Cyberlaw Remedies

by

Tim Headley

at

The 23rd Annual HIPLA - UHLC Institute On IP Law

October 4-6, 2007

Wright Brown & Close, LLP
3 Riverway, Suite 600
Houston, TX 77056
713 490 4025 (direct dial)
713 572 4320 fax
713 398 1045 cell
headley@wrightbrownclose.com
www.wrightbrownclose.com

Table Of Contents

I. Scope of Article 1

II. Procedural Issues 2

A. Personal Jurisdiction 2

First Circuit 3
Second Circuit 4
Third Circuit 5
Fourth Circuit 5
Fifth Circuit 8
Sixth Circuit 10
Seventh Circuit 11
Eighth Circuit 13
Ninth Circuit 13
Tenth Circuit 17
Eleventh Circuit 17
D.C. Circuit 18
Federal Circuit 19

B. Venue 19

Fourth Circuit 19
Fifth Circuit 20
Sixth Circuit 20
Ninth Circuit 21

C. Service of Process 21

Ninth Circuit 21

III. Ex Parte Remedies 22

IV. Substantive Issues 23

A. Trademarks and Unfair Competition 23

1. Trademark Infringement and Dilution 23
Second Circuit 23
Fourth Circuit 25
Fifth Circuit 26
Sixth Circuit 27
Seventh Circuit 28
Ninth Circuit 28

2. Metatags, Header Tags, and Underline Tags 29
Seventh Circuit 30
Ninth Circuit 30

B. Domain Names 32

1. Arbitrator For Disputes Involving .biz gTLD 34
2. Domain Name Disputes 34
First Circuit 35
Second Circuit 35
Third Circuit 36
Fourth Circuit 37
Sixth Circuit 39
Seventh Circuit 39
Ninth Circuit 40
Tenth Circuit 43
3. Anticybersquatting Consumer Protection Act ("ACPA") 43
First Circuit 45
Second Circuit 46
Third Circuit 48
Fourth Circuit 49
Fifth Circuit 54
Sixth Circuit 55
Seventh Circuit 56
Ninth Circuit 57
4. International Arbitration Panels For Domain Name Disputes 60
Third Circuit 69
Fourth Circuit 69
WIPO Arbitration Panel 70
5. The European Union's Domain Name Dispute Resolution Policy .. 71
6. Fighting Overly-Aggressive Attempts to Cancel Domain Names .. 71
WIPO Arbitration Panel 72
Citizen Groups 73

C. Copyrights 75

1. Clickwrap and Browse-Wrap Licensing 75
First Circuit 75
Second Circuit 76
2. Infringement 76
Second Circuit 77
Fourth Circuit 77
Seventh Circuit 79
Ninth Circuit 79
3. Fair Use 81
Second Circuit 81
Third Circuit 81
Seventh Circuit 82
Ninth Circuit 82
4. Linking & Framing 84
Ninth Circuit 84
5. Crawling 85
Ninth Circuit 85
6. Audio Home Recording Act ("AHRA") 85

Ninth Circuit 85
7. Digital Millennium Copyright Act ("DMCA") 86
Second Circuit 87
Third Circuit 89
Fourth Circuit 90
Ninth Circuit 90
D.C. Circuit 92
8. Webcasting 93
9. Electronic Databases 93
10. Copyrights in Government Works 94
D. Defamation, Privacy & Child Protection 94
1. Communications Decency Act ("CDA") 47 U.S.C. § 230 94
Supreme Court 97
First Circuit 97
Third Circuit 98
Fourth Circuit 98
Sixth Circuit 99
Ninth Circuit 99
Tenth Circuit 101
Eleventh Circuit 101
2. Children's Online Privacy Protection Act of 1998 102
3. Children's Internet Protection Act 104
Supreme Court 104
4. TLD kids.us 105
E. Deceptive Acts 15 U.S.C.§ 45(a) 108
1. Hijacking & Mousetrapping Internet Surfers 108
Third Circuit 108
2. Other Unfair & Deceptive Acts 109
F. Crimes 111
1. Trafficking in Counterfeit Labels: 18 U.S.C. § 2318 112
2. Piracy of Copyrighted Works 18 U.S.C. § 2319 112
3. Trafficking In Counterfeit Goods Or Services 113
4. Computer Fraud And Abuse 18 U.S.C. § 1030 114
First Circuit 115
Second Circuit 115
Third Circuit 116
Fourth Circuit 116
Fifth Circuit 117
Seventh Circuit 120
Eighth Circuit 120
Ninth Circuit 121
5. Digital Millennium Copyright Act 122
Ninth Circuit 122
6. No Electronic Theft Act 123

Seventh Circuit 123
7. Economic Espionage Act of 1996 124
First Circuit 124
Third Circuit 125
Seventh Circuit 125
8. Electronic Communications Privacy Act, Wiretap Act, Stored Communications Act, & Communications Act. 126
First Circuit 126
Second Circuit 127
Third Circuit 127
Fourth Circuit 127
Fifth Circuit 128
Sixth Circuit 128
Seventh Circuit 129
Eighth Circuit 130
Ninth Circuit 130
Tenth Circuit 132
Eleventh Circuit 132
9. Child Online Protection Act of 1998 133
Supreme Court 133
Third Circuit 133
10. Wire Fraud 18 U.S.C. § 1343 134
Second Circuit 134
Third Circuit 134
Seventh Circuit 135
Ninth Circuit 135
Tenth Circuit 135
11. Spamming: Federal & State Laws 136
Fourth Circuit 142
Fifth Circuit 142
Ninth Circuit 143
Eleventh Circuit 145
State Laws 145
12. Texas Computer Crimes Statute 7 Texas Penal Code 33 147
Conclusion 148

I. Scope of Article

This paper surveys remedies available for actions involving the Internet. Here's a brief listing of some of the issues:

1. personal jurisdiction ("In what states can our company be sued for operating our website from our server in our home town?")

2. trademarks, domain names, and metatags ("Why can't I stop others from using variations of our company's domain name, 'bestchemicalengineers.com'?")

3. copyrights ("Why can't our graphics department put on our website those pictures that they found on the Internet?")

4. privacy rights ("Why can't we use someone's password to monitor an employees' gripe website?")

5. criminal activities with civil causes of actions (the Computer Fraud And Abuse Act, the Digital Millennium Copyright Act, the CAN-SPAM Act, the Communications Decency Act, the Stored Wire and Electronic Communications and Transactional Records Access Act, and the Stored Communications Act)

II. Procedural Issues

A. Personal Jurisdiction

Recall that the Due Process Clause of the 14th Amendment prohibits the deprivation of property or liberty without due process of law. In *International Shoe* the issues were

> "(1) whether, within the limitations of the due process clause of the Fourteenth Amendment, appellant, a Delaware corporation, has by its activities in the State of Washington rendered itself amenable to proceedings in the courts of that state to recover unpaid contributions to the state unemployment compensation fund exacted by state statutes, . . . , and (2) whether the state can exact those contributions consistently with the due process clause of the Fourteenth Amendment."

