7. Newman cites figures from the U.S. Advisory Commission on Intergovernmental Relations.

<sup>84</sup> Newman, “Prop 13,” p. 17.

Another analysis emphasizes California's risk from out-of-state mail order and Internet sales:

Ironically, the state most severely hit by the move to catalog and online shopping is California--home to many of the companies and universities that invented the technology that makes the Internet possible. Because of Proposition 13, which limits California's ability to raise money through property taxes, towns and cities are extremely dependent on sales taxes. Cupertino, for example, where Apple Computer has its headquarters, depends on sales taxes for 45 percent of all city revenues, prompting mayor Wally Dean to call the sales-tax dependence "a house of cards for government finances."<sup>85</sup>

Clearly this is an area in transition, and one that will not become easier if online commerce grows substantially and stimulates a large shift from in-state sales to untaxed interstate sales.

### Income Tax and the Web

Does every state have a potential claim to *income* tax from a business on the Web? Each would if the business had an office, warehouse, or employees or other representatives in the state. Each also would if the company "Is doing business in the state," and this does *not* require physical presence, although "rules about what activity will create sufficient nexus vary depending on whether goods or services are being sold."<sup>86</sup>

Although the Internet does not itself create new questions about liability for *individual* state income taxes, it does seem likely to exacerbate existing questions and issues. Could a person in an income-tax-free state work for a company in California, conduct all transactions online, be paid in some form of digital cash, and thereby avoid all state income tax? Could he or she do so as a practical matter only? Or do so legally? Does the use of online communications make any fundamental change from communications conducted by telephone and mail services? These questions will assume real significance only if interstate work and payment becomes common and if the technique is exploited as a means of avoiding or evading tax liability. As long as the practice is rare, not used for tax avoidance or evasion, or both, then it raises no important issue.

Definitions and practices regarding taxes and their applicability vary from state to state, and circumstances come in an enormous variety. Neither a full analysis of tax issues nor a state-by-state comparison can be attempted in this paper.<sup>87</sup> The essential point, and one

---

<sup>85</sup> Nathan Newman, "The Great Internet Tax Drain," *Technology Review*, May/June 1996, as posted on line at <http://web.mit.edu/afs/athena/org/t/techreview/www/articles/mj96/>.

<sup>86</sup> Smedinghoff, *Online Law*, p. 382-3.

<sup>87</sup> There is a Web site devoted to state taxes on electronic commerce (from a software industry perspective): <http://www.SoftwareIndustry.org/issues/lec-sttx.html>.

that may require a follow-up paper to explore, is that the area is complex, full of conflicts, and highly unsettled. The entire area will bear watching.

### **Business and Professional Licensure and Certification**

Many professions are subject to state licensure and certification. In California, these include:

- Lawyers
- Physicians
- Nurses
- Pharmacists
- Psychologists
- Dentists
- Funeral directors and embalmers
- Geologists and geophysicists
- Landscape architects
- Speech and language pathologists
- Structural pest control operators
- Veterinarians
- Accountants
- Architects
- Barbers and cosmetologists
- Contractors

Many of these fields are unlikely candidates for competition over the Internet. Barbers and dentists probably have little to fear (or to gain, for that matter) from the technology. Others fields, however, might well be practiced online, crossing state or even national lines

at will, raising potential questions of licensure and regulation. These fields certainly could include law, accounting, architecture, psychology, and at least some aspects of medicine.

### **Competition with Local Businesses**

Local businesses will increasingly face competition from cyberspace-based businesses, with impacts that cannot readily be determined. While this does not appear to affect government directly, it certainly could have indirect effects if the state or local economy is challenged as a result of Web-based competition. Some of the competition might come from businesses in the same metropolitan area, some from businesses elsewhere in the state, and some from businesses across the country or in foreign nations, depending on the types of products and services involved.

Some types of business (automotive repair shops, pizza parlors, barbershops, plumbing repair businesses, and so on) that provide hands-on service direct to the customer are unlikely to be affected by non-local competitors on the Web. You still cannot download a pizza or a haircut. Other types of businesses (book dealers, clothing stores, hobby and crafts suppliers, and so on) may face stiff competition from entrepreneurs who need not provide a storefront and might even be able to avoid significant inventory costs and sales taxes. These kinds of goods can be shipped to the purchaser in response to orders placed online, and online catalogs and "digital cash" mechanisms will facilitate selection and payment.

