

The State of the Law on Cyberjurisdiction and Cybercrime on the Internet

Prepared by: Gabriole Zeviar-Geese [*]

California Pacific School of Law

It is in this digital soup, this is a hyper-relational environment, that we see the death of the barrier. . . . What we do have is the network and the death of dichotomy. This is fatal for the legal system, which depends for its very life on the existence of barriers- after all, that's what the law does: it utters the line between this and that, and punishes the transgressor.

Curtis E.A. Karnow [1]

INTRODUCTION

THE ARCHITECTURE OF CYBERSPACE

I. CYBERCRIME

A. The Scope of Cybercrime

B. The Types of Cybercrime

1. Fraud

2. Forgery

3. Computer Sabotage

4. Unauthorized Access to Computer Services or Systems

5. Unauthorized Copying of Computer Programs

6. Cyberstalking

C. The Cybercriminal

II. CYBERJURISDICTION

A. Cyberjurisdiction in Civil Cases

B. Minnesota's Internet Warning: Signpost of the Future

C. Cyberjurisdiction in Criminal Cases

D. Cyberjurisdiction in International Cases

III. CONCLUSION

INTRODUCTION

With the advent of the Internet, cyberlaw has become an emerging field. Cyberlaw encompasses cybercrime, electronic commerce, freedom of expression, intellectual property rights, jurisdiction and choice of law, and privacy rights. [2] Cybercrime involves activities like credit card fraud, unauthorized access to computer systems, child pornography, software piracy and cyberstalking. [3] Electronic commerce includes with encryption and data security. [4] Freedom of expression includes defamation, obscenity issues and censorship. [5] Intellectual property rights covers copyright, software licensing and trademark protection. [6] Jurisdiction focuses on who makes and enforces the rules governing cyberspace. [7] Privacy rights addresses data protection and privacy on the Internet. [8]

There are many issues to be resolved in Cyberlaw. Two areas of cyberlaw requiring further clarification are cybercrime and jurisdiction. For example, in cyberlaw there are only a limited number of cases on point and no major statutory schemes on the books. Policy makers and attorneys dealing with cybercrime are often confined to referring to the imprecisely applicable, and scarce existing statutes and cases. [9] In cyberjurisdiction, the Courts must address the question of which law-maker has jurisdiction over actions taking place on the Internet. In the few cases the Courts have adjudicated they have applied long-arm statutes and personal jurisdictional principals in making decisions. Due to the paucity of cyberjurisdiction cases there is a limited amount of law for the legal practitioner to reference.

The purpose of this article is threefold. First, to give an overview of the Internet by discussing its history, how it works, and the different ways users can communicate over it. Second, to briefly examine cybercrime by looking at its scope, the types of crimes typically committed and the kind of person who commits cybercrime. Third, to examine how cyberjurisdiction is resolved in civil, criminal and international cases with the view toward understanding jurisdictional issues in cybercrime cases.

THE ARCHITECTURE OF CYBERSPACE

The Internet is a term that describes the global connection of interconnected computer networks [10] spanning state and national borders. [11] The notion of interconnecting computers originally began in 1969 as part of a military program called "ARPANET." [12]

ARPANET was designed to enable the military, defense contractors and academics conducting defense related research to communicate with each other through alternate channels. This redundancy was created to ensure that communications could continue even if part of the network was damaged in war. ARPANET has provided the foundational design for the development of many of the civilian networks used to enable millions of people to communicate with one other and to access information from all over the world. [13]

In the last decade the Internet has undergone considerable expansion. In 1994 there were an estimated 21,000 connected networks in over 60 countries with 15 million users, and

an expected growth rate of 7 to 10 percent per month. [14] Today it is estimated that there are over 9.4 million computers and as many as 40 million people worldwide linked to the Internet. [15] It is projected by the end of this century there could be over 200 million Internet users. [16]

Access to the Internet is available to users through a wide variety of communication and information retrieval methods. Popular access methods are E-mail, mail exploders, newsgroups, chatrooms and the World Wide Web. Via E-mail users can send an electronic message to another user or to a group of users. Upon receipt of the E-mail message, the message is stored electronically in the user's mailbox to be read immediately or at a later time. [17]

A mail exploder is like an E-mail group where subscribers can send messages to a common E-mail address. The messages are then forwarded to each of the group's subscribers. [18]

A newsgroup can be seen as an online discussion group where there are tens of thousands of discussion areas each focusing on a specific topic. Newsgroups are arranged into hierarchies such as comp (computers), soc (social issues), or sci (science). Each hierarchy is divided into branches and sometimes into subbranches. [19]

Chatrooms are common areas in cyberspace where users can engage in real time dialogue by sending E-mail messages that can be read by anyone in the chatroom or on a one-on-one basis. [20] Recent technical developments enable users to move beyond the limitations of chat rooms to include real-time voice communication between users anywhere in the world via the Internet. [21]

All of these methods can be used to transmit text. Most of these methods can also transmit pictures, sound and video images. In aggregate, these methods create a unique medium known as cyberspace. [22]

A Uniform Resource Locator ("URL") is used by browsers [23] to locate an item on the Internet. A URL can reference a Web site, a sound file, a graphic image, or a Web page. URLs consist of five elements. The first element is the protocol to use to access the Internet site. The second element is the Web server's name. The third element is the path to locate the item on the Web server. A path can consist of one or more slash separated directory names. The fourth element is the file name. The fifth element is the anchor name. Anchor names are used to reference a specific location within a long Web page. [24]

Sending E-mail on the Internet requires a different addressing format from URL. E-mail addresses contain four elements. [25] The typical address, however, consists of three elements. The first is the user's Internet account name. The second is the host or domain name. (Whereby, the host name is the name of the computer that contains the Internet account and the domain name is the name of the network to which the host computer is connected.) The third is the top-level domain. International E-mail contains a fourth

element, the abbreviation of the country in place of or in addition to the top-level domain name.

The World Wide Web ("WWW") has been defined as a vast collection of documents stored on Internet computers. [26] Actually, the Web is only a part of the Internet, but its name has become so popular that many new users believe that the Web is the Internet. [27] From a technical standpoint the Web is an information presentation system. [28] The Web was begun by Tim Berners-Lee while working at CERN, the European Laboratory for Particle Physics. He started the WWW project with the purpose of building a distributed hypermedia system. Berners-Lee has continued his work with the W3 Consortium at the Massachusetts Institute of Technology. [29]

A Web site consists of one or more Web pages created by an individual or an organization residing on a Web server. [30] Web pages can have one of two characteristics. A Web page can either restrict users to viewing a Web page or it can be interactive and allow users to read and/or update fields on the Web page. [31] Two examples of an interactive Web page are a questionnaire or an order form.

Web documents or Web pages have two important characteristics. First, they contain icons or links (consisting of either blue or underlined text) that can be clicked on to access other Web pages. [32] These links can point to other portions of the same Web page, to other pages on the same Web server or to pages on a computer located anywhere in the world. Second, they can contain sound, graphics, animation, and/or other multimedia elements. [33]

I. CYBERCRIME

The definition of what constitutes a crime on the Internet is still being developed. In the past, the states and federal government have defined cybercrime activities to include the destruction or theft of computer data and programs to be computer crime. More recently, the definition has expanded to include activities such as forgery, illegal gambling, and cyberstalking. [34]

Both the states and Federal government have laws addressing cybercrime. Cybercrime is being prosecuted under statutes similar to California's penal code dealing with unauthorized access to computers, computer systems and computer data [35] or New York's computer crime law. [36] Both statutes address tampering, interfering, damaging or unauthorized access to computer data and computer systems. The Federal government's computer crime statute, 18 U.S.C. sect. 1030 (1995), proscribes the unauthorized use of certain computers and the alteration or destruction of the records they contain.