The undisputed facts were:

> Appellant is a Delaware corporation, having its principal place of business in St. Louis, Missouri, and is engaged in the manufacture and sale of shoes and other footwear. It maintains places of business in several states, other than Washington, at which its manufacturing is carried on and from which its merchandise is distributed interstate through several sales units or branches located outside the State of Washington.
>
> Appellant has no office in Washington and makes no contracts either for sale or purchase of merchandise there. It maintains no stock of merchandise in that state and makes there no deliveries of goods in intrastate commerce. During the years from 1937 to 1940, now in question, appellant employed eleven to thirteen salesmen under direct supervision and control of sales managers located in St. Louis. These salesmen resided in Washington; their principal activities were confined to that state; and they were compensated by commissions based upon the amount of their sales. The commissions for each year totaled more than $31,000. Appellant supplies its salesmen with a line of samples, each consisting of one shoe of a pair, which [326 U.S. 310, 314] they display to prospective purchasers. On occasion they rent permanent sample rooms, for exhibiting samples, in business buildings, or rent rooms in hotels or business buildings temporarily for that purpose. The cost of such rentals is reimbursed by appellant.
>
> The authority of the salesmen is limited to exhibiting their samples and soliciting orders from prospective buyers, at prices and on terms fixed by appellant. The salesmen transmit the orders to appellant's office in St. Louis for acceptance or rejection, and when accepted the merchandise for filling the orders is shipped f.o.b. from points outside Washington to the purchasers within the state. All the merchandise shipped into Washington is invoiced at the place of shipment from

which collections are made. No salesman has authority to enter into contracts or to make collections.

The Supreme Court held that due process requires "minimum contacts" between the defendant and the forum such that "the maintenance of the suit does not offend traditional notions of fair play and substantial justice", *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945), and thus held that the State of Washington could collect unemployment taxes from International Shoe.

In *World-Wide Volkswagen Corp* the Supreme Court held that for personal jurisdiction, due process requires that "the defendant's conduct and connection with the forum State are such that he should reasonably anticipate being haled into court there." *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980).

The issue in *World-Wide* was:

> "The issue before us is whether, consistently with the Due Process Clause of the Fourteenth Amendment, an Oklahoma court may exercise in personam jurisdiction over a nonresident automobile retailer and its wholesale distributor in a products-liability action, when the defendants' only connection with Oklahoma is the fact that an automobile sold in New York to New York residents became involved in an accident in Oklahoma."

The Supreme Court held that there could be no personal jurisdiction in such case.

The business described in a business plan for just about any .com company would probably give any court in the United States personal jurisdiction over the company. So, your client might want to consider that, when it estimates its legal fees in its business plan. Also, as part of any "click" agreement on the website, your client might want to include statements that 1) only Your State law applies, 2) only courts in Your County, Your State, have personal jurisdiction over the company, and 3) venue is proper only in Your County, Your State.

The following is a brief survey of the status of the law on personal jurisdiction and the Internet, beginning in 1999. Except for the most recent cases, I have grouped these by Circuits.

First Circuit

2003
D. Me.

McBee v. Delica Co., No. 02-198-P-C (D. Me. 4/14/03). The sale over the Internet by a company in Japan of items that misappropriated the name of an American musician, Cecil McBee of Yarmouth, Maine, including three transactions in Maine, constituted purposeful minimum contacts sufficient to support an exercise of jurisdiction by a court in Maine. The defendant, Delica Co. of Tokyo, sold a line of clothing and

accessories for teen-aged girls under the name “Cecil McBee”, and bearing the label “Produced by Cecil McBee”.

The court applied the five-part test from *United Electrical, Radio, and Machine Workers of America v. 163 Pleasant St. Corp.*, 960 F.2d 1080 (1st Cir. 1992). Under this test, a court must consider: (1) the defendant’s burden of appearing, (2) the forum state’s interest in adjudicating the dispute, (3) the plaintiff’s interest in obtaining convenient and effective relief, (4) the judicial system’s interest in obtaining the most effective resolution of the controversy, and (5) the common interests of all sovereigns in promoting substantive social policies.

The court rejected as insufficient the defendant’s claims that it would bear “enormous” burden in contesting a suit in the United States, because the defendant had presented “no evidence of its ability to bear the expense involved nor of the plaintiff’s relative ability to bear the cost of continued litigation in Japan.” Because the defendant had not demonstrated “any special or unusual burden,” the alleged inconvenience did not outweigh the second and third factors.

Second Circuit

1997

Bensusan Restaurant Corp. v. King, 126 F.3d 25, 44 U.S.P.Q.2d 1051 (2d Cir. 1997). The operator of a well-known New York jazz club called “The Blue Note” sued the operator of a Missouri jazz club of the same name for trademark infringement. To promote his club, the defendant operated an Internet web site which contained general information about his club, a calendar of events, and ticketing information, including the names and addresses of ticket outlets in Missouri and a telephone number for charge-by-phone orders. The district court refused to exercise jurisdiction over the defendant, reasoning that the maintenance of a web site alone, without more, did not rise to the level of purposeful availment of New York's laws. In finding that the exercise of jurisdiction would violate due process, the district court reasoned that the defendant had done nothing to purposefully avail himself of the benefits of New York.

2002

S.D.N.Y.

Thomas Publishing Co. v. Industrial Quick Search Inc., 237 F. Supp.2d 489 (S.D.N.Y. 2002), Thomas Publishing Co., a directory publisher, sued Industrial Quick Search, a Michigan-based operator of a Web site located at http://www.industrialquicksearch.com, for allegedly violating plaintiff’s copyrights and trademarks, due to the defendant's unauthorized use of the plaintiff's directory listings of manufacturing and industrial companies. The defendant moved to dismiss the complaint, arguing no personal jurisdiction. The court refused to dismiss, stating, “IQS's presence in New York, by way of an interactive website, is more closely akin to actual physical presence in New York than it is to running an advertisement in a national

magazine. If IQS wishes to operate an interactive website accessible in New York, there is no inequity in subjecting IQS to personal jurisdiction here. If IQS does not want its website to subject it to personal jurisdiction here, it is free to set up a "passive" website that does not enable IQS to transact business in New York."

Third Circuit

2001

Remick v. Manfredy, 238 F.3d 248 (3rd Cir.2001) (affirming a finding of no personal jurisdiction)Remick, a Pennsylvania attorney, sued his former Illinois client, Manfredy, alleging various claims, including misappropriation of Remick's image and likeness. This claim was based on the posting on Manfredy's old website of a single photograph of numerous persons, including Remick. The Third Circuit agreed with the district court that the mere posting of information or advertisements on an Internet website does not confer nationwide personal jurisdiction.

2003

Toys "R" Us v. Step Two Toys "R" Us had acquired a number of U.S.-registered IMAGINARIUM marks and was using them in its stores and on the website imaginarium.com. Step Two operates a chain of toy stores in Spain under the name "Imaginarium" and had registered the mark IMAGINARIUM in Spain. Since 1996, Step Two also operated a website using the domain imaginarium.es, advertising merchandise available in its stores. Toys "R" Us sued Step Two, a Spanish company, for infringement and unfair competition.

The trial court dismissed the case for lack of personal jurisdiction. Although Step Two had an interactive website (thereby meeting the *Zippo* test for personal jurisdiction), it did not do any business in the United States, and did not "purposefully avail" itself of New Jersey customers: Step Two's website was entirely in Spanish, showed prices in pesetas or euros, and the company shipped orders only to Spanish addresses. The Third Circuit agreed that "purposeful availment" was the appropriate test, but held that the trial court had erred in denying the plaintiff's request for further discovery on the jurisdiction issue, and stated that the defendant's non-Internet activities should also be considered "as part of the 'purposeful availment' calculus".