Sellers of big-ticket items, such as automobiles, boats, and possibly even major appliances, might be affected by Web-based competition or Web-based comparison shopping services. This could certainly be the case in regions where it is feasible for the products to be delivered economically or for customers to go to where the best deal is.

### **Fraud**

According to the National Fraud Information Center:

Fraudulent commercial activity on the Internet and "online" services is not yet a major problem. However, as use of the Internet expands, there is certain to be a major increase in deceptive and misleading promotions, bogus travel offers, contests, lotteries, and other illegal practices.<sup>88</sup>

The Internet, because of its dispersed nature and frequent lack of known physical addresses for individuals and businesses online, could become a haven for fraud of many types. Some evidence of that has appeared already, although Internet-based fraud is still dwarfed by the traditional types pursued through telephone, mail, and in-person solicitation.

---

<sup>88</sup> National Fraud Information Center, <http://www.fraud.org/tips.htm>, October 30, 1996.



The CyberCop Precinct House, an online anti-fraud effort of the Internet Consumer Action Center (which uses the acronym ICAN in its postings, not ICAC), sees more of a current threat than does the National Fraud Information Center:

The Internet is developing a reputation as the commercial equivalent to an early American western frontier town with few rules and no sheriff to keep the peace. Until now, cyber-citizens have kept order through mutual trust, integrity and self-help when necessary. This approach worked when the Internet was a small community of like-minded individuals.

Today, however, the Internet has grown into a sprawling, rowdy boom town, complete with virtual shopping malls, traffic congestion, e-pollution, and, yes, superhighway-robbers who victimize Internet travelers. Most vulnerable are the growing numbers of new travelers, including many men[,] women[,] and children with little or no online experience.

. . . In addition to well-publicized offenses like defamation, copyright infringement, computer hacking and theft of data, a variety of new consumer abuses may lurk on the horizon. These abuses include misrepresentation, deceptive advertising, fraud, service and pricing abuses, pyramid schemes, and the sale of second-rate or damaged merchandise.

The problem is not so much that the Internet is unregulated, but that no entity is actually monitoring what is going on in Cyberspace.<sup>89</sup>

One recent (Fall of 1996) Internet-aided fraud used e-mail messages as the medium. The scam was designed to produce international phone calls to the British Virgin Islands, generating income for the phone company there. The scam operator sent e-mail messages with a faked return address, threatening some unexplained legal action in the event of failure to respond promptly, and gave a phone number in the 809 area code to call to discuss the matter. The caller is billed \$3 to \$5 for the call (possibly much more), kept on the phone listening to a taped message, and sometimes eventually told that it must be a trick played by the caller's friends and to pass it along to someone else, chain letter fashion.<sup>90</sup> It is not clear what sort of protection there is against this sort of fraud except for a well-developed incredulity on the part of Internet users.

Another type of scam has involved stock sales. According to a report in the *San Francisco Examiner*, "Securities regulators are investigating several cases in which brokers or corporate insiders may have used the Internet last month [May 1996] to

---

<sup>89</sup> CyberCop Precinct House, <http://www.ucan.org/holdcell.htm>. The organization's Web site states, "CyberCop is NOT a public law enforcement agency. In fact, ICAN [its sponsor] does not receive any tax dollars. It is a project of UCAN, a nonprofit membership consumer group based in San Diego, California."

<sup>90</sup> Summarized from Ramon G. McLeod, "Internet Scam Has you Dialing the Caribbean," *San Francisco Chronicle*, October 3, 1996, p. A2.

anonymously tout stock that they were trying to dump . . . .”<sup>91</sup> The Securities and Exchange Commission has published a brochure alerting investors to fraud on the Internet and advising on ways to avoid it. SEC cautions include:<sup>92</sup>

- Be wary of promises of quick profits, offers to share “inside” information, and pressure to invest before you have an opportunity to investigate.
- Be careful of promoters who use “aliases.” Pseudonyms are common on-line, and some salespeople will try to hide their true identity. Look for other promotions by the same person.
- Watch out for offshore scams and investment opportunities in other countries. When you send your money abroad, and something goes wrong, it’s more difficult to find out what happened and to locate your money.

