Chapter 5
Cite as 22 Energy & Min. L. Inst. ch. 5 (2002)

Jurisdiction, Domain Names, Privacy
and Security: How the Digital Age
Has Changed Business

James V. Corbelli
Stephen L. Korbel
Babst, Calland, Clements & Zomnir, P.C.
Pittsburgh, Pennsylvania

Synopsis

§ 5.01. Introduction.................................................................118

§ 5.02. Jurisdiction .......................................................................119

[1] — Traditional Notions of Personal Jurisdiction ................. 120
   [a] — General and Specific Jurisdiction .......................... 120
   [b] — Traditional Jurisdictional Analysis ........................ 121
   [c] — Stream of Commerce Approach ............................... 122

[2] — The Internet and Personal Jurisdiction ......................... 123
   [a] — Zippos and Its Legacy ........................................... 124
   [b] — Another Approach to Internet Jurisdiction:
      the Effects Test and Panavision .................................. 126

   [a] — The Mink Case .................................................... 129
   [b] — Cybersell, Inc. ..................................................... 130
   [c] — Bensusan Restaurant Corporation:
      a pre-Zippo Passive Web Site Case ............................. 132

[4] — Commercial Web Site ............................................... 133

[5] — In-between Web Sites .................................................. 135
   [a] — People Solutions ................................................. 135
   [b] — American Eyewear .............................................. 136

[6] — International Disputes and Personal Jurisdiction ............ 137
   [a] — Ty, Inc. v. Clark .................................................. 137
   [b] — Euromarket Design, Inc.
      v. Crate and Barrel, Ltd. ........................................... 138

[7] — Conclusion ................................................................... 139

§ 5.03. Domain Names .......................................................... 140

[1] — Early Years of Domain Naming ...................................... 141
[2] — NSI to ICANN ............................................................ 143
[3] — Internet Corporation for Assigned Names and Numbers .... 146
§ 5.01

Within the last five years, the Internet and electronic mail (e-mail) have become common tools for virtually all business. The Internet has dramatically increased the speed that information can be exchanged. With
e-mail, the World Wide Web, instant messages, and bulletin board systems, communication has not only become widespread, but now occurs instantaneously and globally. On an economic and business level, the Internet has become a business necessity. For example, annual Internet retail sales are projected to reach nearly $200 billion by 2004, double the amount of retail sales through traditional catalogs.\(^1\) Despite its explosion into the business conscience, the Internet also poses a number of challenges. Novel issues of law are apparent in the world of cyberspace. The real battle concerns whether new laws are needed for the novel issues arising from the Internet, or whether the application of traditional laws is sufficient. An understanding of the ways in which the Internet can impact business is important in all economic sectors, including (and in some ways especially) traditional business sectors.

This chapter will address four of the most pressing issues facing the Internet today from the perspective of a business. Part one discusses how courts have applied traditional notions of personal jurisdiction to the Internet as well as the trends that have emerged from Internet jurisdiction cases. Part two is a broad discussion about domain names and how the courts and legislative initiatives have dealt with the practice of cybersquatting. Part three reviews privacy concerns arising from Internet use and the protections fashioned by Congress, the Federal Trade Commission and the European Union. Part four contains a brief discussion which analyzes the security issues facing organizations with an Internet presence and common sense steps organizations may take to limit the losses that result from a security breach.

§ 5.02. Jurisdiction.

The explosive growth of the Internet has raised concerns as to the application of existing substantive and procedural law doctrines from a world with physical borders to one without physical borders. The laws of personal jurisdiction present particularly difficult problems. Some

commentators believe the existing doctrine can adequately solve most Internet jurisdictional conflicts, while others believe new laws and statutory schemes need to be developed to deal with these novel issues of law. Currently, a business with an Internet presence has the potential to be haled into a distant court without the types of minimum contacts that have historically been necessary to subject that business to litigation far from home. This section of the chapter will review the jurisdiction principles that will allow an organization to determine the extent to which it wishes to be exposed to distant litigation.

A court may exercise jurisdiction over defendants if jurisdiction is proper under both state statutory law and the United States Constitution. All states have long arm statutes that define in what circumstance it is proper for a court to exercise jurisdiction over a defendant. A state long-arm statute can only confer jurisdiction as far as is allowable under the Due Process Clause of the United States Constitution. Jurisdiction may be asserted under the theory of general jurisdiction or the theory of specific jurisdiction.

[a] — General and Specific Jurisdiction.
General jurisdiction permits a court to exercise personal jurisdiction over a non-resident for a cause of action arising outside the state or without connection to the forum. This power is permissible under the Due Process Clause of the United States Constitution when the defendant’s connections and activities with the forum state are so substantial that the defendant would expect to be subjected to suit there on a claim not related to the defendant’s activities in the forum state. Additionally, the plaintiff must demonstrate the defendant would suffer no inconvenience from defending

2 U.S. Const. Amend XIV.
4 U.S. Const. Amend XIV.
itself in the forum state.\textsuperscript{6} In other words, when the defendant has engaged in “systematic and continuous” activities in the forum state, general jurisdiction can be said to exist.\textsuperscript{7} If the defendant is domiciled, incorporated or has its principle place of business within the forum state, the constitutionally-required “systematic and continuous” connection is satisfied. If the defendant’s connection to the forum state is due to actions undertaken only by the plaintiff, the defendant will not be subject to jurisdiction unless the defendant has “purposefully availed itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws.” \textsuperscript{8}

Specific jurisdiction is appropriate when the plaintiff’s cause of action arises out of the defendant’s contacts with the forum, but only if jurisdiction would be proper under the long-arm statute.\textsuperscript{9} A defendant’s contacts could be sporadic or isolated, but if the cause of action arises out of those contacts and they are at least “minimum contacts,”\textsuperscript{10} specific jurisdiction may be appropriate because the defendant had fair warning he may be sued in the foreign jurisdiction.

[b] — Traditional Jurisdictional Analysis.

A court, therefore, must determine whether the defendant has “minimum contacts” with the forum. This is accomplished by a two-step analysis. First, the plaintiff must show that the defendant had the “minimum contacts with the forum necessary for the defendant to reasonably anticipate being haled into court there.”\textsuperscript{11} The Court has developed a number of factors to consider when determining whether minimum contacts have been met, such as (1) whether the defendant “purposefully directs his activities at residents of the forum and whether the litigation results from alleged injuries that arise out of or relate to

\begin{itemize}
  \item \textsuperscript{6} Id.
  \item \textsuperscript{7} Id. at 414-416.
  \item \textsuperscript{8} Hanson v. Denkla, 357 U.S. 235 (1958).
  \item \textsuperscript{9} Doe v. Unocal Corp., 248 F.3d 915, 923 (9th Cir. 2001).
  \item \textsuperscript{10} International Shoe Co. v. Washington, 326 U.S. 310 (1945).
  \item \textsuperscript{11} World Wide Volkswagen Corp. v. Woodson, 449 U.S. 286, 297 (1980).
\end{itemize}
those activities;”\(^\text{12}\) (2) whether the defendant “purposefully availed itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws;”\(^\text{13}\) and (3) whether the “defendant’s conduct and connections with the forum State are such that he should reasonably anticipate being haled into court there.” \(^\text{14}\)

In addition, a court must determine whether the assertion of jurisdiction “would comport with the traditional notions of fair play and substantial justice.”\(^\text{15}\) In \textit{Burger King}, the Court stated that meeting the minimum contacts portion of the test would make it “presumptively not unreasonable to require the defendant to submit to the burdens of litigation in that forum.”\(^\text{16}\) This presumption can be enhanced or overcome by the application of the “fair play and substantial justice” factors. Those factors are (1) the burden on the defendant to defend in the foreign jurisdiction; (2) the adjudicative interest of the forum state; (3) the plaintiff’s interests in obtaining convenient and effective relief; (4) the court’s interest in obtaining the most efficient resolution to the controversies; and (5) shared interest of the states in furthering substantial social policies.\(^\text{17}\)


The Supreme Court has also established a number of factors to consider when determining whether jurisdiction is proper through a stream of commerce theory. In \textit{Asahi Metal Industries Co. v. Superior Court}, the Court was divided into two conflicting four-Justice pluralities.\(^\text{18}\) In her opinion, Justice O’Connor concluded that, “the placement of a product into the stream of commerce without more is not an act of the defendant purposefully directed toward the forum state.”\(^\text{19}\) Moreover, “additional

---

14 Burger King Corp., 471 U.S. at 473.
16 471 U.S. at 476.
17 World Wide Volkswagen Corp., 449 U.S. at 292.
19 Id. at 112.
conduct of the defendant” such as advertising or marketing specifically in the forum, may be sufficient to establish minimum contacts. Justice O’Connor’s opinion has become recognized as the authority in stream of commerce cases, particularly when the cases involve electronic streams of commerce and the Internet.


The rise of the Internet has added a new wrinkle to the world of personal jurisdiction. Thus far, courts have generally applied the traditional tenets of personal jurisdiction doctrine to the world of the Internet. Courts still look to the state long arm statute to determine whether the exercise of personal jurisdiction over non-residents would be permissible under state law. If jurisdiction is proper under the state long-arm statute, courts then determine whether the exercise of personal jurisdiction would satisfy the Constitution. Central to that analysis is whether the defendant has contacts with the state that would lead the defendant to reasonably anticipate being haled into court in the forum state.

Today, with the increasing popularity of the Internet and the relative ease of access, courts have been forced to consider to what extent “electronic contacts” should be considered in the process of establishing a defendant’s contacts with the forum state. The difficulty with determining whether contacts are sufficient to satisfy the fair play and substantial justice test is tied directly to the essence of the Internet because the Internet is boundless and ever present in nearly every jurisdiction conceivable. This could arguably subject every Web site operator to suit across the nation and worldwide. Courts have yet to come to a definitive answer as to what level of Internet contact would be sufficient to establish personal jurisdiction, but they have carved out three levels of electronic contact to consider when assessing whether personal jurisdiction exists.

The first level of electronic contact recognized by the courts occurs when a defendant clearly does business over the Internet with either individuals or corporations within the forum state. In these instances, all

\[20\] Id.
courts have found personal jurisdiction to be proper. The second level of
electronic contact occurs when a user in the forum state exchanges
information with the defendant through the defendant’s Web site. In these
instances, jurisdiction has been determined by examining the level of
interactivity and the commercial nature of the exchange that occurs through
the Web site. The final level of electronic contact recognized by the court
occurs when the defendant posts information or advertisements on an
Internet Web site that is accessible to users both within and outside the
forum state. Courts have generally found jurisdiction does not exist in
these cases. Exercising jurisdiction over these types of Web sites would
create nationwide jurisdiction for any individual or business that has a
presence on the Internet. The law has not followed this draconian approach.