Fourth Circuit

2001

Alitalia-Linee Aeree v. Casinoalitalia.com (E.D. Va. January 19, 2001). The national airline of Italy sued for trademark infringement and, under the ACPA, included an in-rem action to cancel defendant's domain name registration. The court decided that it had jurisdiction over defendant's offshore casino website, because there was realtime interactivity, defendant had contracts with members in the district, and defendant derived substantial revenue from Virginia.

2002

ALS Scan v. Digital Service Consultants, 293 F.3d 707 (4th Cir. 2002), *cert. denied* 537 U.S. 1105 (2003). ALS Scan, which creates and markets adult photographs of female models for distribution over the Internet, claimed that Alternative Products appropriated copies of hundreds of ALS Scan's copyrighted photographs, and placed them on its websites, thereby gaining revenue from them through membership fees and advertising. The district court dismissed the complaint against the Internet Service Provider for lack of personal jurisdiction.

"Digital functioned from Georgia as an ISP and in that role provided bandwidth to Alternative Products, also located in Georgia, to enable Alternative Products to create a website and send information over the Internet," the court said. "It did not select or knowingly transmit infringing photographs specifically to Maryland with the intent of engaging in business or any other transaction in Maryland."

"The question presented in this appeal is whether a Georgia-based Internet Service Provider subjected itself to personal jurisdiction in Maryland by enabling a website owner to publish photographs on the Internet, in violation of a Maryland corporation's copyrights."

"Thus, adopting and adapting the Zippo model, we conclude that a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts. Under this standard, a person who simply places information on the Internet does not subject himself to jurisdiction in each State into which the electronic signal is transmitted and received. Such passive Internet activity does not generally include directing electronic activity into the State with the manifested intent of engaging business or other interactions in the State thus creating in a person within the State a potential cause of action cognizable in courts located in the State." The Fourth Circuit affirmed the dismissal.

Young v. New Haven Advocate, 315 F.3d. 256 (4th Cir. 2002), *cert. denied* 538 U.S. 1035 (2003). Connecticut contracted with Virginia to house Connecticut prisoners at Wallens Ridge. In reporting on this, the newspapers New Haven Advocate and Hartford Courant published articles on their Web sites. Stanley Young was a Virginia resident, and warden of Wallens Ridge State Prison. Young sued the newspapers and the authors of the articles in the Western District of Virginia.

The court relied on the three-pronged test in *ALS Scan*, and held that the content of the Web sites failed to demonstrate a manifested intent to target Virginia readers. "[I]t appears that these newspapers maintain their websites to serve local readers in Connecticut, to expand the reach of their papers within their local markets, and to provide their local markets with a place for classified ads. … The websites are not designed to attract or serve a Virginia audience."

E.D. Va.

Verizon Online Services, Inc. v. Ralsky, 203 F.Supp.2d 601 (E.D.Va. 2002). The defendants, Michigan residents, had sent millions of spam messages to Verizon's servers in Virginia. Verizon is an Internet service provider, with servers in Reston, Virginia. The spamming constituted sufficient minimum contacts to satisfy constitutional due process considerations, giving personal jurisdiction over the out-of-state defendant.

2003

Carefirst of Maryland v. Carefirst Pregnancy Centers, 334 F.3d 390 (4th Cir. 2003). The Fourth Circuit affirmed a dismissal of a suit, holding that an Illinois crisis pregnancy organization did not subject itself to personal jurisdiction in Maryland by operating an Internet website that allegedly infringed the trademarks of a Maryland insurance company. Carefirst of Maryland ("Carefirst") accused Chicago-based Carefirst Pregnancy Centers, Inc. ("CPC") of selecting the name CAREFIRST, despite having notice both of Carefirst's federal registrations for CAREFIRST and of Carefirst's common law use of the CAREFIRST mark.

CPC, an Illinois corporation with its principal place of business in Illinois, is a pro-life advocacy organization. CPC's mission is to "care[ ] for Chicago-area women in pregnancy-related crisis by meeting their emotional, physical and spiritual needs, enabling them to choose life." CPC originally incorporated in 1985 under the name "Loop Crisis Pregnancy Center," changed its name in 1993 to "ChicagoCare Pregnancy Centers," and in 1999 to "Carefirst Pregnancy Centers, Inc. d/b/a Carefirst." CPC has no physical presence in Maryland.

In 1998, CPC contracted with NetImpact, Inc., a web hosting and web development company headquartered in Ocean Pines, Maryland. On CPC's behalf, NetImpact purchased several domain names, including "www.carefirstpc.com," "www.carefirstpc.org," "www.carefirstpc.net," "chicagocare.org," "love4real.org," and "care1pregnancy.com." CPC uses its various domain names to direct Internet traffic to CPC's website, throughout which the CAREFIRST name appears. On that website, CPC solicits donations; educates pregnant women about nutrition, infant care, and prenatal care; provides references to Chicago-area medical doctors and hospitals; promotes its counseling services and parenting classes; and advertises the pregnancy tests and ultrasound services that it offers free of charge. The website asserts at several points that the geographic focus of CPC's activities is the Chicago metropolitan area.

In soliciting donations, CPC's website offers prospective donors two methods of contribution: (1) they can call an advertised toll-free number and make a credit card transaction over the phone; or (2) they can make a credit card donation directly through the website. In either case, the donor's name and address are recorded in CPC's database, and the donor thereafter receives advertising materials through the mails. If the donation is made online, the donor also receives a thankyou e-mail.

CPC acknowledged that it received $1,542 in donations (about 0.0174% of its total donation receipts) from Maryland residents between 1991 and September of 2001. Of this amount, only $120 was donated (by nine different Marylanders) after CPC adopted the name "Carefirst Pregnancy Centers, Inc." in 1999. Apart from a single online donation made by the lawyer for Carefirst, there was no evidence that the Maryland donations were made through the website.

Based on these facts, the Fourth Circuit held that CPC could not have reasonably anticipated being haled into a Maryland court.

Fifth Circuit

1999

Mink v. AAAA Development LLC**,** 190 F.3d 333, 52 U.S.P.Q.2d (BNA) 1218 (5th Cir. 1999) (adopting the reasoning of *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997)) There are two possible types of personal jurisdiction over a defendant: general and specific jurisdiction. The Fifth Circuit, in this case arising out of the Southern District of Texas, held that there was no personal jurisdiction over the defendant who operated a web site, stating that personal jurisdiction depends on the "nature and quality of commercial activity that an entity conducts over the Internet."

> "Specific jurisdiction exists when the nonresident defendant's contacts with the forum state arise from, or are directly related to, the cause of action. *See id*. (citing *Helicopteros Nacionales de Columbia, S.A. v. Hall*, 466 U.S. 408, 414 n.8 (1984)). General jurisdiction exists when a defendant's contacts with the forum state are unrelated to the cause of action but are 'continuous and systematic.' Because we conclude that Mink has not established any contacts directly related to the cause of action required for specific jurisdiction, we turn to the question of whether general jurisdiction has been established.
>
> "At the one end of the spectrum, there are situations where a defendant clearly does business over the Internet by entering into contracts with residents of other states which "involve the knowing and repeated transmission of computer files over the Internet...." *Zippo*, 952 F. Supp. at 1124. In this situation, personal jurisdiction is proper. *See id*. (citing *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996)). At the other end of the spectrum, there are situations where a defendant merely establishes a passive website that does nothing more than advertise on the Internet. With passive websites, personal jurisdiction is not appropriate. *See id*. (citing *Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd*, 126 F.3d 25 (2d Cir. 1997)). In the middle of the spectrum, there are situations where a defendant has a website that allows a user to exchange information with a host computer. In this middle ground, "the exercise of jurisdiction is determined by the level of interactivity and commercial nature of the exchange of information that occurs on the Website." *Id*. (citing *Maritz Inc. v.*

Cybergold Inc., 947 F. Supp. 1328 (E.D. Mo. 1996)). We find that the reasoning of Zippo is persuasive and adopt it in this Circuit.