The SEC summarizes, “While investment con-artists have been quick to seize upon on-line computing as a new way to cheat investors, the types of investment fraud seen on-line mirror frauds perpetrated over the phone or through the mail. Consider all offers with skepticism.”<sup>93</sup>

The speed with which messages may move and multiply on the Internet appears to spread investment fraud more quickly than might be expected through print and telemarketing means, but does not change the basic methods.

Standard warnings to users of the Internet include:

- Don’t reveal passwords.
- Be cautious with credit card information or other confidential or sensitive information.
- Purchase only from organizations known to be reliable--know who you are dealing with.
- Report suspicious activity.

These are the same kinds of cautions that consumers should observe when solicited on the telephone or doing business in the local mall, not just on the Internet.

Aggressive con artists online besiege users of America Online and other services with artfully phrased requests for passwords and credit card information, claiming that they

---

<sup>91</sup> Neil Roland, “Regulators probe possible Internet Investment Fraud,” *San Francisco Examiner*, June 14, 1996, p. B1.

<sup>92</sup> Selected from list in “Be Alert For Telltale Signs of On-Line Investment Fraud,” posted at <http://www.sec.gov>.

<sup>93</sup> “Investment Fraud and Abuse Travel to Cyberspace,” posted at <http://www.sec.gov>.

represent the service provider and need the information for validation purposes or to correct some problem with the system.<sup>94</sup> New users (called “newbies”) sometimes fall for these frauds and then find that their accounts have been hijacked.

Even large, legitimate, established companies have been found by consumer protection organizations to have engaged in improper or misleading solicitations for online services. CyberCop, for example, has cited America Online and CompuServe for their “free trial” promotions, which require use of a credit card in order to take advantage of the offer and may make cancellation of the service at the end of the free trial period difficult.

The Council of Better Business Bureaus has announced plans for an online service, endorsed by the Federal Trade Commission, to certify businesses online and to combat online fraud and deception. According to a *Web Week* report on the proposal:

A group of founding sponsor companies, including Hewlett-Packard Co., AT&T, Ameritech, Eastman Kodak Co. and Netscape Communications Corp., have invested a total of about \$2 million to launch the service . . . . In banding together, the group also is sending a signal to federal regulators that self-regulation, rather than restrictive government mandates, can keep the Internet safe for electronic commerce.<sup>95</sup>

Signal or no signal, fraud is fraud, and it seems unlikely that state or federal law enforcement and regulatory agencies will feel comfortable in leaving prevention and enforcement entirely to private initiative, or believe that it is appropriate to do so. Further, private agencies do not have the criminal sanctions that are available to law enforcement agencies.

The key need with respect to law enforcement agencies attempting to cope with Internet-based fraud is *multi-jurisdictional cooperation*. Senior Assistant Attorney General Herschel Elkins is head of the Consumer Law Section of the California Department of Justice, and in that capacity handles fraud complaints. He describes Internet frauds as being the same types as are perpetrated by other means: investment scams, get-rich-quick schemes, advance fee loans, and gambling. Difficulty in determining exactly where a particular scheme originates leads to the need for state attorneys general, the U.S. Department of Justice, Federal Communications Commission, and Federal Trade Commission to cooperate, sometimes along with authorities from other nations.

The National Association of Attorneys General has set up a committee to deal with Internet-related issues. That committee has not yet issued a report. In the meantime, Mr. Elkins feels that “the State of California is doing about all it can now,” although the arrival of digital cash will increase the risk of online fraud. In summary, he added, specific cases

---

<sup>94</sup> I can attest to this from long personal experience. It is an almost constant annoyance on America Online.

<sup>95</sup> Susan Moran, “Better Business Bureau Targets Electronic Fraud,” *Web Week*, August 5, 1996, posted at <http://www.webweek.com>.

require communication among agencies to determine who has jurisdiction and who should file lawsuits or criminal charges.<sup>96</sup>

California state law (*Business and Professions Code*, §17358) provides certain protections for purchasers of goods and services through telephone and mail order. These protections include prompt delivery of merchandise, provisions for notification of delays and refund if preferred by the customer, and various notices to purchasers. Assembly Bill 3320 (Speier, enacted as Chapter 785, Statutes of 1996) extended those protections to purchases made via the Internet. Although these protections cannot eliminate fraud, they do establish standards, define them in the context of the Internet, and make them consistent across the competing sales media.