[b] — Zippo and Its Legacy.

Undoubtedly, the most important, significant and oft-cited Internet
jurisdiction case to have been decided thus far is Zippo Manufacturing
Co. v. Zippo Dot Com, Inc. In that case, the plaintiff, a Pennsylvania
Corporation whose principle place of business is located in Bradford,
Pennsylvania, commenced a trademark infringement and false designation
suit against Zippo Dot Com, Inc., a California Corporation with its
principle place of business located in Sunnyvale, California. Zippo Dot
Com operated an Internet news service and had registered domain names
“zippo.com,” “zippo.net,” and “zipponews.com” as its Web addresses.

An individual who wanted to subscribe to the defendant’s newsgroup
service had to fill out an on line application and either pay the defendant
through the Web site or over the phone. Zippo Dot Com would, after
payment, issue a password to the users that would enable them to download
the newsgroup files of their choice from the defendant’s server in
California. The only contacts the defendant had with Pennsylvania were

22 Id. at 1121.
23 Id.
24 Id.
25 Id.
through its Web site. The defendant had approximately 3000 subscribers from Pennsylvania, which constituted about two percent of its total subscribers. In order to be able to reach those 3000 customers, the defendant entered into contracts with seven Internet Server Providers (ISPs) from Pennsylvania, two that resided within the Western District of Pennsylvania.

Zippo Dot Com moved for dismissal based on the lack of personal jurisdiction. The court denied the motion, holding that the defendant’s “conducting of electronic commerce with Pennsylvania residents, constitutes the purposeful availment of doing business in Pennsylvania.” Moreover, the court found that personal jurisdiction comported with “traditional notions of fair play and substantial justice,” relying on Zippo Dot Com’s 3000 Pennsylvania’s subscribers and the seven contracts it had entered into with local ISPs.

While the conclusion of the court in Zippo is important, the most significant portion of the decision was the court’s Web site analysis. The test used in Zippo, which has been cited in nearly every Internet jurisdiction case that has followed Zippo, provides a straightforward method to determine whether jurisdiction could be properly applied to a Web site based upon the manner in which the Web site interacts with the user. The court opined:

. . . the likelihood that personal jurisdiction can be Constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well-developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into any contracts with residents of a foreign

---

26 Id.
27 Id. at 1121.
28 Id.
29 Id.
30 Id. at 1125-1126.
31 Id. at 1121.
jurisdiction that involved the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end of the spectrum are situations where a defendant has simply posted information on an Internet Web site that is accessible to users in the foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it are not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In those cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.\textsuperscript{32}

Most Web sites fall into the middle category. Under the middle category analysis, the courts have used broad discretion to determine on a case-by-case basis whether the level of interactivity and commercial nature of the information is such that the exercise of personal jurisdiction is warranted.

\textbf{[b] — Another Approach to Internet Jurisdiction: the Effects Test and Panavision.}

In 1984, the Supreme Court expressly approved the effects test in \textit{Calder v. Jones}.\textsuperscript{33} In that case, the Court upheld jurisdiction in California over two Florida individuals because their activity in Florida was deliberately targeted, and calculated to cause injury to the California plaintiff.\textsuperscript{34} The Florida individuals were the authors of a libelous article published in the \textit{National Enquirer}.\textsuperscript{35} Neither individual had any contact with California and, therefore, the court had no basis to hold that either of the individuals purposefully availed themselves to the benefits and protections of California law.\textsuperscript{36} However, the court held it was reasonably

\begin{itemize}
  \item \textsuperscript{32} \textit{Id.} at 1124.
  \item \textsuperscript{34} \textit{Id.} at 787 n. 6, 788-789.
  \item \textsuperscript{35} \textit{Id.}
  \item \textsuperscript{36} \textit{Id.}
\end{itemize}
foreseeable that the conduct by the defendants in Florida would cause harm in California. Therefore, because they aimed their conduct intentionally at California knowing that the subject of their story would be harmed there, the defendants should have “reasonably anticipated being haled into court” in California. In sum, the effects test can be applied if a non-resident defendant deliberately directs activity toward the forum state in a calculated effort to cause harm to a plaintiff residing there. Under those circumstances, the defendant should reasonably anticipate being haled to court in the plaintiff’s forum. The “effects test” is at the center of many of the controversies that arise in jurisdictional disputes arising from the use of the Internet.

One of the more significant Internet jurisdiction cases, and the leading Internet effects test case, is Panavision International, L.P. v. Toeppen. In that case, Panavision, a Delaware limited partnership based in California and the holder of trademarks to the names “Panavision” and “Panaflex,” sued a citizen of Illinois, Dennis Toeppen, for dilution and infringement of their trademark by registering the domain names “panavision.com” and “panaflex.com,” for use on his Web sites. Panavision requested that Toeppen give up his right to “panavision.com” and transfer it to them, but Toeppen refused and instead demanded that Panavision pay $13,000 for the domain name. Panavision refused Toeppen’s demand. Toeppen subsequently registered “panaflex.com” and displayed the word “Hello” at that site. After Panavision discovered that Toeppen had also registered “panaflex.com,” the suit followed. The district court held that it had jurisdiction over Toeppen in California. Toeppen appealed and the Ninth

37 Id. at 790.
38 Id. at 787 n.6.
39 Panavision Int’l, L.P. v. Toeppen, 114 F.3d 1316 (9th Cir. 1998).
40 Id. at 1318-1319.
41 Id. at 1318.
42 Id. at 1319.
43 Id.
44 Id. at 1319.
45 Id.
Circuit affirmed. The Ninth Circuit held that in tortious injury cases like this, “jurisdiction may attach if the defendant’s conduct is aimed at or has an effect in the forum state.” In so holding, the court noted that Toeppen “purposefully registered” Panavision’s trademarks as his own domain name in order to force Panavision to pay him money for the right to the domain names he registered. Furthermore, the “harm was felt in California” and Toeppen knew the plaintiff would suffer some harm because even though Panavision was a Delaware limited partnership, “its principle place of business was California, and the heart of the theatrical motion picture and television industry is located there.”

The court noted that the act of registering another’s trademark as a domain name and posting information on the Internet under that domain name does not subject a non-resident to personal jurisdiction in the forum state without some demonstration that the defendant directed his activity to the forum state. In this case, the Ninth Circuit found that Toeppen’s efforts to extort money from Panavision met the directed activity standard and concluded that Toeppen’s conduct in Illinois was designed to, and in fact did cause injury to the plaintiff in California.

Many plaintiffs attempt to invoke Panavision’s “effects test” when trying to establish personal jurisdiction over non-resident defendants. However, courts are more inclined to use Zippo’s sliding scale approach rather than Panavision’s “effects test” when adjudicating personal jurisdictional disputes.


It is Zippo and its progeny, therefore, that largely control the ability of a plaintiff to hale an out-of-state party into court based on a defendant’s Internet presence.

---

46 Id. at 1327.  
47 Id.  
48 Id. at 1321.  
49 Panavision at 1322.  
50 Id.
[a] — The Mink Case.

David Mink (Mink), a Texas resident, claimed to be developing a computer program, the Opportunity Tracking Computer System (OTC), to track information on sales and opportunities missed on sales not made. Mink alleged that AAAA Development, LLC (AAAA) conspired with another company and a single individual to copy his copyrighted and patent pending system. AAAA is a Vermont corporation with its principle place of business in Vermont. AAAA owns no property in Texas, has made no sales in Texas, and has sent no agent or employee to Texas. The only tenuous contacts AAAA had with Texas was through an advertisement it placed in a national furniture trade journal and through its Web site that advertised its sales management software on the Internet. The district court granted AAAA’s motion to dismiss for a lack of personal jurisdiction and the Fifth Circuit affirmed the district court’s holding.

The Fifth Circuit held that operating a Web site without any other contacts with the forum state was not enough for personal jurisdiction to be exercised over a non-resident. The court concluded that Mink had not established any contacts related to the cause of action, a requirement for specific jurisdiction. The court went on to explicitly adopt the reasoning of Zippo.

In applying the Zippo analysis, the court concluded that the AAAA Web site was insufficient to subject it to personal jurisdiction. The AAAA Web site did nothing more than post information about its products and services. The Web site did contain a mail-in form, a toll-free number, mailing address and e-mail address, however, no orders were taken through the Web site. The court found that this type of Web site was nothing

51 Mink v. AAAA Development, LLC, 190 F. 3d 333, 334 (5th Cir. 1999).
52 Id.
53 Id. at 335.
54 Id.
55 Id. at 336.
56 Id.
57 Mink at 336.
58 Id. at 337.
more than a “passive” advertisement which was not grounds for personal jurisdiction. The court also noted that although AAAA did provide e-mail to permit interaction with customers, AAAA could do nothing but reply to these e-mails. The Web site lacked other interactive qualities such as ordering or purchasing on line, which the courts found were necessary to exercise personal jurisdiction over a non-resident defendant.

[b] — Cybersell, Inc.

Cybersell, Inc. (“Cybersell AZ”) was an Arizona corporation that provided Internet, Web advertising and marketing services. In June of 1995, Cybersell AZ applied to register “Cybersell” as a service mark and, in October 1995, its application was approved. During the summer of 1995, two Florida residents created Cybersell, Inc. (“Cybersell FL”), a Florida corporation, with its principle place of business in Orlando. Cybersell FL was to provide business-consulting services for strategic management and marketing on the Web. When Cybersell FL chose “Cybersell” as its name, Cybersell AZ had no homepage on the Web nor had their service mark been approved.