"AAAA maintains a website that posts information about its products and services. While the website provides users with a printable mail-in order form, AAAA's toll-free telephone number, a mailing address and an electronic mail ("e-mail") address, orders are not taken through AAAA's website. This does not classify the website as anything more than passive advertisement which is not grounds for the exercise of personal jurisdiction."

2002

Revell v. Lidov, 317 F.3d 467 (5th Cir. 2002). Revell sued Lidov, a Massachusetts resident, and Columbia University (in New York City) in Texas, for defamation arising out of Lidov's authorship of an article that he posted on an internet bulletin board hosted by Columbia. Lidov's article concerned the terrorist bombing of Pan Am Flight 103, which exploded over Lockerbie, Scotland, in 1988. The article singled out Revell, then Associate Deputy Director of the FBI, accusing him of complicity in the conspiracy and cover-up of a willful failure to stop the bombing despite clear advance warnings.

The Fifth Circuit distinguished its prior holding in *Mink,* stating "because even repeated contacts with forum residents by a foreign defendant may not constitute the requisite substantial, continuous and systematic contacts required for a finding of general jurisdiction—in other words, while it may be doing business *with* Texas, it is not doing business *in* Texas." "Irrespective of the sliding scale, the question of general jurisdiction is not difficult here. Though the maintenance of a website is, in a sense, a continuous presence everywhere in the world, the cited contacts of Columbia with Texas are not in any way 'substantial'."

On the issue of specific personal jurisdiction, the Court distinguished the Supreme Court *Calder v. Jones* case, stating, "We find several distinctions between this case and *Calder*—insurmountable hurdles to the exercise of personal jurisdiction by Texas courts. First, the article written by Lidov about Revell contains no reference to Texas, nor does it refer to the Texas activities of Revell, and it was not directed at Texas readers as distinguished from readers in other states. … We also find instructive the defamation decisions of the Sixth, Third, and Fourth Circuits in *Reynolds v. International Amateur Athletic Federation, Remick v. Manfredy, and Young v. New Haven Advocate*, respectively."

2002

E.D. La.

Planet Beach Franchising Corp. v. C3ubit Inc. Plaintiffs, Planet Beach Franchising Corporation and Planet Beach Tanning Salons, Inc., are Louisiana

corporations in the business of franchising tanning salons. Defendant TanToday.com operated a website on which users shared information and news related to the tanning salon industry. Bruce Schoenfelder, also a defendant, was TanToday.com's sole managing officer. Schoenfelder resides in Pennsylvania. TanToday.com is a Pennsylvania corporation that is operated and managed by Schoenfelder in Pennsylvania. It was undisputed that defendants have no officers, employees or property in Louisiana. It was also undisputed that defendants have never entered into or performed a contract or other transaction with a Louisiana citizen or business.

About May 22, 2002, defendants posted an article on their website entitled: "SCOOP: Planet Beach - the DEATH Of A Franchising Chain?" In the article, defendants stated that “we are alerting the ENTIRE INDUSTRY of a meltdown, and warning everyone with business dealings with Planet Beach to review your status, your arrangements, and hunker down."

Plaintiffs sued. On defendant’s motion to dismiss, the court found specific jurisdiction over the defendants “because they committed an act outside of the forum that allegedly caused a tortious injury within the forum, and the harm suffered was intended or highly likely to follow from defendants' acts. The presence of these key elements, along with the fact that defendants drew from sources in the forum, placed phone calls to the forum, and obtained an electronic copy of plaintiffs' registered trademark from a server located in the forum, are enough to establish defendants' minimum contacts with the forum.”

N.D. Tex.

Carrot Bunch Co. v. Computer Friends Inc. An interactive Web site that provided for online ordering of goods, combined with evidence of actual sales to forum residents, constituted sufficient minimum contacts to support an exercise of specific personal jurisdiction. Judge Buchmeyer found the case to be similar to *American Eyewear Inc. v. Peeper's Sunglasses and Accessories Inc.*, 106 F.Supp. 2d 895 (N.D. Tex. 2000) (involving actual sales), and different from *People Solutions Inc. v. People Solutions Inc.*, 2000 U.S. Dist. LEXIS 10444 (N.D. Tex. 2000) (no actual sales).

Sixth Circuit

1996

CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1264, 39 U.S.P.Q.2d 1502 (6th Cir. 1996). A Texas resident advertised his product via CompuServe, located in Ohio. The Sixth Circuit held that he was subject to personal jurisdiction in Ohio, because he had taken direct actions that created a connection with Ohio: he subscribed to CompuServe, he loaded his software onto the CompuServe system for others to use, and he advertised his software on the CompuServe system.

2000

Cyberspace Communications Inc. v. Engler, 142 F.Supp.2d 827 (E.D.Mich. 2001). On June 2, 2000, Governor Engler of Michigan signed into law an act making it

a felony to disseminate “sexually explicit materials” deemed “harmful to minors” via the Internet. The American Civil Liberties Union (“ACLU”) sued the Governor on behalf of ten companies, some of which are not located in Michigan, asking for a preliminary injunction to prevent enforcement of the law. Among other findings, the district court found that the law would violate the commerce clause, because it would regulate conduct outside of Michigan, and so granted the preliminary injunction. The Sixth Circuit affirmed.

2002

Bird v. Parsons, Dotster, & Afternic.com, 289 F.3d 865 (6th Cir. 2002)***.*** Since 1983, plaintiff Bird of Dayton, Ohio, had operated a software business using the name Financia Inc. In 1984, he obtained a trademark registration for FINANCIA. He also registered the domain name financia.com. In 2000, defendant Marshall Parsons of California registered the domain name efinancia.com with defendant domain name registrar Dotster Inc. of Longview, Wash. The day after Parsons registered the domain name, Afternic.com Inc. of New York listed efinancia.com on its domain name auction Web site. Bird sued, alleging jurisdiction over Dotster. In this ACPA case, the Sixth Circuit held that, under the U.S. Constitution and the Ohio long-arm statute, an allegation that a domain name registrar had registered about 5,000 domain names for residents of Ohio supported the exercise of specific personal jurisdiction over the registrar, but affirmed dismissal of the case, for failure to state a claim for failed to state a claim of infringement, unfair competition, dilution, or liability under the ACPA.

2003

Bridgeport Music Inc. v. Still N the Water Publishing, 66 USPQ2d 1492 (CA 6 2003) (affirming a finding of no personal jurisdiction over defendant NTW in Houston, and reversing a finding of no personal jurisdiction over defendant DM in Florida). "In her plurality opinion, which embraces what has come to be known as the 'stream of commerce plus’ theory, Justice O’Connor opined that '[t]he placement of a product into the stream of commerce, without more, is not an act of the defendant purposefully directed toward the forum State.' *Asahi*, 480 U.S. at 112. ... [W]e make clear today our preference for Justice O’Connor’s stream of commerce 'plus' approach, for the reasons set forth in that opinion, and conduct the remainder of our analysis accordingly. ... Bridgeport does not assert that NTW hosts or operates a website, let alone one that is sufficiently interactive for a finding a purposeful availment. ... Bridgeport notes that DM operates a website, dmrecords.com, through which users can access DM’s catalog and purchase DM’s records. Through the DM site, users select a recording of choice and then are redirected to Amazon.com to complete their purchases. ... In the instant action, as in Bird, there is evidence indicating the volume of business DM conducts through the internet for at least two of the allegedly infringing albums, *i.e.*, 36 internet sales of Tag Team and 30 of Future Rhythm."