The development of cybercrime laws has not been without controversy. In 1996, the Federal government enacted a statute dealing with pornography on the Internet. [37] In the first Internet-related U.S. Supreme Court case, *Janet Reno v. American Civil Liberties*

Union, [38] the Court held that certain provisions of the Communications Decency Act [39] were unconstitutional under the First Amendment.

A. The Scope of Cybercrime

In 1987 the American Bar Association conducted a survey of three hundred corporations and government agencies regarding the extent of computer crime and their resulting losses. Seventy-two of the respondents claimed to be the victim of computer-related crime within the past twelve months, experiencing losses estimated to range from \$145 million to \$730 million. [40]

In 1991, a survey of computer related crime of 3,000 Virtual Address Extension sites in the United States, Canada, and Europe was conducted. Eight percent of the respondents were uncertain whether they had experienced a breach of security. Forty-three percent of the respondents said they experienced a security incident that had been a criminal offense. Seventy-two percent of the those who responded said they had been the victim of computer-related crime within the past twelve months. [41]

In October, 1992, at the international level, the Association Internationale de Droit Penal ("AIDP") held The Colloquium on Computer Crimes and Other Crimes against Information Technology in Wartzburg, Germany. The AIDP released its report on computer crime at the conference. The report was based on other reports received from its member countries. The report stated that less than five per cent of computer crime was being reported to law enforcement authorities. [42]

There are several reasons by computer crime statistics do not reflect the true scope of computer crime. Criminologists use the term "dark figure" to refer to undiscovered computer crimes. Several factors contribute to this dark figure. First, the operational speeds and storage capacity of computer hardware makes criminal activity very difficult to detect. Second, law enforcement officials often lack the necessary technical expertise to deal with criminal activity in the data processing environment. Third, many victims of computer crime have failed to create contingency plans to deal with computer crime. Fourth, once criminal activity has

been detected, many businesses have been reluctant to report criminal activity because of fear of adverse publicity, loss of goodwill, embarrassment, loss of public confidence, investor loss, or economic repercussions.[43]

B. The Types of Cybercrime

The definition of cybercrime is under development with much debate among experts centering on what constitutes a computer crime or computer-related crime. [44] Computer crime involves traditional activities such as fraud, theft or forgery. It can include the more recent crime of cyberstalking. It can even extend to activities not considered criminal in one jurisdiction, yet be proscribed and punished in another jurisdiction. [45]

Examples of the sorts of activities that are considered cybercrime can be found in The "United Nations Manual on the Prevention and Control of Computer-Related Crime." [46] The manual includes fraud, forgery, computer sabotage, unauthorized access, and copying of computer programs as examples of computer crime.

1. Fraud

Organized crime has used cyberspace to target credit card information, personal and financial information for computer fraud. The sale of this information to counterfeiters of credit cards has proven to be extremely profitable. No longer do bank or credit cards need to be stolen. Counterfeiters using specialized computer hardware and software programs can encode falsified information on credit and bank card magnetic strips. [47] The sale of personal and financial information to create false travel documents has also become big business. [48]

Fraudulent activity has extended to the Internet in the form of fake franchise offerings. In April, 1997 the Federal Trade Commission and the North American Securities Administrators Association, both involved in investigating fraud on the Internet, sent notices to over two hundred Web sites which offer business opportunities, warning them that state and federal laws required them to be able to substantiate their earnings claims. [49]

2. Forgery

Computer forgery is the alteration of computerized documents. Since the advent of high-resolution computerized color laser copiers a new generation of fraudulent counterfeiting has emerged. [50] These copiers can modify existing documents the quality of which is indistinguishable from the original without referring to an expert for analysis. The perpetrators can even create false documents without the necessity of referring to an original document. [51]

3. Computer Sabotage

The use of the Internet to hinder the normal functioning of a computer system through the introduction of worms [52], viruses [53], or logic bombs [54] is referred to as computer sabotage. [55] Computer sabotage can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists, or to steal data or programs for extortion purposes. [56]

In April, 1997 the U.S. Department of Energy Computer Incident Advisory Capability Unit announced that a highly dangerous Trojan horse program capable of deleting all of a user's hard disk files was circulating on the Internet. The program was masquerading as AOL4free.com. Its victims were tricked into believing it was a program allowing them to create fraudulent accounts on America Online. [57]

In another Internet Trojan horse warning, in August, 1997 AOL warned its online users of a program pretending to be from the AOL Keyword List Area. A user with the screen name KEY List2 sent mail out to some users with an attached file pretending to be the keyword LIST. The purpose of this program was to sniff out user passwords. [58]

4. Unauthorized Access to Computer Services or Systems

Unauthorized access to a computer system can be motivated by a computer hacker's curiosity or perhaps by a desire to sabotage the computer system. Hackers frequently impersonate the system administrator using default maintenance passwords, which the real system administrator failed to change, to break into the system. The modern hacker can bypass existing system password protection by creating a Trojan horse program to capture the passwords of legitimate users of the system. [59]

5. Unauthorized Copying of Computer Programs

The unauthorized copying and distribution of computer programs can cause considerable economic loss to the legitimate owners. [60] Several jurisdictions have dictated that this activity should be subject to criminal sanctions. In *U.S. v. David LaMacchia*, Crim. A. No. 94-10092-RGS, U.S. Dist. (D. Mass. Dec. 28, 1994), the court declined to hold the defendant liable under the wire fraud statute [61] because his infringement activities of distributing computer software did not result in a profit. The court went on to rule that criminal and civil penalties should attach to defendants involved in wilful, multiple infringements of copyrighted software, even if the infringer lacked commercial motive. The court left it to the legislature to define the crime and to establish the penalty. [62]

6. Cyberstalking

Cyberstalking refers to the activity of users sending harassing or threatening E-mail to other users. Women are especially being targeted by cyberstalkers. For example, a South Carolina woman has been stalked for several years via E-mail by an unknown person who has threatened her life, threatened to rape her daughter, and posted her home address on E-mail making it openly available to anyone with access to the Internet. [63] It has been estimated that approximately 200,000 people stalk someone each year. [64] California was the first state to pass a stalking law. [65] Seven states have passed statutes that include stalking by computer. [66]

C. The Cybercriminal

Students, terrorists, amateurs and members of organized crime have been involved in cybercrime. The most prevalent source of computer criminals are inhouse. Over ninety percent of economic computer crimes are perpetrated by a company's own employees. [67] The motivation of cybercriminals typically involves revenge, a desire for notoriety, the technical challenge, monetary gain, or the promotion of ideology. [68] Cybercriminals ages range from ten to sixty years. Their computer skills run from novice to professional level. [69]

II. CYBERJURISDICTION

The Internet can be seen as multi-jurisdictional because of the ease which a user can access a Web site anywhere in the world. It can even be viewed as a-jurisdictional in the sense that from the user's perspective state and national borders are essentially transparent. [70] For courts determining jurisdiction, however, this situation is more problematic. The court in *Zippo Mfg. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D.Pa. 1997) said there is a global revolution looming on the horizon, and the development of the law in dealing with the allowable scope of personal jurisdiction based on Internet use is in its infancy. *Id.* at 1123.