Cybersell FL established their presence on the Web with a home page displaying a “Cybersell” logo on the first page. Cybersell AZ found Cybersell FL’s homepage on the Web and notified Cybersell FL by e-mail that “Cybersell” was a service mark of Cybersell AZ. Consequently changed their name to WebHorizons, Inc., and replaced the “Cybersell” logo with a WebHorizons logo. However, Cybersell FL

59 Id.
60 Id.
61 Id.
62 Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 415 (9th Cir. 1997).
63 Id.
64 Id.
65 Id.
66 Id. at 416.
67 Cybersell at 416.
68 Id.
failed to replace the “Welcome to Cybersell!” greeting on the first page.\textsuperscript{69} Cybersell AZ then proceeded to file suit, alleging trademark infringement, unfair competition, and fraud.\textsuperscript{70} Cybersell FL moved to dismiss for a lack of personal jurisdiction.\textsuperscript{71} The district court granted Cybersell FL’s motion and the Ninth Circuit affirmed.\textsuperscript{72}

The Ninth Circuit expressly adopted the \textit{Zippo} analysis that “the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet.”\textsuperscript{73} The court held that the contacts of Cybersell FL with Arizona were insufficient to establish personal jurisdiction because it conducted no commercial activity over the Internet, no part of its business was sought or achieved in Arizona, no citizen of Arizona signed up for its services, and the only demonstrable contact was an e-mail sent to Cybersell FL by Cybersell AZ.\textsuperscript{74} Cybersell FL posted a passive Web site with the name “Cybersell.” The fact that anyone in Arizona could access that Web site and learn of the services offered was not enough, without more, to infer that Cybersell FL deliberately directed its merchandising efforts toward Arizona residents.\textsuperscript{75} In short, Cybersell FL had performed “no act, consummated no transaction, nor had it performed any act by which it had purposefully availed itself the privilege of conducting activities in Arizona.”\textsuperscript{76}

Cybersell AZ argued, alternatively, that the “effects test” should apply because Cybersell FL should have reasonably foreseen the injury it would have caused to Cybersell AZ by using its service mark.\textsuperscript{77} The court disagreed. The court reasoned that the focal point of the injury in this

\textsuperscript{69} Id.
\textsuperscript{70} Id.
\textsuperscript{71} Id.
\textsuperscript{72} Id. at 415.
\textsuperscript{73} \textit{Cybersell} at 419.
\textsuperscript{74} Id.
\textsuperscript{75} Id.
\textsuperscript{76} Id. at 420.
\textsuperscript{77} Id. at 420.
case was not clear as it was in Calder, and furthermore, the “effects test” did not apply with the same force to a corporation like Cybersell AZ as it would to an individual because a corporation “does not suffer harm in a particular geographic location in the same sense that an individual does.”

In this case, Cybersell FL’s Web site was not aimed intentionally at Arizona with knowledge Cybersell AZ was likely to be harmed.


The Bensusan Restaurant Company (BRC), a New York corporation, was the creator of a New York City Jazz club known as “The Blue Note.”

BRC owned all rights, title and interest in and to the federally registered trademark, “The Blue Note.”

Richard King (“King”), an individual who resided in Columbia, Missouri, owned and operated a small club in Columbia that was also called “The Blue Note.”

In April of 1996, King posted a Web site to promote his club with a logo that was substantially similar to the logo used by BRC. King’s site was available to anyone worldwide that had access to the Internet. The page itself contained general information about the club in Missouri, a calendar of events and ticketing information. The information included the addresses of ticketing outlets in Missouri and a telephone number in Missouri for charges by phone.

BRC brought suit alleging trademark infringement, trademark dilution and unfair competition. King moved for dismissal based on a lack of personal jurisdiction. The court, ruling on King’s motion, found “the mere fact that a person can gain access to information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product to New York.”

---

78 Cybersell at 420.
79 Id.
81 Id.
82 Id.
83 Id.
84 Id.
85 Id. at 298.
court reasoned that King had done nothing to purposefully avail himself of the benefits of New York and although “creating a Web site, like placing a product in to the stream of commerce, may be felt nationally or worldwide it is not an act purposefully directed toward the forum state.”

King’s only presence in New York was his Web site and that fact, “without more,” was not enough for the forum state to constitutionally exercise jurisdiction over a non-resident.


The first case dealing with personal jurisdiction in relation to a commercial Web site was *CompuServe, Inc. v. Patterson*. CompuServe was a computer information service headquartered in Columbus, Ohio that contracted with individual subscribers to provide access to computing and information services via the Internet. Richard Patterson, an attorney and a resident of Houston, Texas, did business as Flashpoint Development. Patterson subscribed to CompuServe and placed shareware items (programs that can be downloaded) on the CompuServe system for other CompuServe subscribers to download. When he became a shareware provider, Patterson entered into a “Shareware Registration Agreement” (SRA) with CompuServe that created an independent contractor relationship, and also incorporated by reference the CompuServe Service Agreement and the Rules of Operation. The SRA and the Service Agreement explicitly stated that the contract was entered into in Ohio and was to “be governed by and construed in accordance” with Ohio law.

---

86 *Id. at 301* (citing Asahi Metals Indus. Co. v. Superior Court, 480 U.S. 102, 112 (1986)).
87 *Id.*
88 *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996).
89 *Id. at 1260.*
90 *Id.*
91 *Id.*
92 *Id.*
93 *Id.*
Patterson’s software was a program designed to help people navigate the Internet. CompuServe began to market a similar product with markings and names that Patterson took to be too similar to his own. After contacting CompuServe, the name was changed, but Patterson was still not satisfied. CompuServe filed for a declaratory judgment in the Southern District of Ohio and Patterson moved to dismiss for a lack of personal jurisdiction. The district court granted his motion.

The Sixth Circuit reversed the district court’s decision and found that personal jurisdiction existed. The court concluded that Patterson had knowingly made an effort, and in fact, purposefully contracted to market a product in other states with the Ohio-based CompuServe as his distribution center. Further, the court concluded that Patterson had purposefully availed himself to the benefits and protections of Ohio’s laws on a number of levels. The court held that Patterson had entered into contracts in Ohio (the SRA and Service Agreement), sent his software via electronic links to the CompuServe system in Ohio, and advertised the software on the CompuServe system. Furthermore, the court found Patterson deliberately set into motion an ongoing marketing relationship with CompuServe and, by doing so should have reasonably foreseen the possible consequences in Ohio. The court also held that entering into the contract would not be sufficient for minimum contacts and, similarly, Patterson’s injection of his software into the stream of commerce would not be enough for personal jurisdiction; with both, the exercise of personal jurisdiction was reasonable.

---

94 CompuServe at 1261.  
95 Id.  
96 Id.  
97 Id.  
98 Id.  
99 Id. at 1263.  
100 Id.  
101 Id. at 1264.  
102 Id.  
103 Id.
§ 5.02


[a] — People Solutions.

People Solutions, Inc., a Texas-based company providing human resource services (“PSTX”), registered the servicemark “People Solutions” with the United States Patent and Trademark Office. People Solutions, Inc., a California-based human resource company (“PSCA”), developed a Web site using the “people solutions” name. The PSCA site contained a number of interactive pages that included such things as performance tests, product demonstrations, order forms for products, and the ability to order brochures. However, PSCA did not sell any products exclusively through its Web site, nor did it sell any product to a resident of Texas through its Web site, although it did have a Texas-based client. PSTX sued PSCA alleging trademark infringement, unfair competition, and injury to business reputation. The court applied the Zippo analysis and held that PSCA’s Web site fell in the middle range of the Zippo spectrum. Consequently, the exercise of personal jurisdiction was to be determined by the level of interactivity and the commercial nature of the exchange of information conducted on the Web site. With this standard, the court found that the defendant’s Web site did not rise to the level of interactivity sufficient to submit PSCA to Texas’ jurisdiction. The court noted that although the Web site had the “potential to interact with, sell products to, and contract with Texas residents,” the level of Texas-based commercial activity actually achieved by the defendant on its Web site was inadequate to establish personal jurisdiction.

105 Id. at *3.
106 Id. at *10.
107 Id. at *3.
108 Id. at *13.
109 Id.
110 Id. at *12.
American Eyewear, Inc. (“American”) a Texas corporation based in Dallas, registered the trademark “Peeper’s” in connection with its retail optical business. Peeper’s Sunglasses and Accessories, Inc. (Peeper’s), a Minnesota retail optical firm, registered the domain names “peepers.com” and “peepers2000.com” to sell its products online. American sued Peeper’s for unfair competition and trademark infringement, while Peeper’s moved to dismiss for lack of personal jurisdiction.

Peeper’s had no offices, sales representative or agents in Texas, it did not own property in Texas, it did not have a bank account in Texas and it did not market or advertise its products in Texas. The only connection that Peeper’s had with Texas was through its Web site. Peeper’s Web site allowed customers to purchase items directly from the Internet. More importantly, Peeper’s regularly sold products to Texas customers through its Web site and, during a period of time in 1999, sales to Texans “occurred almost daily and typically involved multiple transactions each day,” although those sales constituted fewer than half of one percent of Peeper’s total sales.

The court held that the exercise of personal jurisdiction over Peeper’s was proper. It concluded that under the Zippo analysis, the Web site was at the upper end of the interactivity continuum but not a per se commercial Web site. The court then further examined the Web site to determine if personal jurisdiction was proper. The court held that jurisdiction was proper because the site could be used by Texas residents.

---

112 Id.
113 Id.
114 Id. at 897.
115 Id. at 898.
116 Id.
117 American Eyewear at 898.
118 Id. at 903.
119 Id. at 901.
to submit orders and communicate directly with Peeper’s customer service department, and because of a statement by a Peeper’s executive that the company “tries to reach every person, including all Texans, who have Internet access, and to provide them with the opportunity to purchase Peeper’s products from anywhere, at any time.”

Interestingly, the court suggested what actions Peeper’s could have taken to avoid jurisdiction in Texas. If Peeper’s had designed its Web site to block orders from or deliveries to Texas residents, included a disclaimer on its site advising consumers that it would not accept orders from a Texas resident, or incorporated a “click wrap” agreement in its Web site that included a choice of venue clause, jurisdiction in Texas would not be proper.


The Internet’s global reach often times will lead to international jurisdictional disputes. The following cases are representative of those disputes.

[a] — Ty, Inc. v. Clark.

Ty, Inc., the maker of Beanie Babies, brought a trademark infringement, unfair competition, consumer fraud and deceptive trade practices action against Clark, who is based in Cheshire, England, because Clark sold Beanie Babies through a Web site called beaniebabiesuk.com. The Web site was available worldwide and contained an e-mail link through which users could obtain product information, although they could not order directly through the Web site. To place an order, the customer had to print an order form from the Web site and either phone, fax or mail a completed form to the United Kingdom.

---

120 Id.
121 Id. at 904.
123 Id. at *2.
124 Id.
Ty, Inc argued that personal jurisdiction was proper in the Northern District of Illinois because the Web site amounted to a transaction of business in Illinois. The court disagreed and dismissed the case pursuant to Clark’s motion to dismiss for a lack of personal jurisdiction. The court found that the Web site was not completely passive because its e-mail link enabled customers to contact the defendant with inquiries related to products and orderings, but the interactivity was tempered because customers could not place orders over the Internet. The court said that without something more than an e-mail link, jurisdiction over a foreign defendant would not be proper.