Seventh Circuit

1999

Ty Inc. v. Beanie World, Inc., No. 99-C-4199 1999 WL 782092 (N.D. Ill. September 27, 1999). The court held that 1% of defendant's sales income from Internet sales was not enough for venue to be proper in Illinois, rather than in defendant's home state of Florida.

2000

Ty, Inc. v. Clark, ------, (N.D. Ill. 2000). A district court in Chicago followed the reasoning of the Fifth Circuit regarding personal jurisdiction. Ty Inc. created and marketed "Beanie Babies" and also operates websites selling "Beanie Babies." Clark, living in England, operated a website also selling "Beanie Babies". Ty sued Clark for trademark infringement, etc., in Illinois. When the court asked Ty to brief the venue issue, Ty stated in its brief that it assumed personal jurisdiction. The court found no jurisdiction because there were no orders taken via Clark's web site, there were no contracts signed via his web site, and customers had to print the order form, and phone, fax, or mail it to England. Clark's site no longer exists.

2002

N.D. Ill.

Ty Inc. v. Sullivan, 2002 WL 500663 (N.D.Ill. March 12, 2002)***.*** Ty Inc. is the manufacturer of the "Beanie Babies" toys. The defendant, Karen Sullivan, d/b/a Ebeanies On Line of Miami, operated a Web site through which she sold Beanie Babies. Ty sued her in Chicago. Over a five-year period, she had sold 38 Beanie Babies to 12 Illinois residents. The district court held that those sales were sufficient to support personal jurisdiction over her.

N.D. Ill.

Tamburo v. eBay Inc., 2002 WL 31655212 (N.D. Ill. Nov. 22, 2002). A buyer of audio equipment on eBay complained that some of the goods were damaged or missing. So, eBay suspended the seller's account. The seller, living in Illinois, sued eBay and the buyer in Illinois. The buyer was a Pennsylvania resident who had never visited, or transacted business in, Illinois. The buyer's only connection with Illinois was his act of wiring the seller money through a PayPal account. The court held, "A single wire transfer to a person whom [the buyer] did not even realize was an Illinois resident is not sufficient contact with this State to justify haling him into court here [in Illinois]."

2004

Jennings v. AC Hydraulic A/S*,* No. 03-2157 (7th Cir. 9/2/04) (affirming dismissal for lack of personal jurisdiction). Jennings' widow sued in Indiana the manufacturer of a floor jack, AC Hydraulic A/S, for the wrongful death of her husband. The district court dismissed the case, and the Seventh Circuit affirmed, for lack of personal jurisdiction. AC Hydraulic's principal place of business is in Denmark. It is not an Indiana corporation, nor is it licensed to do business in the state. It does not maintain there a registered agent for service of process, an office, a telephone listing, a bank

account, property, or any employees. AC Hydraulic maintains a website (www.achydraulic,com) with English translations that is accessible throughout the United States. On the website AC Hydraulic provides contact information and descriptions of its various product lines, but consumers cannot order its products via this website.

The 7th Circuit assumed, as did the district court, that AC Hydraulic's conduct was sufficient to establish personal jurisdiction under Indiana's long-arm statute. Jennings relied on "specific jurisdiction", arguing in part that AC Hydraulic advertised its products to consumers in the United States, including Indiana residents, by maintaining an English-translated website. The 7th Circuit held that "The exercise of personal jurisdiction based on the maintenance of a passive website is impermissible because the defendant is not directing its business activities toward consumers in the forum state in particular."

Eighth Circuit

1999

State of Missouri v. Coeur d'Alene Tribe, 164 F.3d 1102 (8th Cir. 1999), *cert. denied*, 119 S. Ct. 2400 (1999)**.** In this Eighth Circuit case, the Court remanded to the district court to determine whether Missouri residents' gambling on the Coeur D'Alene Tribe's Internet gambling site are "on Indian lands" and therefore controlled by the Indian Gaming Regulatory Act, or on state lands, in which case the state may regulate or prohibit the activity.

Ninth Circuit

1997

Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 419-420, 44 U.S.P.Q.2d 1928 (9th Cir. 1997). An Arizona corporation, Cybersell, Inc. ("Cybersell AZ"), held a registered servicemark for the name Cybersell. A Florida corporation, Cybersell, Inc. ("Cybersell FL"), created a web site with the domain name cybsell.com. The web page had the word "Cybersell" at the top and the phrase, "Welcome to Cybersell!" Cybersell AZ claimed that Cybersell FL infringed its registered trademark and brought an action in the district court in Arizona. The Ninth Circuit held the Arizona court could not exercise personal jurisdiction over Cybersell FL, because it had no contacts with Arizona other than maintaining a web page accessible to anyone over the Internet.

1998

Panavision Int'l L.P. v. Toeppen, 141 F.3d 1316, 46 U.S.P.Q.2d 1511, 1514 (9th Cir. 1998). Panavision holds registered trade-marks to the names "Panavision" and "Panaflex" in connection with motion picture camera equipment. In December 1995, Panavision attempted to register a website on the Internet with the domain name Panavision.com. It could not do that, however, because Toeppen had already

established a web site using Panavision's trademark as his domain name. Toeppen's web page for this site displayed photographs of the City of Pana, Illinois.

Toeppen demanded $13,000 for the panavision.com domain name, and Panavision refused to pay. After Panavision refused Toeppen's demand, he registered Panavision's other trademark with NSI as the domain name Panaflex.com. Toeppen's web page for Panaflex.com simply displays the word 'Hello.' Toeppen engaged in a scheme to register Panavision's trademarks as his domain names for the purpose of extorting money from Panavision." *Id*. at 1516.

Toeppen, living in Illinois, alleged that the California district court did not have personal jurisdiction over him.

The Ninth Circuit requires three conditions to be met, in order for there to be personal jurisdiction over a non-resident: purposeful availment, forum-related activities, and reasonableness. To find purposeful availment, the Court applied the "effects doctrine", which is that "personal jurisdiction can be based upon: (1) intentional actions (2) expressly aimed at the forum state (3) causing harm, the brunt of which is suffered -- and which the defendant knows is likely to be suffered -- in the forum state." *Id*. at 1517.

The Court found that Toeppen had injured Panavision in California, Panavision's principal place of business. Thus, Toeppen had conducted forum-related activities. Finally, the Court considered seven factors, finding that personal jurisdiction was reasonable. *Id*. at 1517.

2000

C.D. Cal.

Nissan Motor Co. v. Nissan Computer Corp., 89 F.Supp. 2d 1154 (C.D. Cal. 2000). The court granted the car company's motion for a preliminary injunction for trademark infringement, denying the defendant's motion to dismiss for lack of personal jurisdiction. The President, Uzi Nissan, of the defendant, a North Carolina Corporation, lived in North Carolina. The court held that Mr. Nissan's receipt of "advertising revenue by intentionally exploiting consumer confusion", by using the "Nissan" trademark for the domain name of his Web sites, was "the 'something more' indicating that the defendant deliberately and substantially directed its activity toward the forum state." However, the court refused to order him to transfer his domain name to the car company, but instead ordered him to post a disclaimer, enjoined his posting of any automobile-related information or advertising, and allowed him to continue to advertise his computer business, and to use "Nissan" as a metatag.