The developing law of jurisdiction must address whether a particular event in Cyberspace is controlled by the laws of the state or country where the Website is located, by the laws of the state or country where the Internet service provider is located, by the laws of the state or country where the user is located, or perhaps by all of these laws. [71] A number of commentators have voiced the notion that cyberspace should be treated as a separate jurisdiction. [72] In practice, this view has not been supported by the Courts or addressed by lawmakers.

Cyberjurisdictional issues have been dealt with primarily in the civil courts. Since the advent of *U.S. v. Thomas, infra*, and *Minnesota v. Granite Gate Resorts, Inc, infra*, however, cyberjurisdiction issues have begun to be examined in criminal courts as well.

A. Cyberjurisdiction in Civil Cases

In determining whether jurisdiction exists over a defendant, the U.S. Federal courts apply the law of the forum state, subject to the limits of the Due Process Clause of the Fourteenth Amendment. [73]

However, other issues dealing with cyberjurisdiction remain unsettled. For example, the United States District Court of Connecticut held that the continuous availability of an Internet advertisement containing an 800 number was enough to establish jurisdiction while the United States District Court of Southern District of New York held that having an Internet advertisement containing an 800 number was not enough to establish jurisdiction.

In *Bensusan Restaurant Corp. v. King*, 937 F.Supp. 295, (S.D.N.Y. 1996), the plaintiff, operator of the New York jazz club The Blue Note, complained that the defendant had infringed on its rights by using its trademark. Defendant, owner and operator of a small club called The Blue Note, in Columbia, Missouri, had created a Web page which allowed users to order tickets to attend the club's shows. The court had to decide whether the creation of a Web site in Missouri containing a telephone number was an offer to sell to citizens in New York.

The defendant argued the court lacked personal jurisdiction under New York's long-arm statute. He defended that all he had done was set up a Web site in Missouri aimed at

Missouri residents. Furthermore, any tickets sold over the Internet to users had to be picked up either at ticket outlets in Columbia, Missouri, or at the club on the night of the show.

The court agreed finding that it took several affirmative steps to obtain access to the Web site and use the information there. *Id.* at 299. The court also ruled that there was no proof that the defendant had directed any infringing activity at New York. *Id.* The court held that merely because someone can access information on the Internet about an allegedly infringing product, it is not equivalent to a person selling, advertising, promoting or otherwise attempting to target that product in New York. *Id.*

Under Due Process, in order for the court to exercise personal jurisdiction, it must be shown that the defendant had purposefully established minimum contact with the forum state such that the maintenance of the suit did not offend the traditional notions of fair play and substantial justice. [74] The court ruled that the defendant's simple creation of a Web site, that was available to any user who can find it on Internet, was not an act of purposeful availment of the benefits of the state of New York. [75] Creating a Web site was similar to placing a product into the stream of commerce. The Web site's effect may be felt nationally or even internationally, but this without more, was not enough to establish an act that was purposefully directed toward the forum state. [76] Based on these rulings the Court held that an exercise of personal jurisdiction would violate the protections of the Due Process Clause. [77]

Inset Systems, Inc. v. Instruction Set, Inc., 937 F.Supp. 161 (D.Conn. 1996), is a case where Inset Systems, Inc. ("Inset"), a Connecticut corporation, discovered that Instruction Set, Inc. ("ISI") a Massachusetts corporation, had infringed on its trademark

by using the domain address INSET.COM and the telephone number 1-800-US-INSET. ISI moved to dismiss for lack of personal jurisdiction and improper venue. In order to determine jurisdiction the Court had to satisfy the solicitation of business provision of Connecticut's long-arm statute and determine whether ISI had sufficient minimum contacts with the forum state to support the exercise of personal jurisdiction.

Inset contended that Connecticut's long-arm statute conferred jurisdiction over ISI because of its Internet advertisement and the availability of its 800 number. The court agreed and relied upon *McFaddin v. National Executive Search, Inc.*, 354 F.Supp. 1166, 1169 (D.Conn. 1973), and *Whelen Eng'g Co. v. Tomar Elecs.*, 672 F.Supp. 659 (D.Conn. 1987), to establish that ISI's advertising over the Internet was solicitation of a sufficient repetitive nature to satisfy Connecticut's long-arm statute.

The court ruled that ISI had been advertising continuously over the Internet to the over 10,000 access sites located in Connecticut. The court also ruled that Internet advertising was not like hard-copy advertisements that had a limited reach and which were normally thrown away after use. Internet advertisements were persistent in nature allowing them to be accessed again and again by a large number of potential readers. [78] The court held

that because of the continuous availability of the advertisement on the Internet the defendant was subject to Connecticut's long-arm jurisdiction. [79]

In order to meet Due Process requirements the court had to satisfy two tests. First, that a nonresident corporate defendant have minimum contacts with the forum state such that it would reasonably anticipate being haled into court. *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 [100 S.Ct. 559, 567, 62 L.Ed.2d 490] (1980). Second, that maintenance of the suit in the forum state would not offend traditional notions of fair play and substantial justice. *International Shoe Co. v. Washington*, 326 U.S. 310, 316 [66 S.Ct. 154, 158, 90 L.Ed. 95] (1945).

ISI claimed that minimum contacts was lacking. ISI said it did not conduct business in Connecticut on a regular basis, it did not maintain an office in the state, nor did it have a sales force or employees in the State. Accordingly, ISI argued, the court should find that the minimum contacts test was not satisfied.

Disagreeing, the court ruled that ISI purposefully directed its advertising activities toward Connecticut on a continuing basis by posting its toll-free number on the Internet and directing its advertising activities toward both the state of Connecticut and to the entire United States since March 1995. *Id.* at 164. These actions led the Court to rule ISI had purposefully availed itself of the privilege of doing business by establishing minimum contacts within the state. Consequently, the court reasoned ISI could reasonably anticipate the possibility of being haled into court. *Id.* at 165. Thus, the court held that Due Process was satisfied, and that assertion of jurisdiction did not offend the notions of fair play and substantial justice. In support of its holding, it ruled that the relative burdens on the defendant were not unreasonable. The travel time between the defendant and the location of the suit was less than two hours and that the defendant had already retained counsel within the forum state. *Id.*

Not all commentators agree with the holding of *Inset Systems*, because of the consequences of its logic. Their concern is that if the courts followed *Inset Systems*, the implications are that there would be nationwide, even worldwide jurisdiction over anyone and everyone who created a Web page on the Internet. [80]

Declining to follow *Inset Systems*, the U.S. District Court of the Southern District of New York in *The Hearst Corp. v. Goldberger*, 1997 WL 97097 (1997), ruled that nationwide jurisdiction was inconsistent with traditional personal jurisdiction case law, and as a policy matter it was unacceptable. [81]

In *McDonough v. Fallon McElligott, Inc.*, 1996 U.S. Dist. LEXIS 15139, No. 95-4037, slip op. (S.D.Cal. Aug. 6, 1996), a federal court in California also refused to exercise personal jurisdiction over the defendant simply because it maintained a Web site. The court held that the fact that the defendant had a Web site accessed by Californians was not enough by itself to establish jurisdiction.