[b] — Euromarket Design, Inc. v. Crate and Barrel, Ltd.

Euromarket Design, Inc., or more specifically, Crate & Barrel, was an Illinois corporation with its principle place of business in Northbrook, Illinois. Crate & Barrel was the owner of the trademarks and servicemarks “Crate and Barrel” and “Crate & Barrel,” and has subsequently established “crateandbarrel.com” to sell its product on the Internet. Crate and Barrel, Ltd. (“Limited”) is a corporation organized under the law of the Republic of Ireland with its principal place of business in Dublin, Ireland. Limited has an established retail store in Dublin, has a “Crate and Barrel” sign prominently displayed outside its store and a Web site (“www.crateandbarrel-ie.com”) that allows visitors to browse an online catalog and purchase directly through the Web site for delivery to the United States. Beyond this Internet contact, Limited also had a

125 Id.
126 Id. at *4.
127 Id. at *3.
128 Id. at *4.
130 Id.
131 Id. at 829.
132 Id.
number of non-Internet contacts with Illinois as it (1) purchased goods from vendors in Illinois and elsewhere in America; (2) participated in trade shows in the United States and Illinois to promote its business; (3) advertised in publications that were circulated in the United States and Illinois; and (4) sold goods to an Illinois resident via its Web site. Limited moved to dismiss for a lack of personal jurisdiction, but the court denied Limited’s motion and found that Limited should be subject to personal jurisdiction in Illinois.

The court adopted the Zippo analysis and found that Limited’s Web site fell in the commercial Web site category in which Limited entered into contracts with residents of the foreign jurisdiction. Further, Limited purposefully and deliberately designed and maintained a Web site with a high level of interactivity, enabling customers to browse on line catalogs and place orders via the Internet. The court held that these contacts alone would most likely be enough to exercise personal jurisdiction over the non-residents, but it also looked to the non-Internet related activities of Limited (listed above) and held that through both the Internet and non-Internet related activities, Limited had “deliberately developed and maintained not only minimum, but significant contacts with the forum.”

Whether personal jurisdiction will be triggered in a foreign jurisdiction based on defendant’s Internet presence will largely be determined as a function of the level of interactivity the Web site provides with the Web site users. Web sites that provide only information that are akin to advertisements do not provide the level of contacts necessary for a court to constitutionally exercise in personam jurisdiction. On the other hand, Web sites that sell products in foreign jurisdictions and communicate with users via e-mail have been found to provide the contacts necessary for personal jurisdiction because the Web site operator is deemed to have

133 Id.
134 Id. at 838.
135 Id.
136 Euromarket Design at 839.
availed itself to the protections of the laws of the foreign jurisdiction. Personal jurisdiction on the Internet is merely an extension of traditional personal jurisdiction precedent. It is applied in a similar manner, but lends more credence to contacts that in the past may have been considered too tenuous for the proper exercise of personal jurisdiction. A business should be aware of the possibility that its Web site might allow a lawsuit to proceed far from home. If the Internet is generating sufficient business, this may be a risk worth taking. If an organization wants to reduce that risk, it could alter its Internet presence with the interactivity principle of Zippo in mind. Alternatively, a business could include language on the Web site which identifies a forum for lawsuits. This approach, however, will not effectively present a suit brought by a party that did not enter into a contract pursuant to the Web site.

Businesses that run a Web site that do more than advertise should be aware of the risk that it may be subject to suit in distant places. The less commercial the site and the less interactive the site, the less likely a Web operator will face litigation at lengthy distances. In addition, careful crafting of the Web site language may reduce the risk of being dragged into a far-away court.

§ 5.03. Domain Names.

Much of the Internet-related litigation has been based on domain name disputes. The availability and use of the right domain name can be critical to an organization’s ability to market and sell products and services. No matter the industry, the right domain name can be an important part of the sales, marketing and other functions of a business. This section of the chapter will summarize the statutes designed to prevent the improper appropriation and use of a domain name and domain name litigation.

Domain names are the unique names that identify an Internet Web site.\textsuperscript{137} Domain names always have two or more parts separated by a dot.\textsuperscript{138} The portion to the right of the dot is the most specific part of the


\textsuperscript{138} \textit{Id.}
domain name, while the portion to the left is the most general.\footnote{Id.} A given domain name directs an Internet user to retrieve the information housed on one single machine.\footnote{Id.} A Uniform Resource Locator (“URL”) is the standard way to enter an Internet address into a Web browser.\footnote{Id.} A URL looks like “http://www.bccz.com” and includes the domain name (“BCCZ”) of the target site.\footnote{Id.} An IP Address or IP Number is sometimes referred to as a dotted quad.\footnote{Id.} It is a unique set of numbers consisting of four parts separated by dots such as “165.113.245.3.”\footnote{Glossary of Internet Terms.} IP Numbers, URLs and domain names are all related.\footnote{Id.} The URL, including the domain name, entered into an Internet Web browser is just a pseudonym for the IP Address. It is much easier to remember that the address for MTV on the Internet is “www.mtv.com,” not “152.654.251.32.” It eliminates confusion and makes a Web site more likely to be visited.


In the past, the Internet was ruled like a monarchy with strong ties to the United States government.\footnote{Id.} The Internet (then called ARAPNet) was born in 1969 at the University of California by a small group of graduate students led by Jon Postel.\footnote{Id.} Postel helped design the Internet Protocol (IP) system, that enabled a computer from ARAPNet to communicate with computers on another network maintained by the National Science Foundation (NSF).\footnote{Id.} In response to the difficulty in remembering the long numbered IP addresses, Postel invented domain

\footnote{“Developments in the Law – The Law of Cyberspace,” 112 Harv. L. Rev. 1657, 1660 (1999).}
names. These names were initially just names given to each computer to assist in remembering the long numbered IP addresses. Each computer had a file that would translate the name entered into the series of numbers that was the IP address. By the 1980s, it became unwieldy to update each computer’s IP address file, so Postel separated the nicknames given to each computer into groups called domains. These domains were separated into two groups: National domains like “.ca” for Canada or “.us” for the United States or generic domains like “.com” or “.edu.” A separate computer (root server) administered each domain and directed traffic among domains.

Postel established the Internet Assigned Number Authority (IANA) to run the root server network. He made all administrative decisions and also assigned IP addresses to correlating domain names. Several non-profit advisory boards assisted Postel in defining Internet policies. Organizations like the Internet Society (ISOC) assisted Postel by issuing policy documents, called Requests for Comment, that allowed Internet policies to be molded by the individuals who used it, truly making the early days of Internet governance an open, informal and consensus based style.

By the early 1990s, with an increased demand by businesses and other organizations for new domain names, IANA and Postel were completely overwhelmed. Congress asked that NSF outsource domain name management to the private sector. NSF selected Network Solutions,
Inc. (NSI) to develop a management system that would assign new domain names in the popular “.com,” “.org,” and “.net” domains as well as operate a new root server.  

NSI’s monopoly on domain name registration eventually proved to be unpopular. Complaints were made because users had no alternative place to register their names and no new registrars were allowed to enter the domain names business. Others complained about the customer service provided by NSI. Considerable controversy had also arisen in the relationship between trademarks and domain names. NSI did not face this issue head on and instead adopted policies that were designed to eliminate its own liability. NSI took the position that domain names would be issued on a “first come, first served” basis. NSI refused to consider whether a new registration could infringe on the intellectual property rights of any third party. NSI’s policy stated that “NSI may revoke, suspend, transfer, or modify a domain name registration that is shown to interfere with a federally registered trademark,” but unless the owner of the trademark brought the infringement action to the NSI’s attention, nothing was done. This policy led to the explosion of “cybersquatting,” the registration of a mark with the purpose of extorting money from the holder of the mark for its unrestricted use.

[2] — NSI to ICANN.

NSI’s contract with the U.S. government came to a close in 1998. This event brought a whirlwind of debate in the Internet community as to how the domain name system should be reformed.

Postel proposed the addition of up to 200 new generic top-level domain names (“TLD”s) in order to dilute the importance of having the “.com”

161 Id.
162 Id. at 1663.
163 Id.
164 Id.
165 Id. at 1664.
166 Id.
167 Id.
168 Id. at 1665.
domain and to multiply the number of names available in the registry.\textsuperscript{169} Following Postel’s lead, ISOC and IANA formed an organization to develop a plan for the domain naming system.\textsuperscript{170} The result of this was the Generic Top-Level Domain Name Space Memorandum of Understanding (“Memorandum”), which called for the establishment of seven new top-level domain names operated by a consortium of private domain name registrars.\textsuperscript{171} The Memorandum has been criticized for three reasons: critics questioned the authority under which the recommendations were made;\textsuperscript{172} critics challenged the accountability of the system because it seemed to give the IANA additional control, and thereby put the power in the hands of academics when the Internet was becoming increasingly commercial;\textsuperscript{173} and finally, many individuals believed that the expansion of TLD names needed to be a more organized and thoughtful process, rather than a gluttony of new names, as Postel had advocated.\textsuperscript{174} In January 1998, the United States government became involved in the domain name reform debate when the Clinton Administration, more specifically the Department of Commerce, issued the “Green Paper,” an initial draft of the plan for the domain name system.\textsuperscript{175} The Green Paper proposed a plan for transferring control of the domain name system from the federal government to the private sector. It recommended the formation of a US-based non-profit corporation to run the domain name system.\textsuperscript{176} In addition, the Green Paper also advocated the immediate creation of new TLDs and competing registrars and registries.\textsuperscript{177}

\begin{itemize}
\item \textsuperscript{169} Id.
\item \textsuperscript{170} Id.
\item \textsuperscript{171} Id. at 1666.
\item \textsuperscript{172} Id.
\item \textsuperscript{173} Id.
\item \textsuperscript{174} Id.
\item \textsuperscript{175} Id.
\item \textsuperscript{176} Id.
\item \textsuperscript{177} Id.
\end{itemize}
The Green Paper was subjected to many public comments and was changed dramatically to what is known as the “White Paper.” 178 The White Paper, unlike the Green Paper’s top-down solution, reflected the established norms and customs of the Internet.179 The White Paper advocated that the development of a new domain names system should be stable, competitive, and coordinated from the bottom up.180 Like the Green Paper, the White Paper advocated the creation of a non-profit corporation to coordinate key Internet functions, such as managing IP addresses and root servers, increasing the number of top-level domains and setting protocol parameters.181 The company would be incorporated and based in the U.S.; however, the board of the corporation would be representative of the world as a whole.182 Official government representation would not be permitted on the board, but governments and intergovernmental organizations would be encouraged to participate in the corporation as Internet users or non-voting advisors.183 The White Paper also suggested that the corporation should govern itself via a “transparent decision making process” that would protect it from “capture” by self-interested factions.184

The White Paper’s most important change from the Green Paper was the proposed treatment of trademark issues. First, the paper stated that current and prospective holders of trademarks should have access to a searchable database of registered domain names in order to avoid potential conflicts.185 Next, the paper recognized cybersquatting as a real concern and asked the World Intellectual Property Organization (WIPO) to devise a means by which a uniform approach to domain name disputes could be undertaken.186 Finally, the paper outlined steps for the transfer of control

---

178 Id.
179 Id.
180 Id.
181 Id. at 1668.
182 Id.
183 Id.
184 Id.
185 Id.
186 Id. at 1669.
from NSI to the private sector and to ensure competition among domain name registrars.  