2001

N.D. Cal.

Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal., 2001). A French court's order directing Yahoo! Inc. to block French citizens' access to Nazi-related items and information linked to its auction site at yahoo.com would, if enforced in the United States, violate the First Amendment right to free speech.

C.D. Cal.

Batzel v. Smith, 2001 WL 1893843 (C.D. CA June 5, 2001). The plaintiff, Ellen Batzel, was a lawyer living in North Carolina. She declined to help her house painter market a script that he had written. So, the house painter sent an e-mail to Ton Cremers, who lived in the Netherlands. "The e-mail indicated that he, Smith, had been working in the home of a lawyer who claimed to be the granddaughter of Heinrich Himler and who bragged about having an art collection stolen from Jewish families by the Nazis. Cremers published the e-mail and related updates on five occasions in September of 1999, allegedly without investigating the veracity of the information received from Smith." Cremers published the rumor in his e-mail newsletter that he regularly sent out to museums around the world. Some of those were located in California. Batzel sued Cremers and others in California. Cremers moved to dismiss, for lack of personal jurisdiction, and on the grounds of forum non-conveniens. The Court refused to dismiss the complaint, stating that 1) Cremers had "transmitted his newsletter via the internet to California multiple times per week", 2) Cremers had "entered into a corporate sponsorship agreement with Mosler, Inc., a museum security company based in Anaheim, California", 3) "several California … organizations and museums were subscribers to Cremers' mailing list during the time the allegedly defamatory email was published", 4) in 1999, Cremers traveled to California to a conference held at the Getty Museum" at which he "solicited subscribers" for his newsletter, and "sought corporate sponsorship" of his website, and 5) Cremers had "republished several articles in his newsletters and website from California newspapers", which implied that "he would have had to enter into copyright licensing agreements with those California newspapers". Did the Court know about the CCC???

2002

D. Nev.

Medinah Mining Inc. v. Amunategui, 237 F.Supp.2d 1132 (D.Nev. 2002). Medinah sued various defendants, alleging defamation because of postings at www.ragingbull.com. The Web site was an interactive site that reported financial news. Medinah argued specific jurisdiction. The court reviewed the requirements for specific jurisdiction:

> the defendant must perform some act or consummate some transaction within the forum, or otherwise purposefully avail himself of the privileges of conducting activities in the forum;
>
> the claim must arise out of or result from the defendant's forum-related activities; and
>
> the exercise of jurisdiction must be reasonable.

The court reviewed its adoption of the "sliding scale" of *Zippo Manufacturing Co. v. Zippo Dot Com Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997), the "something more" requirement than merely posting information of *Cybersell Inc. v. Cybersell Inc.*, 130 F.3d 414 (9th Cir. 1997), and the requirement of tortious conduct aimed at or affecting the forum state in *Calder v. Jones*, 465 U.S. 783 (1984). The court relied on two similar

cases to reject specific jurisdiction: *Bailey v. Turbine Design Inc.*, 86 F.Supp. 2d 790 (W.D. Tenn. 2000), and *Barrett v. Catacombs Press*, 44 F.2d 717 (E.D. Pa. 1999). "We hold that, similar to the situations considered in *Bailey* and *Barrett*, Plaintiffs have failed to show that the alleged defamatory postings were directed at residents of Nevada."

2004

***Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisemitisme*,** No. 01-17424 (9th Cir. 8/23/04) (reversing a grant of summary judgment in favor of Yahoo, for lack of personal jurisdiction over the French). Section R645-2 of the French Criminal Code bans exhibition of Nazi propaganda for sale and prohibits French citizens from purchasing or possessing such material. French users can access the American Yahoo! website that carries Nazi-related auction items.

On May 22, 2000, a French court issued an order requiring Yahoo — subject to a fine of approximately $13,300 per day — to destroy all Nazi relics, objects, insignia, emblems, and flags on its auction site, and to remove any excerpts from Mein Kampf and Protocole des Sages de Sion, books promoting Nazism. On November 20, the French court reaffirmed its May 22 order, giving Yahoo! three months to comply with the first order and reiterating that fines would accrue daily if Yahoo! did not comply with the order. The imposition of penalties is provisional in France and cannot be imposed without further court proceedings. Yahoo! chose not to pursue its appeal in France, and its right to appeal expired on February 7, 2001. (The fines continued to accrue daily!!)

The French parties have not yet chosen to sue Yahoo in the U.S. to collect the judgment, so Yahoo sued in California for a declaration that the orders were unenforceable. Later, a district court in the Northern District of California granted Yahoo's request, declaring the French court's orders of May 22 and November 20 were not enforceable in the United States.

The District Court based this holding on three contacts with Northern California: (1) the cease-and-desist letter sent to Yahoo; (2) the use of the United States Marshals Service to serve process; and (3) the French parties' request to the French court that Yahoo perform certain acts on its server and remove certain Nazi items from its website in California. On appeal, the Ninth Circuit agreed with the French parties that the district court lacked personal jurisdiction over the French parties.

In *Bancroft & Masters*, the Ninth Circuit had held that the "express aiming" requirement of the Supreme Court in *Calder v. Jones,* 465 U.S. 783 (1984)*,* is satisfied "when the defendant is alleged to have engaged in **wrongful** conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state." *Bancroft & Masters*, 223 F.3d at 1087 (emphasis added). The Ninth Circuit held that the French parties' conduct, to enforce French hate speech laws, was not wrongful, and therefore, there was no personal jurisdiction. The dissent argued that the use of the U.S. Marshals to serve process should have led the French parties to reasonably anticipate being haled into court in California.

2006

Pebble Beach Co. v. Caddy, 453 F.3d 1151 (9th Cir. 2006) (affirming the district court's 1) dismissal of a trademark infringement complaint for lack of personal jurisdiction, and denial of Pebble Beach's motion to conduct additional jurisdictional discovery).

> Caddy, a dual citizen of the United States and the United Kingdom, occupies and runs a three-room bed and breakfast, restaurant, and bar located in southern England. Caddy's business operation is located on a cliff overlooking the pebbly beaches of England's south shore, in a town called Bar-ton-on-Sea. The name of Caddy's operation is "Pebble Beach," which, given its location, is no surprise. Caddy advertises his services, which do not include a golf course, at his website, www.pebblebeach-uk.com. Caddy's website includes general information about the accommodations he provides, including lodging rates in pounds sterling, a menu, and a wine list. The website is not interactive. Visitors to the website who have questions about Caddy's services may fill out an on-line inquiry form. However, the website does not have a reservation system, nor does it allow potential guests to book rooms or pay for services on-line.
>
> Except for a brief time when Caddy worked at a restaurant in Carmel, California, his domicile has been in the United Kingdom.

The Ninth Circuit held that Caddy 1) did not purposefully avail himself of the privilege of conducting activities in California, or the United States as a whole, and (2) did not purposefully direct his activities toward either of those two forums.

Tenth Circuit

1999

Soma Medical Int'l v. Standard Chartered Bank, 196 F.3d 1292 (10th Cir. 1999)**.** In this Tenth Circuit case, a Utah account-holder sued for breach of contract and negligence against a British bank after it disbursed funds upon an unauthorized signature. The bank's maintenance of a web site accessible in Utah was not sufficient to establish personal jurisdiction. The court affirmed the *Zippo* three-part test, and found no jurisdiction because the web site was purely passive in nature.