### **Trademark and Domain Name Disputes**

In brief, “Trademarks [and service marks] are words, symbols, or other devices used to distinguish the goods or services of one person from those of another.”<sup>97</sup> Trademarks and service marks may be words and phrases, graphic designs, letters and numerals, abbreviations and nicknames, and even colors under some circumstances.<sup>98</sup> Internet domain names may now qualify as trademarks, although this is an area that is unsettled at this time, as “a number of problems arise if traditional trademark law is applied to domain names.”<sup>99</sup> The term “service mark” applies to a term or symbol that identifies a *service* rather than tangible *goods*.<sup>100</sup> In the rest of this section, the term “trademark” encompasses both service marks and trademarks.

Unlike copyright (a federal responsibility under the U.S. Constitution, Article I, Section 8), trademark falls under state and federal jurisdiction. California’s law regarding trademarks is §§14200-14214 of the *Business and Professions Code*. A trademark may be registered with the state if it meets the applicable requirements. “Registration of a mark with the Secretary of State under this chapter,” which is effective for 10 years and may be renewed, constitutes “constructive notice of the registrant’s claim of ownership” of the trademark.<sup>101</sup>

The rise of the Internet is affecting the registration, use, and protection of trademarks. The instant worldwide availability of information on the Web places trademarks before national and global audiences, where previously they might be seen only in a relatively small geographic area. Acme Widgets Company’s “AcmeWidget” brand, registered in California as a trademark, might now appear around the world at “www.AcmeWidget.-

---

<sup>96</sup> Herschel Elkins, personal communication, October 31, 1996.

<sup>97</sup> Thomas J. Smedinghoff, ed., *Online Law* (Reading, Massachusetts: Addison-Wesley, 1996), p. 209.

<sup>98</sup> List adapted from *ibid.*, pp. 209-10.

<sup>99</sup> Jonathon Agmon, Stacey Halpern, and David Pauker, “What’s in a Name” (section: “The Relationship Between Domain Names And Trademarks”), posted at <http://www.law.georgetown.edu/lc/internic/-domain1.html>.

<sup>100</sup> See *California Business and Professions Code*, §§14206 and 14207.

<sup>101</sup> *Business and Professions Code*, §§14242 and 14250.

com.” That is, unless some other company has already claimed that domain name or otherwise posted an “AcmeWidget” mark online, in which case multi-jurisdictional litigation may be required to settle the question of who is entitled to use the mark.<sup>102</sup>

Trade *names* pose similar, but not identical issues. The trade name applies to the business, while the trademark applies to the specific product (or if a service mark, to the specific service). It is not uncommon for many businesses to use similar trade names because they are serving different areas or are in different lines of business. There may be a Domino Pizza, a Domino Sugar, and a Domino Software, as the products and services are so different as to have no significant potential for confusion among the public. There may be a Papa John’s Pizza in Dubuque, another in Sacramento, and another in Chicago, each duly registered in the respective state. But there can be only one [www.papajohnpizza.com](http://www.papajohnpizza.com) on the Worldwide Web--and for that matter, only one [www.papajohn.com](http://www.papajohn.com). In these examples, “papajohnpizza” and “papajohn” are *second-level domain names*, in contrast to com, net, edu, mil, and gov, which are top level domain names. Conflicts arise over second-level domain names. Second-level domain names are currently assigned by designated registries, including InterNIC (see Chapter 1, above), under the general oversight of Network Solutions, Inc., which in turn exercises authority granted by the National Science Foundation.<sup>103</sup>

Disputes over second-level domain names include hijacking, reverse hijacking, and legitimate competing claims. In the case of hijacking, someone has acquired a second-level domain name in order to keep someone else from using it or to demand payment for relinquishing it. Reverse hijacking involves a trademark holder’s seeking to take a second-level domain name away from someone else who as a legitimate claim to use it. Legitimate competing claims involve disputes among companies that each have a valid claim on the name (for example, Acme Widgets, Acme Construction, and Acme Foods all claiming [www.acme.com](http://www.acme.com)).<sup>104</sup>

The likelihood of dozens of new top-level domain names, administered by dozens of new organizations, promises to complicate and multiply domain name disputes.