[3] — Internet Corporation for Assigned Names and Numbers.

Once the White Paper became accepted, the Internet community faced the task of preparing for privatization. In so doing, a broad based coalition of Internet associations, including the NSI and ISOC, held a worldwide forum to discuss the various implementation issues left unresolved by the White Paper.  

At the conclusion of a number of conventions held around the world, most of the Internet engineering, commercial and user communities had essentially agreed on the structure of the new corporation.  

In September 1998, Network Solutions, Inc. (NSI) and Internet Assigned Number Authority (IANA) agreed to form the Internet Corporation for Assigned Names and Numbers (ICANN).

ICANN is a California-based non-profit corporation that was formed for the purposes of “lessening the burdens of government and promoting the global public interest” in the operation and stability of the Internet by (1) coordinating the assignment of Internet and technical parameters as needed to maintain universal connectivity on the Internet; (2) performing and overseeing the functions related to the coordination of the IP address space; (3) performing and overseeing functions related to the coordination of the Internet domain name system (DNS), including developing policies for determining the circumstances in which new TLDs will be added to the DNS root server system; and (4) overseeing the operation of the Internet DNS root server system. In short, ICANN is the global consensus entity to coordinate the technical management of the Internet’s domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system.

---

187 Id.
188 Id. at 1672.
189 Id.
190 Id. at 1673.

In November 2000, ICANN chose to add seven new top level domain (TLD) names and the seven companies that would be responsible for administering them. ICANN believed that the additional TLDs would make the Internet easier to use, because entities would be placed in a specific genre-based group that should alleviate over crowding at the “.com” level. The new TLDs are restricted, meaning only groups that service or will service the areas covered by the TLD will be able to register for the new TLD.

The new TLDs that ICANN has approved for use are as follows: (1) “.aero” – Dot-aero was established for the air transportation industry to improve efficiency, safety, and regularity of air transportation worldwide; (2) “.coop” – Dot-coop is reserved for bona fide business cooperatives such as credit unions; (3) “.info” – Dot-info is an unrestricted use TLD. Anyone can use it for any purpose, however, trademark holders will have a 30-day grace period to register their marks and any disputes arising will be handled by WIPO; (4) “.Museum” – Dot-Museum is reserved only for museums; (5) “.name” – Dot-name is only for the use of individuals and only for a third level TLD such as www.jane.smith.name; (6) “.pro” – Dot-pro is the only TLD reserved for use by professionals such as doctors, lawyers, accountants, professional companies and associations; and (7) “.biz” – Dot-biz is reserved for established businesses and companies and is limited to commercial use.

The company that is administering the “.biz” TLD, NeuLevel, is charging $2,000 to register new domain names in order to prevent cybersquatting. NeuLevel also requested that ICANN amend its Domain Name Dispute resolution procedures in

---

193 Id.
194 Id.
195 Id.
196 Id.
order for a business to challenge the ownership of a “.biz” that is not being used commercially.  


Domain name registration has been the subject of much litigation. Many trademark and copyright holders have had their famous marks or words registered by individuals who have no vested interest or connection to the marks other than the possibility of financial gain. Cybersquatting occurs when an individual registers a domain name only to attempt to sell it at a profit to the rightful holder of a famous mark or even to a third party who will in turn try to sell it to the holder for a profit. Both ICANN and the Federal Government have taken steps to stop this activity. The government has enacted the Federal Trademark Anti-Dilution Act and the Federal Anti-Cybersquatting Consumer Protection Act while ICANN has adopted the Uniform Domain Name Dispute Resolution Policy.


The Federal Trademark Anti-Dilution Act (FTADA) was enacted to provide protection for trademark holders against the dilution of their famous mark by an individual’s unauthorized use by registering the trademarks as a domain name. The FTADA defines dilution as “the lessening of the capacity of a famous mark to identify and distinguish goods or services regardless of the presence or absence of: (1) Competition between the owner of the famous mark and other parties; or (2) Likelihood of confusion, mistake or deception.”

The Act purposefully defines “dilution” broadly so the requirement that there be a likelihood of mistake, confusion or deception is more easily met. A trademark holder must have a famous mark to obtain relief in the courts. The FTADA does not define what a “famous mark” is, but instead provides a non-exhaustive list of factors that includes: (1) the degree of inherent or acquired distinctiveness of the mark; (2) the duration and extent of use of the mark in connection with the goods or services with which

197 Id.
the mark is used; (3) the duration and extent of advertising and publicity of the mark; (4) the geographical extent of the trading area in which the mark is used; (5) the channels of trade for the goods or services with which the mark is used; (6) the degree of recognition of the mark in the trading areas and channels of trade of the mark’s owner and the person against whom the injunction is sought; (7) the nature and extent of the use of the same or similar mark by third parties; and (8) whether the mark is registered.\textsuperscript{199}

To succeed in obtaining an injunction, a plaintiff must show that the mark is famous, the defendant’s use of the mark occurred after the mark had become famous, and the use causes dilution of the mark.\textsuperscript{200} Generally, any suit brought under this section will only entitle the owner of the famous mark to injunctive relief.\textsuperscript{201} However, if the owner of the mark can show that the defendant willfully intended to trade on the owner’s reputation or willfully caused dilution of the famous mark, the owner of the famous mark will be entitled to money damages.\textsuperscript{202} Even if the trademark holder proves the mark is famous, if the mark is used either in comparative advertising or promotion, a non-commercial setting or in news reporting and news commentary, then relief cannot be granted.\textsuperscript{203}

[b] — Cases Under the FTADA.
   [i] — The Candyland Case.

\textit{Hasbro, Inc. v. Internet Entertainment Group, Ltd.}, was the first case to test how the FTADA applied to domain names.\textsuperscript{204} In that case, the plaintiff moved for a temporary restraining order against Internet

\textsuperscript{199} 15 U.S.C. § 1125(c).
\textsuperscript{200} 15 U.S.C. § 1125(c)(2).
\textsuperscript{201} \textit{Id.}
\textsuperscript{202} \textit{Id.}
\textsuperscript{203} 15 U.S.C. § 1125(c)(4).
Entertainment claiming, *inter alia*, trademark dilution under FTADA.\(^{205}\) The court found, based on the submissions by both parties, that Internet Entertainment had been diluting Hasbro’s CANDYLAND mark by using the name CANDYLAND to identify a sexually explicit Internet site and also by using CANDYLAND.com as a domain name. The court granted the motion and enjoined Internet Entertainment from using the name CANDYLAND or CANDYLAND.com as well as ordering the defendants to immediately remove all content from CANDYLAND.com.\(^{206}\)

[ii] — *Toys “R” Us.*

*Toys “R” Us, Inc. v. Akkaoui* was also an early test of FTADA’s application to domain names.\(^{207}\) Plaintiff moved for a preliminary injunction against defendant’s alleged trademark dilution of the plaintiff’s family of “R Us” trademarks under the FTADA. Akkaoui ran an Internet service site, “adultsrus.com,” featuring a variety of sexual devices and clothing for purchase.\(^{208}\) According to the criteria set forth in Section 1125(c)(1) of the FTADA, the court found that Toys “R” Us’ family of marks to be famous before the defendant used it in connection with adultsrus.com.\(^{209}\) Furthermore, the court found that Akkoui’s use tarnishes the Toys “R” Us family of marks by associating them with a line of sexual products that are inconsistent with the image Toys “R” Us has strived to maintain for itself. As a result, the court granted the temporary restraining order against Akkoui.

[iii] — The Children’s Place.

*TCPIP Holding Co. Inc. v. Haar Communications, Inc.* is a more recent example of the FTADA being applied to domain name use.\(^{210}\) Haar

---

205 Id. at *1.
206 Id. at *1,*2.
208 Id. at *1.
209 Id. at *2.
210 TCPIP Holding Co. v. Haar Communications, Inc., 244 F.3d 88 (2d Cir. 2001).
Communications registered 81 Internet domain names consisting of variations of the words “The Children’s Place.” The district court held that the names were likely to dilute TCPIP’s trademark and servicemark, “The Children’s Place,” in violation of FTADA. The Second Circuit reversed the district court’s decision, holding that while TCPIP’s mark was descriptive, it failed to show that its mark was famous. FTADA Section 1125(c)(1) protects the unauthorized use of the mark when it “causes dilution of the distinctive quality” of the mark. The court held that “Children’s Place” was nothing more than a descriptive phrase that trademark law considers non-distinctive and weak. In addition, the court also found that TCPIP needed to demonstrate that its mark was famous through evidence such as consumer surveys, press accounts or other evidence of fame.


In November of 1999, President Clinton signed into law the Anti-Cybersquatting Consumer Protection Act (ACPA). The ACPA creates a new cause of action for trademark holders under section (d) of the Lanham Act. The ACPA creates a cause of action for bad faith registration, trafficking or use of domain names that infringe or dilute distinctive or famous marks, as well as creating a federal cause of action for profiteering in registrations of personal names as domain names. Under the ACPA, relief is available against anyone who with bad faith intends to profit or use a domain name that (1) is identical or confusingly similar to a mark that was distinctive when the domain name was

---

211 Id. at 89.
212 Id. at 88.
213 Id. at 93.
214 Id.
215 Id. at 99.
218 Id.
registered; (2) is identical or confusingly similar or dilutive of a mark that was famous when the domain name was registered; or (3) infringes on marks or names by protected the statute.\textsuperscript{219}

The ACPA provides a list of factors to consider in determining whether bad faith is present. These factor are as follows: (1) the trademark or other intellectual property rights of the person, if any, in the domain name; (2) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person; (3) the person’s prior use, if any, of the domain name in connection with the bona fide offering of any good or service; (4) the person’s bona fide noncommercial or fair use of the mark in a site accessible under the domain name; (5) the person’s intent to divert consumers from the mark owner’s online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site; (6) the person’s offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in a bona fide offering of any goods or services, or the person’s prior conduct indicating a pattern or such conduct; (7) the person’s provision of material and misleading false contact information when applying for the registration of the domain name, the person’s intentional failure to maintain accurate contact information, or the person’s prior conduct indicating a pattern of such conduct; (8) the person’s registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and (9) the extent to which the mark incorporated on the person’s domain name registration is or is not distinctive and famous within the meaning of Section 1125(c)(3).\textsuperscript{220}

[i] — Volkswagen.