In a 1994 case, a plaintiff attempted to extend personal jurisdiction to include users of the Internet. The court in *Pres-Kap, Inc. v. System One, Direct Access, Inc.*, 636 So.2d 1351 (Fla.App. 1994), *review denied*, 645 So.2d 455 (Fla. 1994), refused to exercise jurisdiction over a consumer of an on-line airline ticketing service. The case involved a suit on a contract dispute in a Florida court by a Delaware corporation against its New York customer. Defendant, a travel agent, only contact with the forum state was accessing plaintiff's airline reservation system data base by logging onto plaintiff's computer located in Florida and forwarding rental payments to Florida. The court found maintaining a suit against defendant, based on the totality of the circumstances, offended traditional notions of fair play and substantial justice.

The court held that to find otherwise would have far-reaching implications to users of on-line computer services. Consumers of on-line services across the country could find themselves being haled into court in the state in which the supplier's billing office and database happened to be located. In a situation where users are solicited, engaged, and serviced entirely in the user's own state by the supplier's local representatives this result offends traditional notions of fair play and substantial justice.

The court in *Zippo Mfg. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D.Pa. 1997), dealt with a cybersquatting case, where the plaintiff sued an Internet news service for trademark dilution, infringement and false designation for using the domain names "zippo.com," "zippo.net," and "zippo-news.com." The court found jurisdiction and held that the likelihood of personal jurisdiction being found can be constitutionally based on an entity's presence on the Internet. *Id.* at 1124. The court held that the extent of the entity's presence, in the manner of sliding scale, was directly proportionate to the nature and quality of the commercial activity conducted over the internet. The court found that a passive web site that only made information available to interested users was not grounds for exercising jurisdiction. A web site that entered into contracts and knowingly and repeatedly transmitted computer files would be properly subject to personal jurisdiction. In cases dealing with the middle ground, where interactive web sites exchanged information with a user, the exercise of jurisdiction should be determined by examining the commercial nature of the exchange and the level of interactivity.

B. Minnesota's Internet Warning: Sign Post of the Future?

The states are beginning to take an aggressive stance toward jurisdiction on the internet. An indication of where the states might be going in Internet regulation is provided by Minnesota, California, and Texas. In an effort to control criminal activity on the internet the Minnesota Office of the Attorney General has a web site where it has published a list of lawsuit summaries and a Memo on Jurisdiction. In response to a query from the Financial Institution Committee, Texas House of Representatives, the Office of the Attorney General of Texas issued an opinion on the legality of internet gambling. California has extended its jurisdictional reach to out-of-state vendors of goods and services through enactment of Assembly Bill 3320.

The Attorney General of Minnesota's undated policy statement regarding internet criminal activity in the form of a memorandum can be found at its Web site titled "Warning to All Internet Users and Providers." [82] The warning contains the legal basis for the Attorney General of Minnesota's assertion of jurisdiction. It states the Attorney General's enforcement position regarding certain illegal activities on the Internet such as gambling, lotteries or sports book making disseminated to Minnesota residents. [83]

The legal basis for jurisdiction is based on Minnesota's general criminal jurisdiction statute. [84] The statute provides that a person may be convicted and sentenced under the law of Minnesota if the person: (1) Commits an offense in whole or in part within Minnesota; or (2) being outside of Minnesota, causes, aids or abets another to commit a crime within the state; or (3) being outside Minnesota, intentionally causes a result within the state prohibited by the criminal laws of Minnesota, Minn. Stat. sect. 609.025 (1994).

The Attorney General for Minnesota gives examples of what provides the legal basis for its assertion of jurisdiction. One example was where the Minnesota Supreme Court applied this statute to a criminal case. In *State v. Rossbach*, 288 N.W.2d 714 (Minn. 1980), the defendant, while standing in an Indian reservation, shot at a person outside the reservation. The court relying on Minn. Stat. 609.26 and the common law affirmed the conviction. It held that the intentional impact within Minnesota land had created jurisdiction. *Id.* at 715-16.

Another example was given where these jurisdictional principles were applied by a Minnesota court in a civil case. In *State v. Red Lake DFL Committee*, 303 N.W.2d 54 (Minn. 1981), the Minnesota Supreme Court held that the state had jurisdiction over a committee of the Red Lake Indian Tribe which had purchased advertising space in a newspaper for political advertisements. The committee argued that it was not required to register under the state ethical practices law because nothing it had done occurred outside the reservation. The court found that the committee's act disseminated a political message that extended beyond the reservation's boundaries. *Id.* at 56.

The Attorney General for Minnesota warning states that these jurisdictional principles of Minnesota law apply equally to activities on the Internet. Organizations or individuals outside Minnesota who disseminate information in Minnesota through the Internet, causing a result to occur in Minnesota are subject to Minnesota criminal and civil laws. [85]

Dan Morales, Attorney General of Texas wrote an opinion on the legality of whether persons may play and bet on card games using computers with modems or other transmission devices and related questions. [86] He found that when two or more persons using computers and modems, play in a private place (there is no public access to the games) a card game with each other and bet on the outcome, there is no criminal activity. However, if there is public access or if a bulletin board service knowingly assists in the game and charges for the service, this activity violates various sections of penal provisions of chapter 47, Penal Code. The Attorney General found additional authority in 18 U.S.C. section 1084, which criminalizes the transmission of wagering information in

interstate commerce and in 18 U.S.C. section 1955, which prohibits illegal gambling businesses.

California enacted Assembly Bill 3320 [87] extending its jurisdiction to out-of-state vendors who use the Internet to advertise, sell, or lease goods and services. Vendors outside California are required to provide specific refund and return policies and make certain disclosures to purchasers located in California. [88]

C. Cyberjurisdiction in Criminal Cases

The question of cyberjurisdiction in a criminal case came to the forefront of attention in early 1996 in *U.S. v. Thomas*, 74 F.3d 701 (6th Cir. 1996), when the Sixth Circuit upheld the highly publicized conviction of a couple operating a pornographic bulletin board from their home. The defendants began operating the Amateur Action Computer Bulletin Board System ("AABBS") from their home in Milpitas, California in February 1991. The AABBS contained approximately 14,000 Graphic Interchange Format ("GIF") files. These files could be accessed by members who possessed the password. Once the password was entered, the users were able to select, retrieve, or download the GIF files to their own computers.

The government got involved in AABBS' activities when a Web surfer found the site, explored the introductory screens, was offended and subsequently complained. In 1994, a U.S. Magistrate Judge for the Northern District of California issued a search warrant authorizing a search of the defendant's home. As a result of the evidence found their computer system was confiscated.

The defendants were convicted in the U.S. District Court, Western District of Tennessee on federal obscenity charges. They appealed and the appellate court affirmed. There were two premises for their appeal: (1) The federal obscenity statute [89] did not apply to intangible objects like computer GIF files, and (2) Congress did not intend to regulate the type of transmissions at issue because the federal obscenity statute did not expressly prohibit such conduct.