---

<sup>102</sup> Senate Bill 1034, Calderon (1995-96 session), would have prohibited “the unauthorized registration or use of another’s registered trademark as a domain name . . . .” The bill passed the Senate 38-0, but was not voted on by the Assembly.

<sup>103</sup> For more information, see, for example, “Domain Name Registration: Frequently Asked Questions,” posted at <http://rs.internic.net/domain-info/registration-FAQ.html>. Note that FAQ is the commonly used acronym for “frequently asked questions,” basic question-and-answer documents on countless topics on the Internet.

<sup>104</sup> This list is loosely adapted from Jamie Murphy and Brian L. Massey, “Battles over Web Addresses Grow As the Internet Explodes,” *New York Times* (on line), September 11, 1996. Murphy and Massey cite Smedinghoff, who is with the law firm of McBride Baker & Coles, as their source. Agmon, Halpern, and Pauker, cited above, provide information on many domain name disputes.

## Antitrust and the Internet

Although the Internet itself is a decentralized phenomenon not subject to monopoly control, the role of a handful of companies producing Web browsers to access the Internet has raised antitrust issues. Netscape Communications' "Netscape Navigator" software quickly dominated the browser market until the entry of Microsoft Corporation, with its Microsoft Internet Explorer. Because of Microsoft's dominance of the PC operating system market (DOS, Windows, Windows 95, Windows NT) and its huge presence in the market for programming languages and tools, office applications, and home and personal software, it has been a target of concern over possible unfair competition.<sup>105</sup>

When Microsoft released Windows 95, it included its browser software and access to the Microsoft Network, a move that was immediately viewed as anticompetitive. Reaction to that bundling of access with the operating system (and the fact that Windows 95 disabled other Internet access products) forced a retreat, but the company has moved forward with new releases and free distribution of the browser, cutting into Netscape's share of the personal-use market. In August 1996 Netscape Communications filed a request with the Justice Department to investigate possible anticompetitive practices by Microsoft in connection with its Worldwide Web-related activities, questioning whether the company had violated an existing antitrust agreement. Netscape charged Microsoft with "a wide variety of predatory pricing and bundling behavior that violates the antitrust laws."<sup>106</sup>

It seems likely that the U.S. Department of Justice will be sensitive to potentially anti-competitive activities and that Microsoft's competitors will continue to seek federal intervention if they deem that necessary. Competitors are also forming alliances to counterbalance Microsoft's influence.

## Telecommunications Regulation

Telephone companies and services are regulated by the states and by the federal government. Interstate aspects are under the jurisdiction of the Federal Communications Commission (FCC), and within California regulation is the responsibility of the Public Utilities Commission (PUC).<sup>107</sup>

In brief, "The [California Public Utilities] Commission has dual jurisdiction with the Federal Communications Commission ('FCC') over California LECs [local exchange carriers--local phone companies]. The CPUC has jurisdiction over *intrastate* matters and

---

<sup>105</sup> For a readable, if opinionated, review of assertions about Microsoft, see James Gleick, "Making Microsoft Safe for Capitalism," *New York Times Magazine*, November 5, 1995, and posted at <http://www.around.com/microsoft.html> (this is on Gleick's Web site).

<sup>106</sup> Netscape's long and detailed letter detailing its claims against Microsoft has been posted on line, including at <http://radon.gas.uug.arizona.edu/~bernster/netletter.html>.

<sup>107</sup> For an overview, see California Public Utilities Commission, Commission Advisory and Compliance Division, Telecommunications Branch, "Telecommunications Regulation in California: A Primer," May 1995.

the FCC handles *interstate* matters. The FCC's jurisdiction applies to the extent that LECs provide access to interstate services. Both jurisdictions impose requirements with which the LECs must comply."<sup>108</sup> Federal telecommunications law was overhauled by the Telecommunications Act of 1996, many provisions of which are yet to be filled out in regulation, are under litigation, or both.