Virtual Works registered the domain name “vw.net” in October 1996. Virtual, an Internet service provider, used the domain name “vw.net” for two years. At the end of two years, Volkswagen dealerships began to make monetary offers to Virtual for its domain name. In reaction to these offers, Virtual contacted Volkswagen of American and offered to transfer “vw.net” in exchange for money. In addition, Virtual also demanded that it receive an offer within 24 hours or they would sell the domain name to the highest bidder. Following this chain of events, Volkswagen filed suit alleging that Virtual’s activities were in violation of ACPA and sought the right to use “vw.net.” The district court granted summary judgment finding that Virtual acted in bad faith. The Fourth Circuit affirmed the district court’s ruling by finding both the circumstantial and direct evidence pointed to Virtual acting in bad faith. Specifically, the court found a comment by a Virtual executive that even though it was not registering “vw.net” in order to sell it, in the future, it could be sold to Volkswagen for a substantial sum of money. Furthermore, because Virtual chose “vw.net” not solely based on its corporate initials, but rather with the hopes of one day profiting on its association with Volkswagen, a finding of bad faith was proper.

[ii] — In rem Jurisdiction Under the ACPA.

The ACPA considers a domain name to be property, and allows for in rem jurisdiction when a foreign or evasive cybersquatter makes in personam jurisdiction impossible. An in rem proceeding is appropriate if (1) the domain name violates any right of the owner of a registered or

221 Virtual Works, Inc. v. Volkswagen of America, Inc., 238 F.3d 264, 266 (2d Cir. 2001).
222 Id.
223 Id. at 267.
224 Id.
225 Id.
226 Id. at 269.
227 Id.
228 Id.
protectable trademark; and (2) the court finds the owner either (a) is not able to obtain in personum jurisdiction or (b) through due diligence was not able to find a person who would have been an allowable defendant.\textsuperscript{229} In rem proceedings can only cancel or transfer a domain name; money damages cannot be awarded.\textsuperscript{230}

In a recent in rem jurisdiction case, the Eastern District of Virginia found that the owner of a trademarked domain name had not acted in bad faith, and could continue to hold and use the domain name in question.\textsuperscript{231} Hartog Co. (Hartog), a Norwegian company, was the owner of the United States trademark of Swix. Borgin, a Swiss citizen, was the owner and operator of an Internet service provider company in Switzerland and operated under the “swix.com” moniker.\textsuperscript{232} Hartog had asked Borgin to relinquishes his rights to “swix.com,” but Borgin refused because the domain name was an integral part of his business, and without it his business would be worthless.\textsuperscript{233} Hartog brought suit under the ACPA in order to obtain possession of the “swix.com” domain name.\textsuperscript{234} The court found in rem jurisdiction over Borgin because in personam jurisdiction could not be constitutionally exercised in any judicial district.\textsuperscript{235} The court also found that Borgin’s domain name and Hartog’s trademark were confusingly similar if not identical.\textsuperscript{236} However, the court held that Borgin’s actions failed to reach the level of bad faith within the meaning of the ACPA because Borgin had a legitimate business interest in the “swix.com” domain name.\textsuperscript{237}

\textsuperscript{232} Id. at 534.
\textsuperscript{233} Id. at 535.
\textsuperscript{234} Id.
\textsuperscript{235} Id. at 536.
\textsuperscript{236} Id. at 538.
\textsuperscript{237} Id.
[d] — ICANN’s Uniform Domain Name Dispute Resolution Policies.

The ACPA, FTADA, and traditional trademark infringement laws provide remedies to those harmed by the inappropriate ownership of a domain name. However, filing suit under those provisions can be an expensive and time consuming task, especially if the defendant has substantial resources and is prepared to fight.\textsuperscript{238} ICANN provides an alternative venue for the resolution of the same rights protected under federal causes of action, but at less of a financial burden.\textsuperscript{239}

ICANN and all of its accredited registrars have agreed that all domain name disputes are subject to the new Uniform Domain Name Dispute Resolution Policy (UDRP).\textsuperscript{240} UDRP allows the registrant and the trademark holder to resolve bad faith registration disputes.\textsuperscript{241} A dispute can be filed with an ICANN-approved dispute resolution provider, most often the WIPO.\textsuperscript{242} WIPO or another dispute resolution provider will appoint a panel that can provide two remedies: (1) transfer possession of the domain name to the party with the trademark rights to that name; or (2) cancel the domain name.\textsuperscript{243}

The ICANN remedies are available for disputes concerning an alleged abusive registration of a domain name that meets the following requirements: (1) the domain name registered is identical or confusingly similar to a trademark or service mark in which the complainant has rights; (2) the domain name registrant has no rights or legitimate interest in respect to the domain name in question; and (3) the domain name has been registered and is being used in bad faith.\textsuperscript{244}

The most difficult of the three tests to prove is the bad faith prong. The panelists will consider the following to determine if bad faith

\begin{footnotesize}
\begin{enumerate}
\item Pencoske at 190.
\item Id.
\item Id.
\item Id.
\item Id.
\item Id.
\item Id.
\item Id.
\item Id. at 191.
\end{enumerate}
\end{footnotesize}
registration of a trademark has occurred: (1) circumstances indicating that the domain name was registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant which is the owner of the trademark or to a competitor of that complainant, for valuable consideration in excess of the domain name registrant’s out of pocket costs related to the domain name; (2) the domain name was registered to prevent the owner of the trademark from using the mark in a corresponding domain name; (3) the domain name was registered primarily for the purpose of disrupting the business of a competitor; and (4) by using the domain name, the domain name registrant intentionally attempted to attract for financial gain Internet users to the registrant’s Web site or other online location by causing a likelihood of confusion with the complainant’s mark.245

[i] — World Wrestling Federation.

The first case decided under the UDRP was *World Wrestling Federation Entertainment, Inc. v. Bosman.*246 Michael Bosman registered “worldwrestlingfederation.com” in October 1999.247 Three days after registering the domain name, he contacted the WWF and offered to sell, rent or otherwise transfer the domain name for valuable consideration in excess of his out of pocket expenditures to register the domain name.248 The panel found that Bosman’s registered domain name and the WWF’s trademark were identical.249 Further, the Panel found Bosman had no legitimate interest or right in the domain name and because he tried to sell it three days after registering it, Bosman had registered the domain name in bad faith.250

245 *Id.*
247 *Id.*
248 *Id.*
249 *Id.*
250 *Id.*

In *Weber-Stephen Products Co. v. Armitage Hardware*, the WIPO panel ruled that the register of the Weber’s trademark as a domain name did not act in bad faith.\textsuperscript{251} Armitage, a hardware store, owned and operated Web sites under the domain name in dispute to promote sales of Weber’s products.\textsuperscript{252} Armitage was an authorized re-seller of Weber’s products.\textsuperscript{253} In it ruling, the Panel concluded that although the Armitage’s domain name was confusingly similar to Weber’s trademark, Armitage was able to demonstrate that it had a “right or legitimate interest in respect of the domain name” because Armitage used the domain name in connection with the bona fide offering of Weber’s goods or services.\textsuperscript{254} In short, Weber failed to prove that Armitage registered and used its trademark in a domain name in bad faith.


Domain name disputes and the emergence of cybersquatting have been viewed as some of the most troublesome areas of Internet law. Initially, traditional trademark law was used to resolve cybersquatting disputes. Subsequently, Congress enacted the FTADA and the ACPA to enable courts to protect the trademark holder by relaxing the rigid standards of traditional trademark law. In addition, ICANN has implemented the UDRP with the assistance of WIPO to provide an alternative to expensive federal litigation. Consequently, it is now easier for an organization to protect and resolve domain names that have been reserved with bad faith. Because of the value of the right domain name, it is important for organizations to protect this valuable piece of intellectual property and to understand the methods by which that protection can occur.

§ 5.04. Privacy.

Since the Internet provides for the transfer of electronic information into the black box of the Web, privacy has been and will continue to be a

\textsuperscript{251} WIPO, No. D2000-01871 (May 11, 2000).
\textsuperscript{252} Id.
\textsuperscript{253} Id.
\textsuperscript{254} Id.
concern of governments, businesses and individuals. Organizations must understand the privacy implications of Internet use and be able to comply with the legislative requirements related to privacy. In the United States, there is no comprehensive privacy legislation that addresses the collection, storage, transmission or use of personal information on or from the Internet or in another business environment.255 Privacy in the U.S. is usually provided through “ad hoc” legislation by Congress, the state legislatures and through the common law.256 Although there are many laws governing the rights of individuals with respect to the government’s use of personal information, there are relatively few laws that govern the use of personally identifying information by private entities.257 This section will review certain statutes applicable to Internet privacy.


[a] — Electronic Communications Privacy Act.

The Electronic Communications Privacy Act (ECPA) is essentially the federal codification of the tort of invasion of privacy as applied to electronic communications. The ECPA makes it illegal to intercept e-mail at the point of transmission, while in transit, when stored by an e-mail router or server, or after the receipt by the intended recipient.258 In addition, the ECPA makes it illegal to intentionally intercept, disclose or use any wire, oral or electronic communication.259 Electronic communication is defined by the statute to include any transfer of signals, writing, images, sounds, data or intelligence of and nature transmitted by means such as a wire or electromagnetic system.260 Under the ECPA, it is also unlawful to access, without authorization, stored electronic communication.261 However, ECPA provides three

255 Peter Brown, Online Privacy in the US: Legislation, Cases, and Industry Standards, 637 PLI/Pat 131 (February-March 2001).
256 Id.
257 Id. at 138.
258 18 U.S.C §§ 2711, 2520.
259 18 U.S.C §§ 2710(1)(c)-(d).
260 18 U.S.C § 2710(12).
261 18 U.S.C § 2701(a).
exceptions to this rule: (1) the conduct is authorized by the party or entity providing the electronic communication service;\textsuperscript{262} (2) the conduct is authorized by users of electronic communications through the service with respect to communications sent or intended from such users;\textsuperscript{263} and (3) the conduct is authorized by certain activities of governmental or law enforcement entities.\textsuperscript{264}

[b] — Computer Fraud and Abuse Act.