The defendants asserted that the GIF files were an intangible string of 0's and 1's which only became viewable images after being decoded in the AABBS member's computer. The court disagreed, ruling that the fashion in which the images were transmitted did not affect their ability to be viewed or printed out by members in Tennessee. [90] The defendants also argued that they were prosecuted under the wrong statute and that their conduct, if criminal at all, fell within the prohibitions of the statute which addresses commercial dial-a-porn operations. [91] The court declined to accept this argument. Instead it ruled that the statute must be construed to effect the intent of Congress, which was to prevent the channels of interstate commerce from being used to disseminate any obscene matter. [92]

Miller v. California, 413 U.S. 15, 93 S.Ct. 2607, 37 L.Ed.2d 419 (1973), held obscenity was to be judged by what the average person applying contemporary community

standards would find to be obscene. Defendants argued the internet environment provides broad-ranging connections among people in cyberspace, as such the notion of obscenity tied to geographic locale would put a chill on protected speech. *Id.* at 710-711. The defendants asserted a more flexible definition was needed because BBS operators could not select who received their material.

The court ruled that the defendants had a preexisting method of screening potential members. By prescreening their members they could protect themselves from being subjected to liability in jurisdictions with less tolerant standards. This could be accomplished by refusing to give passwords to users from those districts. [93] The court further ruled the defendants were free to tailor their messages on a selective basis to the communities it chose to serve. Accordingly, it was held by the court that there was no need to develop a new definition of community. [94]

The case turned on the fact that even though the GIF files never actually left Northern California and were arguably not obscene under Northern California, Bay Area standards, [95] they were obscene by the standards of Memphis, Tennessee. The Court applied the community standards of the geographic area where the materials were sent as the proper test, in affirming the lower court's holding that defendants were violating federal obscenity laws. [96]

In *Minnesota v. Granite Gate Resorts, Inc.*, 65 USLW 2440, 1996 WL 767431 (D.Minn. Dec 10, 1996), the policy Minnesota's Attorney General had stated in its Internet warning was tested in court. The Attorney General had asserted the right to regulate the activities of an online gambling service based in Las Vegas, Nevada. The Attorney General argued that the defendant had explicitly misrepresented its services as lawful on its Web page. [97] The court denied the defendant's motion to dismiss for lack of jurisdiction because of hits from Minnesota at the defendant's Web site, the availability of a toll-free number that users could call advertised on its Web page, and the number of Minnesota residents who had signed on to the defendant's mailing list. [98]

Relying on *Inset*, the court held that the defendant's advertising on the Internet constituted a direct marketing campaign directed at residents of the state of Minnesota which was sufficiently purposeful to subject the defendant to suit in the forum state. [99]

D. Cyberjurisdiction in International Cases

When adjudicating cases involving foreign nationals, the courts must balance several factors. On a case by case basis, the courts must consider the procedural and substantive policies of other countries whose interests are affected by the court's assertion of jurisdiction. Keeping these policies in mind, the court must then consider the reasonableness of assertion of jurisdiction examined in the light of the interest of the federal government in its foreign relation policies. When extending jurisdiction into the international field great care and reserve must be exercised. [100] Because of these sovereignty concerns, there is a higher jurisdictional barrier when litigating against a foreign national. [101]

There are no international cyberjurisdiction cases, however, *Asahi Metal Industry Company*, referenced *infra* and *Core-Vent*, discussed *infra* can both provide the framework for future cyberjurisdiction cases. *Playboy Enterprises*, *infra* discusses an international civil case involving trademark infringement. In that case the court sidestepped the issue of international cyberjurisdiction relying on a previous 1981 injunction against the defendant to base its finding of jurisdiction. Nevertheless, the case provides useful insights into the application of cyberjurisdiction principals in international cases. The Supreme Court in *Asahi Metal Industry Company v. Superior Court*, 480 U.S. 102 [107 S.Ct. 1026] (1987), indicated that a plaintiff seeking to hale a foreign citizen into court in the United States must meet a higher jurisdictional threshold than is required when the defendant is a United States citizen. In *Asahi* the court found that even though Asahi had minimum contacts with the forum state, it would be unreasonable and unfair to find jurisdiction for three reasons: (1) the distance between defendant's headquarters in Japan and the Superior Court of California and the unique burdens of submitting a dispute between two foreign nationals in a foreign legal system; (2) California's and the foreign plaintiff's slight interest in having the case heard in California; (3) the affect on the procedural and substantive interests of other nations by California's assertion of jurisdiction over a foreign nationals. *Id.* at 105-106. Commentators have proposed that these international factors were dispositive in the court's decision. [102]

This higher jurisdictional threshold was further examined in *Core-Vent Corp. v. Nobel Industries AB.*, 11 F.3d 1482 (9th Cir. 1993). The plaintiff, a California corporation, brought suit against the defendant, five Swedish citizens and three American citizens for publishing articles containing false and misleading comparisons between Core-Vent's and Nobelpharma's dental implants. The United States District Court for the Central District of California dismissed for lack of personal jurisdiction. The plaintiff appealed and the United States Court of Appeals, Ninth Circuit affirmed the lower court.

The appellate court found that California's long-arm statute allowed courts to exercise personal jurisdiction over defendants to the extent permitted by the Due Process Clause of the United States Constitution. The court ruled that in a case like this, where the defendant has not had continuous and systematic contacts with the state in order to subject it to jurisdiction, the three-prong minimum contacts test should be applied. The this test consists of (1) whether there was purposeful availment; (2) whether the claim arises out of or is related to defendant's activities; and (3) whether the exercise of jurisdiction comports with fair play and substantial justice. *Id.* at 1485.

The first prong of the test looks to whether the nonresident defendant had purposefully directed his activities or consummated some transaction with the forum or resident thereof, or had performed some act by which he purposefully availed himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws. The Supreme Court has allowed jurisdiction be exercised over a defendant whose only contact with the forum state is the purposeful direction of a *foreign* act having *effect* in the forum state. [103]

The plaintiff claimed that the Swedish defendants contacts were analogous to those of the individual defendants in *Calder v. Jones*, 465 U.S. 783 (1984). *Calder* stands for the proposition that personal jurisdiction can be based on intentional actions expressly aimed at the forum state causing harm, the brunt of which is suffered in the forum state. The court ruled that because the libel was distributed through the stream of commerce, and that it was circulated worldwide, it was unclear whether the majority of the harm suffered was in California. [104] The court ruled the defendants were aware of the fact that the plaintiff was a California corporation and that their actions would cause harm in California. [105] Although it was a close call, the court concluded that it would assume that the personal availment prong had been satisfied. [106]

The second prong of the test, is that the claim must be one which arises out of, or relates to the defendant's forum-related activities. This prong was not examined by the Court because it said that the libel claims clearly arose out of the publication of the articles. [107]

The third prong of the test, is that the exercise of jurisdiction must comport with fair play and substantial justice consists of seven factors which must be balanced. The factors are (1) the extent of the defendant's purposeful interjection into the forum state's affairs; (2) the burden on the defendants of defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum.