Local exchange carriers in California range from giant Pacific Bell, with over 15 million lines, to Pinnacles, with about 200. Pacific Bell and GTE California (about 3.9 million lines after merger with Contel) account for nearly 99 percent of all telephone access lines in California.<sup>109</sup>

Neither the FCC nor the California PUC regulates Internet access services as such. The PUC has no plans to do so, as "Internet access is completely competitive," according to one staff member. Another PUC staff member confirmed that ISPs simply provide a service over the phone lines, but are not an element of the regulated telecommunications industry. Regulation affects Pacific Bell and other telephone service providers (some of which have begun to provide Internet access services not subject to rate-setting by PUC), and there is no apparent statutory authority to regulate ISPs, nor any apparent potential benefit in doing so.<sup>110</sup>

There may, however, be reason for the PUC to evaluate the impact of Internet access services on local phone loops, to determine whether some regulatory response is required to congestion generated by lengthy Internet access calls. This issue is explored in the next section.

### **The Load on the Phone System**

Recent press reports have cited telephone industry assertions that POTS is threatened by growing dial-up Internet access.<sup>111</sup> The problem is that calls to Internet service providers are much longer than typical phone calls, averaging nearly 21 minutes, compared to under 4 minutes. Some Internet calls last for hours, and some for days.<sup>112</sup> Once the call reaches

---

<sup>108</sup> *Ibid.*, p. 2.

<sup>109</sup> Condensed from *ibid.*, p. 1.

<sup>110</sup> Personal communication, October 29, 1996, with PUC staff members who wished not to be quoted directly. The Public Utilities Commission has adopted standards for "universal access" to telecommunications services, although the PUC's definition of that term does not yet include Internet access. The Federal Communications Commission on November 8, 1996, issued a massive "recommended decision" regarding universal access that touches on Internet access, but that decision came too late for review for this paper. A follow-up paper by the California Research Bureau will examine state and federal universal service requirements and proposals and their relevance to Internet services.

<sup>111</sup> For example: "Soaring Internet usage threatens to create gridlock in American phone system, *Nando Times* (from Reuter Information Service), October 29, 1996; Simson Garfinkel (technology columnist), "PhoneCrash: Who will pay to prevent the Internet from killing the national phone system?", <http://www.packet.com>). Similar reports also appeared in the *Sacramento Bee*, *San Jose Mercury News*, and *Los Angeles Times*.

<sup>112</sup> Days-long dial-up Internet connections are probably very rare, as services typically disconnect the user after 15 minutes of idleness.

the ISP it is handed off to a data network and leaves the voice telephone system (although data may travel over lines owned or leased by long-distance phone carriers). It is the lengthy use of the local loop (local exchange phone line) en route to the ISP that is overloading switch capacity. That problem affects local phone services, not long-distance carriers.

According to one news report, "PacTel [Pacific Telephone] said a study of one Silicon Valley telephone switch showed 16 percent of call attempts failed during peak evening hours because of Internet traffic, and 2.5 percent of lines used by Internet service companies absorbed 20 to 36 percent of the switch's capacity."<sup>113</sup> Added capacity reduced the level of failed connect attempts to 1 percent, although some areas in Los Angeles are at risk of similar congestion.<sup>114</sup>

Long-distance telephone carriers, such as AT&T and Sprint, pay an access charge to local phone companies for calls from and to the local company (called a local exchange carrier, LEC).<sup>115</sup> Online service providers, however, are exempted from access charge provisions:

Back in the early 1980s, just before online services started taking off, the FCC issued an order giving online firms a "temporary exemption" from telco access charges. The rationale was that access charges would have added significantly to the cost of online access--more than \$2 an hour (access charges were higher then)--and could have kept the industry from getting off the ground.<sup>116</sup>

A 1987 FCC finding that the exemption was no longer necessary died under a hail of opposition from online service users. The telcos sought reopening of the case for online service access charges as a means of funding system improvements to handle the load generated by Internet dial-up access. In December 1996, the FCC explicitly declined to levy access charges on Internet service providers and other data networks, although it may revisit the issue in the future.