2000

Intercon, Inc. v. Bell Atlantic Internet Solutions Inc., 205 F.3d 1244, 1248 (10th Cir.2000) (personal jurisdiction available based on defendant's unauthorized and knowing use of plaintiff's servers located in the forum state). In this Tenth Circuit case, after defendant received notice that it was inadvertently routing its customers' e-mail through the plaintiff's Oklahoma mail server, the defendant continued to do so willfully. The Court held that personal jurisdiction was available, based on defendant's unauthorized and knowing use of plaintiff's servers located in the forum state.

Eleventh Circuit

Future Tech. Today, Inc. v. OSF Healthcare Sys., 218 F.3d 1247 (11th Cir. 2000) (affirming dismissal for lack of personal jurisdiction). The defendant Illinois corporation moved to dismiss a suit (for breach of contract and conversion) for lack of personal jurisdiction in Florida. The negotiations on the contract were conducted via telephone, and the contract was signed by the Illinois corporation in Illinois. Although all of the computer files were sent by the Illinois corporation to the plaintiff's Florida office via the Internet, the Eleventh Circuit affirmed the district court's holding that the transfer of the files via the Internet to Florida was not sufficient to establish the requisite minimum contacts with the forum for purposes of personal jurisdiction because, although the sender knew the destination of the transmission, it did not care where the work was done, nor did the contract specify where the work was to be completed. The Florida corporation chose the Florida destination, and the Illinois corporation, by agreeing to the location of the work, did not purposefully avail itself of Florida's jurisdiction.

D.C. Circuit

2000

GTE New Media Services Inc. v. BellSouth Corp., 199 F.3d 1343,1349 (D.C.Cir.2000) (no personal jurisdiction because no evidence of a contractual relationship or comparable market activity in the district). In this D.C. Circuit case, the Court held that there was no personal jurisdiction, because there was no evidence of a contractual relationship or comparable market activity in the district.

GTE alleged that in July 1997, five regional Bell operating companies (Ameritech Corp., Bell Atlantic, BellSouth, SBC Corp., U.S. West) and their relevant subsidiaries conspired to capture, control, and dominate the Internet business directories' market. After the alleged conspirators held meetings in California, Colorado, Georgia, and Michigan, they agreed to provide jointly a coded map of the United States that would allow users of their Internet Yellow Pages to access particular states and particular businesses. Each of the regional Bell operating companies would provide exclusive service to a particular region, and the other companies apparently agreed not to compete with the designated exclusive server in its given region. The regions designated to each regional Bell operating company corresponded to the region to which the company provided telecommunications service. The regional Bell operating companies' next step was to obtain exclusive links for their map on well-known Internet browser sites run by Netscape and Yahoo, to ensure that users of these sites would be specifically directed to the operating companies' Internet Yellow Pages.

Before the alleged conspiracy, GTE had a non-exclusive contract with Netscape, pursuant to which Netscape offered a choice of Internet business directories on its site, including GTE's SuperPages. When users accessed the "Yellow Pages" option on Netscape's toolbar, they had access to GTE's website. However, Netscape terminated this arrangement on July 18, 1997, by removing its links to GTE's SuperPages, including hyperlinks on Yahoo.

The Court maintained that “personal jurisdiction surely cannot be based solely on the ability of District residents to access the defendants' websites, for this does not by itself show any persistent course of conduct by the defendants in the District.”

2002

Gorman d/b/a Cashbackrealty.com v. Ameritrade Holding Corp, 293 F.3d 506 (D.C. Cir. 2002). An out-of-state defendant's website, enabling the company to enter into binding contracts with District customers, constituted the "continuous and systematic" contacts required by the forum's long-arm statute, and was consistent with constitutional due process. Therefore, there was general personal jurisdiction.

D.C. Court of Appeals

Forrest v. Verizon Communications, 805 A.2d 1007 (D.C. 2002). A DOJ attorney living in D.C. sued Verizon in a purported class action in the District of Columbia for allegedly poor DSL Internet service. On appeal from dismissal, based on a forum selection clause, the appeals court held that the forum selection clause included in clickwrap language for digital subscriber line service was reasonable and enforceable against a subscriber.

Federal Circuit

1998

3D Sys., Inc. v. Aarotech Lab., Inc.**,** 160 F.3d 1373 (Fed. Cir. 1998). In this patent infringement suit, jurisdiction in the central district of California was not proper for a co-defendant who merely maintained a web site viewable in California, and any email he received from California he forwarded to the other co-defendant.

B. Venue

Fourth Circuit

2002
E.D. Va.

Verizon Online Services, Inc. v. Ralsky, 203 F.Supp.2d 601 (E.D.Va. 2002). "[T]ransmission of UBE [unsolicited bulk e-mail or "spam"] to and through Verizon's Virginia computers constitutes a 'use' of those servers which in turn constitutes an act within the Commonwealth. See VA CODE § 8.01-328.1(B). Thus, because a substantial portion of Defendants' actions giving rise to Verizon's claims occurred in Virginia and a substantial part of the property harmed by these actions occurred in Virginia, venue is proper in this forum under 28 U.S.C. §1391(b)(2)."
"In addition, the cost and convenience of the witnesses and the evidence counsel toward keeping the case in Virginia. Many of Verizon's employee-witnesses reside in Virginia. Most of the documents relevant to this matter are also located in Virginia. Finally, there is a substantial interest in having the instant controversy decided in Virginia because Verizon is a company with its principal place of business in Virginia

and the Commonwealth has enacted legislation seeking to protect Virginia corporations from the type of unlawful conduct allegedly at issue in this case."

Fifth Circuit

2002
N.D. Tex.

Carrot Bunch Co. v. Computer Friends Inc. An interactive Web site that provided for online ordering of goods, combined with evidence of actual sales to forum residents, constituted sufficient minimum contacts to support an exercise of specific personal jurisdiction. Additionally:

"Defendant requests transfer to federal district court in Oregon. This transfer is unwarranted. In the Fifth Circuit, a plaintiff is generally entitled to choose the forum. *See Peteet v. Dow Chemical Co.,* 868 F.2d 1428, 1436 (5th Cir. 1989). For this reason, courts "should not transfer venue where the result will be merely to shift the expense and inconvenience from one party to the other." *Enserch Int'l Exploration, Inc. v. Attock Oil Co.,* 656 F.Supp. 1162, 1167 n.15 (N.D.Tex. 1987)."

"Transferring venue to Oregon will simply shift the inconvenience of litigating outside of one's home state from Defendants to Plaintiff. Under such circumstances, Plaintiff's choice of forum trumps. The importance of Plaintiff's selection of forum is increased in this case because its principal place of business is in the Northern District of Texas. *See e.g., Nat'l Group Underwriters, Inc. v. Southern Sec. Life Ins. Co.*, 2001 U.S. Dist. LEXIS 18969, *5 (N.D.Tex. 2001) (Citing *Continental Airlines, Inc. v. American Airlines, Inc.,* 805 F.Supp. 1392, 1396 (S.D.Tex.1992))."

2003

International Truck And Engine v. Quintana and International Bus & Coach, 259 F.Supp.2d 553 (N.D. Tex. 2003) (denying motion to dismiss for lack of personal jurisdiction, and denying motion to transfer venue). In addition to various acts of trademark infringement allegedly committed in the Northern District of Texas, the plaintiffs also alleged that the defendants advertised their business on an Internet website accessible in Texas using plaintiffs trademark "INTERNATIONAL".