In applying the seven factors to the defendants actions the Court ruled that: (1) that their contact with the forum state was attenuated; (2) that the burden of defense weighed heavily on the defense; (3) that the Swedish doctors were individuals with no United States-based relationships; (4) that California maintained a strong interest in providing effective redress for its residents; (5) that the forum would provide efficient means of adjudicating the issue; (6) although it may be inconvenient and costly, that the plaintiff could effectively maintain a suit in Sweden, that a mere preference on the part of the plaintiff did not affect the balancing; and (7) that the plaintiff had not met its burden that it had no alternative forum i.e., sue in Sweden. [108]

The Court held based on these findings that exercise of its jurisdiction would not comport with fair play and justice. [109] The Court added that requiring the Swedish defendants to submit to the jurisdiction of the court would impose substantial burdens on them and interfere with a foreign nation's sovereignty. [110]

While adjudicating the case, the Court remarked on the legal tensions existing in a number of the Court's decisions in dealing with the seven factors used to determine jurisdiction. For example, some of its cases have suggested that once a minimum contacts threshold is met, the degree of intrusion into the forum becomes irrelevant. [111] The court noted that a commentator on the court's decision in *Asahi*, suggested that a larger

number of additional connections should be required to justify the exercise of jurisdiction when the reasonableness factors weigh in the favor of the defendant. [112]

Another point of tension was whether the corresponding burden on the plaintiff to bring a claim against the defendant in an alternative forum lessened the impact of this factor when determining overall reasonableness. In *Pacific Atlantic Trading Co. v. M/V Main Exp.*, 758 F.2d 1325 (9th Cir. 1985), the court said that the burden on the defendant is the primary concern, while in *Sinatra v. National Enquirer, Inc.*, 854 F.2d 1191 (9th Cir. 1988), the court ruled that the burden on the defendant must be examined in light of the corresponding burden on the plaintiff.

In *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*, 939 F.Supp. 1032 (S.D.N.Y. 1996), the issue at bar was whether personal jurisdiction applied in enforcing a court injunction entered June 26, 1981. The court found that jurisdiction applied because of the earlier court injunction where jurisdiction had previously been established. *Id.* at 1037. The appeals court upheld the 1981 injunction against the defendant, enjoining it from publishing or distributing its "Playmen" magazine in the United States.

The defendant had a pay Web site located in Italy and accessed by United States residents. Because the users had to subscribe to access the files on the Web page the court ruled the defendant could determine which of its subscribers were United States citizens, and was therefore, knowingly allowing them to access the Web site. Once at the Web site users could download the pictorial images and store them on their computers. Based on these facts the court found the site to be a United States distribution in violation of the injunction. *Id.* at 1039-40.

The court ruled that the defendant could not be prohibited from operating its Web site merely because the site was accessible from within a country which had banned its product. *Id.* The court held that the Internet deserved special protection as a place where public discourse could be held without regard to nationality, religion, sex, age, or to monitors of community standards of decency. *Id.* Nevertheless, the court continued, this special protection did not extend to ignoring court orders. If this were allowed injunctions would cease to have meaning and intellectual property would cease to be properly protected. [113]

The scope of personal jurisdiction over a foreign defendant still has many issues to be resolved. For example, in *Digital Equipment Corporation v. Altavista Technology, Inc.*, Civ. Action 96-12192NG (D.Mass. March 12, 1997), the court pointed out an area of law yet to be decided. It asked whether any Web activity by anyone done without commercial intent; i.e., without the advertisement or solicitation of sales, absent a sale with a contract or other contacts with the forum state, absent the potentially foreseeable harm of trademark infringement, would be sufficient to permit the assertion of jurisdiction over a foreign defendant.

Another unresolved question is whether a user at one Web site creating a document with a hyperlink into another person's Web site (perhaps without their knowledge or consent,

which would be freely accessible to any user of the Internet) would provide sufficient contacts to create jurisdiction over the owner of the linked site. [114] An indication of how the courts may decide this issue can be found by referring to *Playboy Enterprises, Inc. v. Frene*, 839 F.Supp. 1552 (M.D.Fla. 1993).

In *Frene*, the defendant operated a subscription electronic bulletin board. Once at the Web site users could read and download unauthorized copies of the plaintiff's copyrighted photographs onto their computers. The court held that the unauthorized uploading of the photographs by the bulletin board service knowing that they would be later downloaded by the bulletin board subscribers was a distribution. *Id.* at 1556. This court decision could be arguably extended to apply to users who include hyperlinks to another user's pornographic documents without the user's knowledge or consent.

III. CONCLUSION

In order to support personal jurisdiction in cyberspace the courts now require that defendants provide more than mere accessibility to a Web site. Some sort of interaction is required. A requirement which may be satisfied by as little as one contact. The trend appears to be that information providers must comply with the limitations of the laws wherever the user is located, or find themselves subject to the user's state jurisdiction, and its civil and criminal laws. Case law indicates that the courts are inclined to expect the information provider to determine where the user is located and to block access to their site if access would be illegal in the user's locale. If they own an 800 or 900 number they could also be expected to block certain area codes to avoid prosecution.

NOTES

[*] Gabriole Zeviar-Geese is a second year law student attending California Pacific School of Law located in Bakersfield, California. She received a B.A. in Philosophy from York University, Toronto, Canada in 1991, a Diploma in Computer Programming and Analysis from Seneca College of Applied Arts and Technology, Toronto, Canada in 1981, and a Certificate in Adult Education-Staff Training and Development from Seneca College of Applied Arts and Technology, Toronto, Canada, in 1988. Prior to entering law school, she wore many hats as course developer, text book writer, technical trainer and data base consultant. I would like to acknowledge Professor C.M. (Bud) Starr, II who facilitated my article. His help was invaluable and greatly appreciated.

[1] Curtis E.A. Karnow, *Recombinant Culture: Crime In The Digital Network*, Address Before Defcon II, Las Vegas (July 1994)(visited Sept 7, 1997))

(transcript available at <http://cpsr.org/cpsr/computer_crime/net.crime.karnow.txt>, p.6)

[2] Author surveyed cyberlaw literature, cases and courses taught at various law schools around the country.

Course: A Law of Cyberspace, by Professor E. Sorkin of The John Marshall Law School, Fall 1996. <<http://www.jmls.edu/cyber/1996/index.html>> (last modified Nov 22, 1996);

Course: Law of Cyberspace Seminar, by Professor David G. Post of Georgetown University Law Center, Fall 1996 (visited Aug. 10, 1997).

<<http://www.cli.org/cyberspace/index.html>>

Course: Law of the Internet, by Professor J. Kaufman Winn of Southern Methodist University School of Law and Professor R. Warner of Chicago-Kent School of Law.

<<http://www.smu.edu/~jwinn/inetlaw.htm>>(visited Aug 22, 1997);

Course: Cyberspace Law for Non-Lawyers by Professor M.Jensen and Professor W. Marr of Cyberspace Law Institute. <<http://www.ssrn.com/cyberlaw>> (visited Aug 10, 1997); and

Course: Law and the Internet by Professor Froomkin of the Univ. of Miami.
<<http://www.law.miami.edu/~froomkin/seminar/index.html>> (visited Aug. 22, 1997)

[3] Course: Law of the Internet by J. Kaufman Winn and R. Warner, Law of the Internet, Southern Methodist University School of Law.
<<http://www.smu.edu/~jwinn/inetlaw.htm>> (visited Aug 22, 1997)

[4] Id.