Complicating the question of access charges for Internet access is that the telcos themselves have entered the Internet access field. Pacific Telesis has an Internet subsidiary (Pacific Bell Internet Services), which offers dial-up access via numerous POPs in California. Pacific Bell has even offered 5 months of free, unlimited dial-up Internet access for subscribers buying a second home phone line (which will also be provided at a discounted

---

<sup>113</sup> "Soaring Internet Usage."

<sup>114</sup> "Surging Internet Use Strains Phone System," *Los Angeles Times*, October 31, 1996, p. A1.

<sup>115</sup> "Access payments to LECs are approximately 45% of IXCs' cost of providing long distance services," according to Mark A. Jamison, Manager, Regulatory Policy and Coordination, Sprint Communications, in "A Competitive Framework for Pricing Interconnection in a Global Telecommunications Market," posted at <http://www.sprint.com/analyst/paper>, and originally published in the *Denver Journal of International Law and Policy*, Vol. 23 No. 3, Summer 1995, pp. 513-33.

<sup>116</sup> Garfinkel, "PhoneCrash."



rate).<sup>117</sup> This would seem to aggravate the problem of local loop congestion, especially as a second line would likely be used for longer Internet-access calls than would a homeowner's single line, which would also be needed for regular phone calls.<sup>118</sup>

AT&T is also an ISP (so is long-distance carrier MCI). The long-distance carriers pay access charges in connection with their phone services, but not their packet-switched data services. Technology columnist Simson Garfinkel quotes Mike Miller, speaking on behalf of AT&T, as saying:

We believe that the access charges that the local exchange companies are charging are really exorbitant. They are way above cost and need to be brought down. We think that when the local exchanges bring down the access charges to a more reasonable level, something approaching costs, then that is the time to look at bringing the access fees for the data circuits into line with the other charges.<sup>119</sup>

Small ISPs are nervous about proposals for fees on their operations to fund telco expansion and upgrading to cope with the dial-up Internet access load, viewing the proposals as anticompetitive.<sup>120</sup>

There may be alternative solutions. Details are beyond the scope of this paper, but one is worth mentioning:

. . . perhaps the most interesting suggestion is to have phone companies reprogram their switches to recognize the phone numbers of popular online service providers in each metropolitan area. Instead of sending the calls through to the provider's central office, the phone company would send them to a special modem bank that the telco would operate at each exchange. The phone company could then run the data over its own packet-switched data network to the particular online service provider for which the phone call was originally destined. Consumers would never see a difference.<sup>121</sup>

---

<sup>117</sup> This offer was made via a flyer sent to Pacific Bell customers. A single month of free unlimited access is advertised at the Pacific Bell Web site, <http://www.kn.pacbell.com>. The notice there describes a \$20 per month flat-rate dial-up service available "in over 350 communities in four key regions of the state-- Sacramento, San Francisco, Los Angeles and San Diego." Access for Fresno, Stockton, and other metropolitan areas in the state is to be added by 1997, according to the notice. Pacific Bell also offers a less-expensive option with limited hours per month. (Strictly speaking, Pacific Bell Internet Services is a wholly-owned subsidiary of Pacific Bell, not a division or department.)

<sup>118</sup> Pacific Bell, Pacific Bell Internet, and Bellcore did not respond to inquiries on this issue.

<sup>119</sup> Garfinkel, "Phone Crash."

<sup>120</sup> This opinion was offered by the president of a Sacramento-area ISP.

<sup>121</sup> Garfinkel, "Phone Crash."

Although this is feasible now, according to Simson Garfinkel, it would still involve costs that phone companies are unlikely to want to absorb.<sup>122</sup>

It does seem clear that the question of Internet's impact on local phone services will have to be addressed somehow. Some estimates suggest that 8 percent of California households currently have Internet access. If that percentage doubles over the coming year, and doubles again over the next year, it will reach nearly a third of households, and the impact on the telcos will grow accordingly.

As if this were not already complicated enough, long-distance carriers, too, face Internet-related issues. It is now possible to conduct telephone conversations via the Internet without incurring long-distance charges.<sup>123</sup> Voice signals are converted by hardware and software into digital signals, conveyed to and across the Internet in the same manner as text and other types of data files, and reconverted into voice at the receiving end. The only requirement is that sender and receiver have compatible systems. If they do, they can carry on conversations, possibly with somewhat reduced sound quality, just as if they were local calls or as if they were text messages exchanged across the system. Internet telephony can span not only the nation, but the world. Internet telephony hardware and software vendors are competing actively in this market, although there is not yet a single standard for the service.