The Computer Fraud and Abuse Act (CFAA) prohibits unauthorized access of a computer, either by someone acting knowingly or exceeding authorized access, to obtain information determined by the United States government to require protection.\textsuperscript{265} “Unauthorized access” is determined by establishing that an individual willfully causes or attempts to communicate, deliver, or transmit restricted data to anyone not entitled to receive it.\textsuperscript{266} A “protected computer” is one that is used exclusively by or for a financial institution or the United States government.\textsuperscript{267} Violation of the CFAA could result in a felony or misdemeanor. The felony offenses include the unauthorized access of a protected computer and actions that result in “malicious damage” which alters information or prevents the use of a protected computer.\textsuperscript{268} Anyone who knowingly traffics in computer passwords with the intent to defraud has committed a federal misdemeanor, but only if it affects interstate commerce or the computer is used by or for the government.\textsuperscript{269} Finally, in 1996, the CFAA was amended to apply to anyone who transmits viruses, programs, information or harmful code that damages protected computers.\textsuperscript{270}

\textsuperscript{262} 18 U.S.C § 2701(c)(1).
\textsuperscript{263} 18 U.S.C § 2701(c)(2).
\textsuperscript{264} 18 U.S.C § 2701(c)(3).
\textsuperscript{265} 18 U.S.C. § 1030(a)(1).
\textsuperscript{266} \textit{Id}.
\textsuperscript{267} 18 U.S.C. § 1030(e)(2)(A).
\textsuperscript{268} 18 U.S.C. § 1030(c).
\textsuperscript{269} 18 U.S.C. § 1030(a)(6).
\textsuperscript{270} 18 U.S.C. § 1030(a)(5).

The Gramm-Leach-Bliley Act (GLB) enhanced competition in the financial services industry by providing a framework for the affiliation of banks, securities firms, and other financial service providers.271 In addition, GLB required federal agencies, such as the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), and the Federal Reserve to issue regulations for implementing notice requirements and restrictions on a financial institution’s ability to disclose non-public personal information about consumers to non-affiliated third parties.272

In May of 2000, the FTC issued its final rule concerning the privacy of consumer financial information.273 The FTC rule applies to information about individuals who inquire about and obtain a financial product or service from a financial institution covered by GLB. Specifically, the rule sets forth the requirement that (1) a financial institution provide notice to consumers about its privacy policies and practices; (2) a financial institution must disclose nonpublic personal information about a consumer to a nonaffiliated third party in certain circumstances; and (3) consumers can “opt out” of having their information disclosed to unaffiliated third parties.274 The SEC and Federal Reserve have also issued rules concerning the privacy of consumer financial information.275 Their rules are substantively similar to the FTC rules.


The Child On-line Privacy Protection Act (COPPA) directed the FTC to promulgate rules for the online collection and use of information concerning children under the age of 13.276 The final rule was issued in October 1999,277 COPPA and the rule apply to Web sites directed to, or

271 Brown at 142.
274 Id.
275 15 C.F.R. 248.
277 Brown at 145.
that knowingly collect information from, children under 13. The Web sites must give notice regarding what information is collected, how that information will be used, and whether the information will be disclosed. Web site operators are also required to obtain verifiable parental consent before collecting, using, or disclosing personal information provided by children. Operators must provide parents access to review and or delete personal information provided by their children, as well as to permit parental control over future use of the collected information. COPPA does provide a safe harbor to Web sites if they comply with industry sponsored data collection guidelines that have been approved by the FTC.

Despite the strict guidelines set forth by COPPA and the FTC, there are some exceptions to parental consent. A Web site is not required to receive parental consent before collecting or using the information from children under the age of 13 when a Web site collects the contact information (1) for the sole purpose of obtaining consent and such information is not maintained afterwards; (2) to answer, on a one-time basis, a request from the child and afterwards deleting the information and not using the information for further contact; (3) if the Web site will need to respond to more than one request from the child, the Web site must make a reasonable effort to notify the parents regarding the information requested and how it will be used after the first response and before any further responses, thus giving the parents the right to request no further contact in the future; (4) for the purpose of protecting the safety of the child and it is not to be used to contact the child, or for any other purpose, and it is not disclosed on the site, and the Web site uses reasonable efforts to give the child’s parents notice of the information collected, how it will be used and the option to request that such use be

279 Id.
281 Id.
discontinued; or (5) that it is necessary to protect the security or integrity of the Web site, to take precautions against liability, to respond to judicial process, or to the extent permitted under other provisions of law, to provide information to law enforcement agencies, and such information is not used for any other purpose.


The European Commission’s Directive on Data Protection (“Directive”) went into effect in October 1998. The Directive prohibits the transfer of personal data to Non-European Union nations that do not meet the European “adequacy” standard for privacy protection. The United States and the European Union both share the goal of enhanced privacy to protect their citizens, but both have differing approaches. The U.S. relies on a mix of legislation, government regulation and self-regulation, whereas the EU relies on comprehensive legislation that creates a data protection agency. There were fears that the Directive could be the death knell to U.S. and European Union business relations. Many were concerned that U.S. companies would not be able to carry out business with companies in the European Union because the manner in which U.S. firms handled personal data was not deemed to be adequate by the Directive.

The U.S. Department of Commerce (DOC) and the European Commission, realizing the problem that loomed ahead, developed a safe harbor framework that allows U.S. companies to avoid interruption of their business dealings with the European Union as well as avoid prosecution by European authorities under European privacy laws. United States companies that are certified under the safe harbor provisions would assure European Union organizations how the company in question would provide “adequate” privacy protection as defined by the Directive.

288 Id.
289 Id.
290 Id.
The Safe Harbor is a voluntary arrangement that involves U.S. companies signing up and adhering to a set of data protection principles similar to those that apply in the European Union. Companies can develop their own policy that meets European Union standards, or they can comply with existing U.S. sector regulations that achieve equivalent standards. Once the company implements the standards, it must self-certify its compliance with the Department of Commerce, which will then list their company name on the DOC Web site. In order to be listed, the company must comply with the seven safe harbor principles: (1) Notice – Organizations must notify individuals about the purposes for which they will collect and use information about them, provide information regarding how to contact the organization with a complaint and identify the types of third parties to which it will disclose the information; (2) Choice – Organizations must generally give individuals the opportunity to choose whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected. For sensitive information, an affirmative or explicit choice must be given if the information is to be disclosed to a third party; (3) Onward Transfer – To disclose information to a third party, organizations must apply the notice and choice principles; (4) Access – Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate; (5) Security – Organizations must take reasonable precautions to protect personal information loss, misuse, unauthorized access, disclosure, alteration and destruction; (6) Data Integrity – Personal information must be kept relevant for the purposes for which it is to be used; (7) Enforcement – In order to ensure compliance with the safe harbor principles, there must be a readily available and affordable independent recourse mechanism so that each individual’s complaints and disputes can be investigated and resolved and damages awarded where the applicable law provides.
If compliance with the safe harbor principles is not feasible, it is still possible to conduct business with the European Union. First, the U.S. entity could receive consent from the European Union citizen whose personal information will be transmitted outside the European Union. Next, a U.S.-based entity could be subjected to an “adequacy test” by the European Union entity that would transmit the protected information. In this arrangement, the European Union company would determine whether the U.S. company will adequately protect the personal data that would be transferred, and if the requisite amount of protection is found, the data exchange can occur. Finally, the U.S. and E.U. entities could enter into a contract that would require that the U.S. company comply with all sections of the Directive that pertain to the personal data the U.S. entity receives from the European Union entity.

Besides these alternative approaches, there are three exceptions to the Directive in which the personal data transmitted does not need to be protected: (1) the transfer is necessary for the performance of a contract between the individual and the company processing the data; (2) the transfer is necessary for the performance or conclusion of a contract between the company and a third party which is in the interests of the individual; and (3) the transfer is necessary for the purpose of or in connection with legal proceedings.


As a result of the fears and concerns that information shared over the Internet will be disseminated beyond the recipient of that information, many organizations have developed a privacy policy. Such a policy can put users of a Web site at ease and, consequently encourage use of the Web site. The FTC has recommended four fair information practices principles to consider when drafting a privacy policy: notice, choice, access, and security. To ensure an online user’s privacy, a Web site

---

295 Id.
296 Id. at 86.
297 Id. at 86.
298 Brown at 154-155.
operator should use these four principles as a guideline when drafting an Internet privacy policy.

[a] — Notice.

Web site operators should provide notice to on line users as to how information will be collected, what types of information will be collected, whether the information will be shared and with whom it will be shared, how it will be kept secure and how users may correct or delete previously collected information. This information should be conspicuously stated in the privacy policy and agreed to by the user before any information is collected.299

If the information collected will be shared with affiliates or non-affiliated third parties, the Web site should disclose the identities of the parties with whom the information will be shared.300 In addition, if information is collected for one purpose and then will be shared for another, Web site operators should also disclose this in their privacy policy.301

Because information can be collected from the user’s IP Address, the privacy policy should also state the purpose for which the site is collecting this information, whether the information will be used only internally or whether it will be shared with affiliates and third parties and whether the information will be given and sold to advertisers and marketers.302 Additionally, the policy should also inform users that when they post to a bulletin board or chat room hosted by the site, they have no expectation of privacy in those postings.303

Finally, the privacy policy should also inform users how updates to the privacy policy will be made to the users.304 The Web site owner could notify users directly or the site could direct them to periodically check

300 Id.
301 Id.
302 Id.
303 Id.
the policy for changes.\textsuperscript{305} The policy should state that any changes in the privacy policy would apply retroactively to all information previously collected by the site. Further, the Web site owner should also disclaim any liability regarding the use or disclosure of any information gathered by a site, other than their own, for which users may link through their site.\textsuperscript{306}

\textbf{[b] — Consent or Choice.}

Privacy policies should give users the opportunity to “opt out” or “opt in” of the various uses of their information.\textsuperscript{307} An “opt in” approach allows companies that want to share information with users for a purpose other than that for which the information was collected to obtain affirmative consent from the user before selling or sharing that information.\textsuperscript{308} An “opt out” approach places the burden on the users to inform the sites gathering the information not to share the information with others.\textsuperscript{309} In short, if a Web site is intending to use or disclose personally identifiable information for purposes other than for which the information was obtained, the site should consider having users “opt in” their consent. If a Web site is intending to use or disclose only aggregate information or anonymous information, the owner should consider providing an “opt out” option for its users.