[5] Id.

[6] Id.

[7] Id.

[8] Id.

[9] Stewart Biegel, The Emerging and Specialized Law of the Digital Revolution, Los Angeles Daily Journal, Jan. 25, 1996, at 1.

<<http://www.gse.ucla.edu/iclp/jan96.html>>

[10] Heidi Steele, How to Use the Internet 6 Ziff-Davis Press (1996).

A network is where several computers are connected using cables, telephone lines, satellite or high speed data lines in order to share information and resources.

[11] Heidi Steele, *supra* note 10, at 6.

[12] Janet Reno, Attorney General of the United States et al. v. American Civil Liberties Union, Supreme Court No. 96-511, 20 n.3 (Jun. 26, 1997).

<http://www.ciec.org/SC_appeal/opinion.html> (visited Aug 10, 1997)

The acronym for the network developed by the Advanced Research Project Agency.

[13] Janet Reno, *supra*, note 12, at 20 n.4.

See also 929 F.Supp. 824, 844 (finding 81).

[14] Curtis E.A. Karnow, *supra* note 2, at 8 n.6.

See also Special Report: Distributed Computing, 19 Byte 125 (June 1994).

[15] Mark Kravitz, Sum & Substance: A Virtual Presence, The Connecticut Law Tribune, Apr. 21, 1997, at 1.

<<http://www.courttv.com/news/422f.html>>

[16] *Id.*

[17] Janet Reno, *supra* note 12, at 2.

[18] *Id.*

[19] Heidi Steele, *supra* note 10, at 99.

[20] Janet Reno, *supra* note 12, at 2.

[21] AOL regularly advertises this service to its users when they log on to AOL.

[22] Heidi Steele, *supra* note 10, at 9.

[23] A browser is a program used to access pages stored on Web servers. A Web server is a very fast computer that is always connected to the Internet. Heidi Steele, *supra* note 10, at 8.

[24] Heidi Steele, *supra* note 10, at 19.

Example of a URL is "<http://www.gse.ucla.edu/iclp/jan96.html>."

"http" refers to the protocol; "www.gse.ucla.edu" refers to the Web server name; "iclp" refers to the path; and "jan96.html" refers to the document name.

[25] Heidi Steele, *supra* note 10, at 17.

Example of a mail address is "zeviar@aol.com." "zeviar" refers to the users Internet account; "aol" refers to the host or domain; and "com" refers to a commercial organization.

The six top-level domains are:

1. com (commercial organization)
2. edu (educational institution)
3. gov (government)
4. int (international organization)
5. net (networking organization)
6. org (nonprofit organization)

[26] Heidi Steele, *supra* note 10, at 8.

[27] Thomas Boutell and Boutell.Com, Inc., World Wide Web FAQ, 1997.
<<http://www.boutell.com.faq>> (visited Aug. 22, 1997)

FAQ stands for frequently asked questions.

[28] *Id.*

[29] *Id.*

[30] A web server is a high speed computer that is connected 24 hours a day to the Internet. Heidi Steele, *supra* note 10, at 9.

[31] *Id.*

[32] *Id.*

[33] *Id.* at 8.

[34] Gambling - Minn. Stat. sect. 609.75 (1994).

Cyberstalking - 11 Del. C. sect. 1312 A, Conn. Gen. Stat. sect. 53a-183, 53a-182b, MSA sect. 28.643(8)E, vi, Mont. Code Ann., sect. 45-5-220, 1b, 21 Okl. St. sect. 1173, F 4f, Wyo. Stat. sect. 6-2-506 B,i, AK St. ?41.270. Barbara Jensen, *infra* note 65, 11 n.16.

Fraud - United Nations, *infra* note 41 at 15.

[35] Cal. Penal Code sect. 502 (amend. 1989) (West 1988 & Supp. 1997).

[36] N.Y. Penal Code Art. 156.00-.50 (1986).

<gopher://lbdc.senate.ny.us/00/.laws/Penal> or

<<http://rampages.onramp.net/~dgmccown/ny-law.htm>>

[37] Communications Decency Act of 1996, 110 Stat. 133, 47 U.S.C.A. sect. 223 (Supp. 1997).

[38] No. 96-511 (U.S. Jun. 26, 1997).

[39] 47 U.S.C.A. section 223(a)(1)(B) (Supp. 1997) prohibits the use of a telecommunication device by interstate or foreign communications to knowingly transmit an obscene or indecent communication to a recipient who is under 18 years old. The term "indecent" was considered too vague. 47 U.S.C.A. sect. 223(d)(1) (Supp. 1997) prohibits interstate or foreign use of an interactive computer service to knowingly send to a person under 18 years old any communication that in context is patently offensive as measured by community standards. The terms "patently offensive" and in "context" were too vague for criminal enforcement and violated simple fairness. *Reno v. ACLU*, *supra*, note 12, at 7.

[40] United Nations, International review of criminal policy -United Nations Manual on the Prevention and Control of Computer Related Crime, at paragraph 29 (July 28, 1997).

<<http://www.ifs.univie.ac.at/%7Epr2gql/rev4344.html>>

It is unclear whether individual losses ranged from \$145 million to \$730 million or whether total losses were between \$145 million and \$730 million.

[41] *Id.*

[42] United Nations, *supra* note 41, at paragraph 27.

[43] *Id.* at paragraph 30.

[44] *Id.* at paragraph 21.

[45] See *U.S. v. Thomas*, 74 F.3d 701 (6th Cir. 1996), where the Court found a California couple who made pictures that were not considered pornography in California available to Tennessee residents prosecutable under federal obscenity laws..

[46] United Nations, *supra* note 41, paragraphs 20 to 73.

[47] Id. at paragraphs 63-65.

[48] Id. at paragraph 62.

[49] Jonathan Rosenoer and Kimberly Smigel, Notable legal developments reported in April 1997, Cyberlex, (May 1997).

<<http://www.cyberlaw.com/cylx0497.html>> (visited July 28, 1997)

[50] United Nations, supra note 41, at paragraph 67

[51] Id.

[52] A worm is designed to alter or destroy data but it lacks the ability to replicate itself. Example of a worm program -- a bank computer program that is instructed to continually transfer money to an illicit account. United Nations, supra note 41, at paragraph 71

[53] A virus is a program that has the ability to attach itself to legitimate programs and to replicate and attach itself to other computer programs. Viruses can enter a computer system by being attached to an infected file or legitimate program or through a Trojan horse. Its activity can involve the display of harmless messages on computer terminals to complete destruction of all the data on a computer system.

In 1990, Europe experienced its first computer virus, it was used to commit extortion in the medical research community. The virus threatened to destroy increasing amounts of data if no ransom was paid for its "cure." United Nations, supra note 41, at paragraphs 69-70

[54] A logic bomb or 'time bomb' is a program that is written to modify or destroy data at a specific date and time in the future. Logic bombs can be timed to cause maximum damage and 'detonate' long after the perpetrator leaves the firm or it can be used as a tool for extortion in exchange for disclosure of the location of the logic bomb. United Nations, supra note 41, at 16.

[55] United Nations, supra note 41, at 16.

[56] Janet Reno, supra note 12, at 16.