If Internet access continues to spread and if use of Internet telephony becomes common, the impact on long-distance carriers could be profound, and that impact could in turn affect local telephone companies that would lose access fees from long-distance telephone carriers.

### **Online Commerce at Risk from Power Failures**

In addition to the threat posed by congestion on the Internet, recent widespread power outages in the West underline the risks of growing dependence on a medium that is crippled when the power is out. A power failure in one part of the country can now affect communications and commercial activity in the entire country and around the world. Bear in mind that the telephone system usually continues to function during power outages, as

---

<sup>122</sup> Whether they could absorb them is another question. Pacific Telesis Group's sales for 1995 totaled \$9.042 billion, with net income of \$1.048 billion. Data at <http://www.hoovers.com>.

<sup>123</sup> This development has been widely covered in the press. See for example: "Internet users discover toll-free long distance calls," *Nando Times* (carrying a Scripps-McClatchy Western report), [http://www.nando.net/newsroom/ntn/info/110696/info6\\_12940.html](http://www.nando.net/newsroom/ntn/info/110696/info6_12940.html); Gus Venditto, "Internet Phones--The Future is Calling," *Internet World*, June 1996; "Wrestling over the Future," *U.S. News and World Report*, April 15, 1996 (as posted at <http://www.usnews.com>). The issue of Internet telephony is also before the FCC, raised by a petition from the America's Carriers Telecommunications Association. A response that petition, posted by a group of Internet telephony providers, is posted at the Voice on the Net (VON) Coalition site, <http://www.von.org/reply.html>. Long-distance carrier (and "world's largest carrier of Internet traffic") Sprint is a member of the VON Coalition, according to a June 19, 1996 VON press release.

copper phone lines also carry the power needed to make phones usable.<sup>124</sup> If network connections fail or if servers are down on account of power failure, however, the fact that consumers' telephone connections still work will still not get around that failure.

*Boardwatch*'s Jack Rickard, in his review of Internet architecture, suggested that "there is a fear that somewhere in the Internet there is a single router that all of this hangs on such that one power hiccup and the entire network takes a tumble."<sup>125</sup> Among the possible consequences of a power failure in a network-dependent commercial world are:

- Business Web sites could become unavailable, leading to deferred or lost sales.
- Individual users, possibly over a wide area, might be unable to access *any* online services, whether information, financial, commercial, or other.
- Corporate users could lose access to e-mail and electronic data interchange across the Internet, interfering with operations.
- Government information sites on the Internet could become inaccessible, with potential result of swamped telephone lines to offices, inaccessibility of services, or both.

The scope of such problems is a factor of the scope and location of any power failure. In an internetworked world, however, a service interruption in, say, San Francisco, could affect users around the world no matter how well their power supply is holding up.

As if to illustrate, the day after the discussion above was written there was such a failure at the campus of Stanford University, possibly the result of rats in a generator ("Workers found two rats, crisp and dead," according to one report). The power failure cut off lines to BBN Corporation, a major Internet access provider. Among the sites affected were those of the *Los Angeles Times*, various technology companies, the University of California at Berkeley, and Stanford University.<sup>126</sup> This is one example of a local power failure affecting worldwide access to prominent Web sites.

---

<sup>124</sup> This does raise the technical issue, beyond the scope of this paper, that slow, copper "twisted pair" phone wiring carries power, while fiberoptic cables do not unless equipped with supplementary wiring to conduct power. This is a point that must be considered during any conversion of last mile systems to fiberoptic.

<sup>125</sup> Rickard, "Internet Architecture" (online version, as printed), pp. 8-9.

<sup>126</sup> Dan Reed, Mike Langberg, and Jennifer Mena, "Stanford blackout shuts off Net Access," *San Jose Mercury News* (online edition), October 12, 1996, and "West Coast Sites Darkened by BBN Power Outage" (Reuters), *New York Times* (online edition), October 12, 1996. The "crispy rats" quote is from the *Mercury News* article.