\textbf{[c] — Access or Correction.}

Web site owners should allow users to access or review their own information retained on the site and provide them with an opportunity to correct, modify, or remove information that is inaccurate.\textsuperscript{310} However, it is up to the Web site owner to determine what information the users will be able to access. Specifically, whether the user will only be allowed to

\begin{flushleft}
\textsuperscript{305} \textit{Brown} at 156.
\textsuperscript{306} \textit{Id}
\textsuperscript{307} \textit{Id.} at 157.
\textsuperscript{308} \textit{Id}
\textsuperscript{309} \textit{Id}
\end{flushleft}
review the information they provided or whether the site will allow them to review a profile of the users developed by the site.\textsuperscript{311} The privacy policy should state what type of access users would have to their information retained by the site.\textsuperscript{312}


Web site owners who collect personally identifiable information should be required to take precautions to protect that information from being lost, stolen, or misused. Measures to limit access to confidential information should be taken to ensure that it is not being used for unauthorized purposes.\textsuperscript{313} The privacy policy should state how and where the information is stored and who has access to that information.\textsuperscript{314} In addition, the privacy policy should state whether the information transmitted by the site is secure, and if it is secure, by what means.\textsuperscript{315}

[e] — Enforcement of the FTC’s Privacy Principles.

Section Five of the Federal Trade Commission Act empowers the FTC to (1) investigate and prevent unfair methods of competition and unfair or deceptive practices affecting commerce; and (2) seek monetary redress and other relief for conduct injurious to consumers.\textsuperscript{316}

The FTC brought suit against Geocities in a 1999 case that helped establish the enforceability of FTC’s information privacy principles. The FTC alleged that Geocities misled its members by disclosing data and information to third parties in contradiction of its promise that it would not do so.\textsuperscript{317} The FTC charged that Geocities misrepresented that it alone maintained the information collected from children, when in actuality, a

\textsuperscript{311} Brown at 158.

\textsuperscript{312} Id.


\textsuperscript{314} Id.

\textsuperscript{315} Id.


\textsuperscript{317} In the Matter of Geocities, No. C-3839, 1999 FTC LEXIS 17 (FTC Feb. 19, 1999).
third party affiliate maintained that information.\textsuperscript{318} Geocities settled the case, agreeing to disclose on its Web site the information it collects, how it is collected, to whom it may be disclosed and how a consumer can view and remove their information from a third party data base. Geocities also agreed to obtain parental consent before collecting information from children.\textsuperscript{319}


Privacy is perhaps the most serious issue facing the Internet. Web sites are able to track user habits as well as compile both public and non-public information. This non-public information about users can be accessed and collected by a savvy computer hacker. Congress has acted to preserve an individual’s privacy rights on the Internet with legislative initiatives such as COPPA, GLB and CFAA. The FTC has also promulgated four principles for Web site operators to implement to better protect user privacy and to inform users what information will be collected and how it will be used. The FTC has also eliminated a massive impediment to U.S. and European Union trade by negotiating a safe harbor agreement with the European Union so that U.S. businesses will be in compliance with the strict privacy laws adopted by the EU Privacy Directive. Organizations with an Internet presence should consider whether their Web site should contain a privacy policy. This decision should be based on factors such as the nature of the site and expectation of the users of that site.

\section*{§ 5.05. Internet Security.}

The Internet has evolved to become a fundamental part of many business operations, with the clearly demonstrated ability to positively affect organizations as well as individuals. Unfortunately, the Internet was not designed with security in mind. In fact, the Internet is inherently insecure. There are some protections available to increase the security of using the Internet. For example, firewalls are used to enhance the security

\textsuperscript{318} Id.
\textsuperscript{319} Id.
of computers connected to a network such as the Internet. A firewall separates a computer from the Internet by inspecting packets of data as they arrive at either side of the firewall to determine whether it should be allowed to pass or be blocked. Firewalls act as guards to the computer’s entry points where the computer exchanges data with other devices on the network and other security programs.\textsuperscript{320}

A person who breaches a network’s security is referred to as a “hacker” (an individual who uses computer skills to test the strength and integrity of computer systems to prove their own ability or to satisfy their own curiosity about how different programs work). Persons who engage in unlawful hacking can cause serious damage and erode confidence in the safety of the Internet. Once entry into the system has been accomplished, an experienced hacker will be able to perform a number of tasks that may be adverse to the organization or business. First, and most obvious, the hacker can actually steal or alter data that is vital to the operation of the business. This theft can result in the business suffering large monetary losses. Next, a hacker could effectively knock the business’ Web site off line with what is known as a “denial of service” attack. Denial of service attacks cause Web page outages because the attacker overloads a system with useless traffic.\textsuperscript{321} The hacker could also infect the business system with a virus. A virus can enter the system through e-mail, by downloading infected software, or by using infected media such as floppy disks or CD-ROMs.\textsuperscript{322} Once the virus enters the system, it deploys its destructive payload and the result could range from an overloaded e-mail system to the removal of vital system files from the computer’s hard drive.\textsuperscript{323} Finally,

\begin{footnotesize}
\begin{enumerate}
\item[\textsuperscript{322}] \textit{Id.}
\item[\textsuperscript{323}] \textit{Id.}
\end{enumerate}
\end{footnotesize}
hackers often will access a particular organization or business’ system, not to cause havoc by damaging the system, but rather to perform less harmful damage, such as the defamation of the organization or a high ranking member of the organization by placing derogatory cyber-graffiti on the Web site.\footnote{324}


The possibility that a business with a presence on the Internet will have their security breached is very real. A business that takes a few common sense steps can minimize the risk and possible damage associated with a breach of security.

[a] — Audit.

The starting point for most organizations should be to perform an audit of their network to locate any weakness in their system and determine how these weaknesses can be addressed.\footnote{325} A comprehensive audit would require the organization to keep detailed records of all security-related events over an extended period of time to ensure that access to information on the network follows the established security policy.\footnote{326} Auditing accomplishes two important security functions: (1) to monitor network compliance of procedures established by a security policy; and (2) provide the ability to reconstruct an audit trail to determine the location or source of security-related events.\footnote{327} Auditing is an essential part of any security policy because the failure to do so could lead to substantial losses by the company. Without auditing security-related events, an organization runs the risk of not noticing a security breach until a substantial financial or data loss has occurred. However, if properly implemented, automated analysis tools and network security devices can analyze audit data and pinpoint any irregularities before substantial damage is done.\footnote{328}

\footnote{324} Id.
\footnote{326} Id.
\footnote{327} Id.
\footnote{328} Id.
[b] — Risk Management and Insurance.

E-business today is inherently insecure. While the Internet has provided business opportunities, it also produces an environment that is vulnerable to unauthorized network access. Organizations can develop comprehensive risk management strategies to protect them from security breaches.

A comprehensive risk management strategy should include three major tenets: (1) risk assessment techniques that identify and quantify potential business risks; (2) risk mitigation, such as a plan of prevention, detection and response to potential security threats; and (3) risk transfer mechanisms, such as insurance policies.

Recently, e-businesses were not able to have a fully comprehensive risk management strategy because most insurance companies did not offer any coverage for losses to e-business caused by a security breach. However, insurance companies and computer security firms have combined their resources to create a feasible insurance solution for organizations with an Internet presence. A computer security firm can perform a security assessment of an organization’s network and report those findings to an insurance company. Subsequently, an insurance company will propose a risk transfer solution that offers protection for the organization with an Internet presence. Most insurance policies offer Internet Asset and Protection Coverage (“Coverage”) as well as Internet Asset and Income Protection Warranty Plans (“Warranty”). For example, the typical Coverage plan offers insurance for loss of or damage to information assets (e.g. data, customer lists, credit card numbers, work papers and other digital information) resulting from a breach of

330 Id.
331 Id.
332 Id.
333 Id.
334 Id.
335 Id.

171
security or technical failure. This insurance also provides coverage for loss of business due to an interruption resulting from a breach of security. A Warranty plan can allow ISPs to extend coverage to their customers.

While these insurance solutions are available to e-businesses and organizations with an Internet presence, the premiums will vary based on both the size of the company and the level of security already provided by the network. For example, a typical premium for a large company (revenue in excess of $250 million) insuring only the loss of information assets would be approximately $20,000 for every $1,000,000 of coverage up to $75,000 for $10,000,000 in coverage. Coverage for loss in business due to service interruptions resulting from a security breach or extortion prevention (expenses for preparing against a threatened computer attack) would of course increase the premium price.


A company’s security policy is the tool to prevent or minimize loss from a security breach. A policy that is complete and wide-ranging will allow the company to thwart most attacks on the system from inside or outside the network. An exemplary security policy would include an initial audit of security systems to determine both weaknesses and strengths of the network, as well as an audit of daily information transactions on the system so that it is easier to determine when and where a breach has occurred as well as the ability to reconstruct events surrounding the breach for future investigations (either in-house or by law enforcement officials). In addition, the policy should also contain meticulous instructions or flow charts that describe how to handle a security breach and what steps to

337 Id.
338 Id.
339 Id.
340 Id.
take in order to contain the attack as well as recover data about the attack for later analysis. The policy should also provide for a risk management assessment of the system and consider a comprehensive insurance policy that covers the potential losses the business could suffer from a breach in security.


The key to maintaining network security is to use the many available services and numerous products that help to prevent security intrusions and breaches. An organization should continually update and adapt these products as the enterprise changes. However, prevention alone is not sufficient because some of these programs and services will have bugs or other inadequacies that can be exploited by hackers. The prevention products produce continuous audit reports and alarms that must be read and analyzed daily or the business risks the possibility of having intrusions go undetected and the network being left vulnerable to attack for an extended period of time. Finally, if a security breach does occur, the response should normally be guided by predetermined protocols provided by a security analyst.

§ 5.06. Conclusion.

The Internet has generated business opportunities and challenges at a rapid pace. The opportunities are perhaps most advantageous to the established business which uses the Internet as a part of marketing or sales arms. The Internet, however, has created numerous challenges, a few of which have been described in this chapter. Organizations should not fear doing business over the Internet, but they should perform that business with an awareness of the risks and should take steps that will allow the company to reap the many benefits offered by the Internet.