[57] Rosenoer and Smigel, supra note 49, at 1.

Perhaps this could also be seen as a form of vigilante computer crime.

[58] This warning was retrieved while logged on to AOL the week of August 18, 1997 by the author while accessing the KEYWORD option.

[59] The Trojan horse does this by impersonating the normal system log on program. When the user logs on to the computer system the Trojan horse program is displayed instead of the normal log on program and prompts the user for his userid and password. It captures and saves this information and logs the user on in a normal fashion. Later the hacker can access his Trojan horse program and read the purloined information. United Nations, *supra* note 41, at 15.

[60] United Nations, *supra* note 38, at 18.

See *U.S. v. LaMacchia*, Crim.A. No. 94-10092-RGS, U.S. Dist. (D. Mass. Dec. 28, 1994) where the indictment alleged a loss of more than a million dollars to software copyright holders, page 2.

<<http://rampages.onramp.net/~dgmccown/c-lamcha.htm>>

[61] 18 U.S.C. section 1343.

[62] This was a case where a twenty-one year old student at MIT set up an electronic bulletin board using a pseudonym and an encrypted address and encouraged his correspondents to upload popular software applications and computer games. He transferred these to a second address where they could be downloaded by users who had the password. He was caught and indicted for violating 18 U.S.C. sect. 1343, the wire fraud statute. The Court did not convict because he received no financial gain for his infringement.

See <<http://rampages.onramp.net/~dgmccown/c-lamcha.htm>>

[63] Barbara Jenson, *Cyberstalking: Crime, Enforcement and Personal Responsibility in the On-Line World* (May 1996), page 10 n.7.

<<http://www.law.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm>> (visited Aug 22, 1997)

See Eileen Ross, *E-mail stalking: Is Adequate Legal Protection Available?*, 13 J. Marshall J. Computer & Info. L. 405 at 409-10.

[64] *Id.* at 1.

See Robert A. Guy, Jr., *The Nature and Constitutionality of Stalking Laws*, 46 Vand.L.Rev. 991, 995.

[65] *Id.* at 2.

Cal. Penal Code sect. 646.9 (Deering 1995).

[66] *Id.* at 11 n.16.

The seven states are Alaska, Connecticut, Delaware, Michigan, Montana, Oklahoma and Wyoming.

[67] United Nations, *supra* note 41, at 10.

[68] United Nations, *supra* note 41, at 10.

[69] United Nations, *supra* note 41, at 9.

[70] David Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. Online L. art. 3, para. 36.

[71] Stuart Biegel, *supra* note 9, at 2.

[72] David R. Johnson and David Post, *Law and Borders--The Rise of Law in Cyberspace*, 48 Stanford L.Rev. 1357, 1367 (May 1996)

[73] U.S.C Const. Amend. XIV

[74] *Darby v. Compagnie Nationale Air France*, 769 F.Supp. 1255, 1262 (S.D.N.Y. 1991) (quoting *International Shoe Co. v. Washington*, 326 U.S. 310, 316 [66 S.Ct. 154, 158, 90 L.Ed. 95] (1945)).

[75] *Bensusan*, 937 F.Supp. at 301.

[76] See *Asahi Metal Indus. Co. v. Superior Court*, 480

U.S. 102, 112, [107 S.Ct. 1026, 1032, 94 L.Ed. 92] (1992)

(plurality opinion).

[77] *Bensusan*, 937 F.Supp. at 301. (D.Conn. 1996).

[78] *Inset*, 937 F.Supp.161 at 164.

[79] *Id.*

[80] *Kravitz*, *supra* note 15, at 3.

[81] *Jensen, Issues In Internet Commerce, Cyberlaw*, at 4.

<<http://www.cyberlaw.com/issues.html>>

[82] *Minn. Stat. Ann. Section 609.025* (West 1987).

The complete text of the AG's memo can be found at its Web site:
<<http://www.state.mn.us.ebranch/ag/memo.txt>>

[83] Minn. Stat. sect. 609.75 (1994).

[84] Minn. Stat. sect. 609.025 (1994).

[85] Attorney General, Warning to All Internet Users and Providers, at 2.

See <<http://www.state.mn.us.ebranch/ag/memo.txt>>

[86] Office of the Attorney General of Texas, Opinion No. DM-344, 1995 Tex. AG LEXIS 56, May 2, 1995.

See <<http://www.jmls.edu/cyber/docs/texas-ag.html>>

[87] Filed with the Secretary of State Sept. 23, 1996, as Chapt. 785 of the Statutes of 1996, effective Jan. 1, 1997.

[88] Thomas E. Jensen, *supra* note 81, at 4.

[89] 18 U.S.C. sect. 1465.

[90] U.S. v. Thomas, 74 F.3d at 706.

[91] 47 U.S.C. section 223(b) (1934, amended 1988).

[92] U.S. v. Thomas, 74 F.3d at 708.

[93] *Id.* at 711.

[94] *Id.*

[95] In 1992 the AABBS computers were seized by the San Jose high-tech crime unit, scrutinized and found insufficiently offensive to warrant prosecution.

See Diamond and Bates, Law and Order Comes to Cyberspace,

Tech Review:Oct 95: Law & Order, at 5.

<<http://web.mit.edu/afs/athena/org/t/techreview/www/articles/oct/1/Diamond.8950/97>>

[96] *Id.* at 710-11.

[97] The advertisement on the Internet stated as follows: a. Wagernet "will provide sports fans with a legal way to bet on sporting events from anywhere in the world. . . 24 Hours a Day!"

[98] Thomas E. Jensen, *supra* note 81, at 4.

[99] Kravitz, *supra* note 15, at 1.

[100] *Asahi Metal Industry Company v. Superior Court*, 480 U.S. 102 (1987).

[101] *Sinatra v. National Enquirer*, 854 F.2d at 1199.

[102] *Core-Vent Corp. v. Nobel Industries, AB*, 11 F.3d 1482, 1490 (9th Cir. 1993)

See Earl M. Maltz, *Unravelling the Conundrum of the Law of Personal Jurisdiction: A Comment on Asahi, Metal Industry Co. v. Superior Court of California*, 1987 *Duke L.J.* 669, 689-90.

[103] *Haisten v. Grass Valley Medical Reimbursement Fund*, 784 F.2d 1392, 1397 (9th Cir. 1986) (citing *Calder v. Jones*, 465 U.S. 783, 789, [104 S.Ct. 1482] (1984)).

[104] *Core-Vent*, *supra* note 109, at 1486.

[105] *Id.* at 1487.

[106] *Id.*

[107] *Id.* at 1485.

[108] *Id.* at 1488-90.

[109] *Id.* at 1490.

[110] *Id.*

[111] *Corporate Invest. Business Brokers v. Melcher*, 824

F.2d 786, 787 (9th Cir. 1987).

[112] See Earl M. Maltz, *Unravelling the Conundrum of the*

Law of Personal Jurisdiction: A Comment on Asahi Metal Industry Co. v. Superior Court of California, *Duke L.J.* 669, 689-90 (1987).

[113] Post and Nunziato, *Personal Jurisdiction on the Internet*, *Cyberspace Law Institute* (May 1997).

[114] Jensen, Issues In Internet Commerce, Cyberlaw, page 4.

<http://www.cyberlaw.com/issues.html>