Sixth Circuit

1996

U.S. v. Thomas, 74 F.3d 701 (6th Cir. 1996) (affirming the conviction of obscenity for defendants' operation of a computer bulletin board). In response to a challenge to venue in the Western District of Tennessee, the Sixth Circuit stated that it had previously recognized that "venue for federal obscenity prosecutions lies 'in any district from, through, or into which' the allegedly obscene material moves." (citing *Peraino*, 645 F.2d at 551 (citing 18 U.S.C. § 3237)).

Ninth Circuit

2002

McNeil v. Stanley Works, Unpublished, 33 Fed. Appx. 322 (9th Cir. 2002) (affirming the dismissal of a suit filed in California for improper venue). A Canadian citizen sued a Connecticut company regarding the Canadian's failed business relationship with the company's Canadian subsidiary. The Ninth Circuit held that the forum choice of a UDRP administrative proceeding, made pursuant to UDRP Rule 3(b)(xiii), is permissive, not binding, and therefore the district court was proper in applying a forum non conveniens analysis to determine the proper venue for the issues in question:

> "A permissive choice of forum does not constitute a concession that the forum selected is convenient, and does not require the party moving to dismiss on the basis of forum non conveniens to make a heightened showing of inconvenience."

N.D. Cal.

Jamba Juice v. Jamba Group, 2002 WL 1034040 (N.D. Cal. May 15, 2002). The defendant asserted improper venue. The trademark plaintiff offered merely the existence of an accessible Web site in his district. Held: not enough for proper venue, because there was no showing that the defendant had otherwise targeted the forum. The Court said that the plaintiff must show "'something more' than the operation of a general access website, specifically 'conduct directly targeting the forum.'"

C. Service of Process

Ninth Circuit

2002

Rio Properties v. Rio International Interlink, 284 F.3d 1007 (9th Cir. 2002). In this trademark infringement suit, the Ninth Circuit held that e-mail service of process on a Costa Rican entity that had no designated agent in the United States complied with the alternate service of process rule in Fed. R. Civ. P. 4(f)(3), which permits the court to direct service "by other means not prohibited by international agreement." The defendant had argued that e-mail service must be a "last resort". The Ninth Circuit stated that the plaintiff did not have to try every permissible means of service before asking the court for alternate relief under Rule 4(f)(3). The plaintiff merely had to show that the circumstances of the case required the district court's intervention.

III. Ex Parte Remedies

Ninth Circuit

"The F.T.C. argues that the district court erred in refusing to order Pantron or Lederman to pay restitution to consumers or disgorge their profits. Because the district court's refusal to award monetary equitable relief was based on the application of erroneous legal principles, we reverse. We conclude that an application of the correct legal principles requires the district court to order monetary relief in this case, especially in light of our conclusion, set forth in the previous Part, that the F.T.C. fully proved its falsity case." *Federal Trade Comm'n v. Pantron I Corp.*, 33 F.3d 1088, 1101-02 (9th Cir. 1994).

Tenth Circuit

2005

"Although § 13(b) [of the FTC Act] does not expressly authorize a court to grant consumer redress (i.e., refund, restitution, rescission, or other equitable monetary relief), § 13(b)'s grant of authority to provide injunctive relief carries with it the full range of equitable remedies, including the power to grant consumer redress. In cases where the FTC seeks injunctive relief, courts deem any monetary relief sought as incidental to injunctive relief." *FTC v. Freecom Communs., Inc.*, 401 F.3d 1192, 1203 n.6 (10th Cir. 2005) (reversing an award of attorneys' fees against the FTC) (citations omitted).

Eleventh Circuit

2004

AT&T Broadband v. Tech Communications Inc., 381 F.3d 1309, 1316 (11th Cir.) (affirming the denial of a motion to unfreeze assets, and to return seized items). The district court granted an ex parte search and seizure order directed to a private residence, and to a warehouse, and an asset freeze order, against sellers of cable descrambling devices. The defendants later argued that the Cable Communications Policy Act ("CCPA"), 47 U.S.C. § 553(c)(2)(A) (2001), did not specifically authorize a district court to issue an ex parte order authorizing a freeze of assets, nor a search and seizure of property belonging to an alleged violator of the Act.

The 11th Circuit quoted the Supreme Court, as saying that unless the underlying statute clearly and validly limits the equitable jurisdiction of the district court, "all the inherent equitable powers of the District Court are available for the proper and complete exercise of that jurisdiction." *Porter v. Warner Holding Co.*, 328 U.S. 395, 398, 66 S. Ct. 1086, 1089 (1946) ("[u]nless a statute in so many words, or by a necessary and inescapable inference, restricts the court's jurisdiction in equity, the full scope of that jurisdiction is to

be recognized and applied. … [when] "the public interest is involved . . ., [the district court's] equitable powers assume an even broader and more flexible character.").

The 11th Circuit held that the district court did not abuse its discretion by 1) issuing the asset freeze, 2) refusing to dissolve the asset freeze, 3) issuing the ex parte search and seizure order directed at a defendant's residence, and 4) refusing to order the return of the seized items.

IV. Substantive Issues

A. Trademarks and Unfair Competition

1. Trademark Infringement and Dilution

Second Circuit

2004

Register.com v. Verio, Inc., 356 F.3d 393 (2d 2004) (affirming the grant of a preliminary injunction). Register serves as one of the registrars of internet domain names. In order to become a registrar, Register was required to enter into the standard agreement with ICANN. The ICANN Agreement requires the registrar to update registrant contact information daily. The registrant's contact information, under the rubric "WHOIS Information" is to be provided for free public access. The ICANN Agreement requires that the registrar "not impose terms and conditions" on the use of the WHOIS data by others. Third-parties, can seek enforcement of the registrar's obligations under the ICANN Agreement. Register includes notification of restrictions on use of the data, and gives registrants the option to receive marketing communications from the company.

Verio sells a variety of website design, development and operation services and competes with Register's website development business. In its pursuit of customers, Verio obtained daily updates of the WHOIS data using an automated software program. After acquiring the updated WHOIS information, Verio would send marketing solicitations by email, telemarketing and direct mail. Initially, Verio made reference to the registration with Register. When Register began receiving complaints regarding the solicitations, Register complained to Verio and demanded that Verio cease and desist. Verio then ceased mention of Register in its solicitations but continued its practices. In the meantime, Register changed its restrictions notification to bar mass solicitation "via direct mail, electronic mail, or by telephone," violating the ICANN Agreement.

When Verio continued its practices, Register brought suit alleging, inter alia, that Verio was: (1) causing confusion among customers, (2) accessing Register's computers without authorization in violation of the Computer Fraud and Abuse Act, and (3) trespassing on Register's chattels in a manner likely to harm Register's computer system. The district court entered a preliminary injunction barring Verio from the following: (1) "[u]sing or causing to be used the 'Register.com' marker or the 'first step on the web' mark or any other designation similar thereto, on or in connection with the advertising, marketing, or promotion of Verio and/or any of Verio's services"; (2) "Representing, or committing any act which is calculated to or is likely to cause third parties to believe that Verio and/or Verio's services are sponsored by, or have the endorsement or approval of Register.com"; (3) "Accessing Register.com's computers and computer networks in any manner, including, but not limited to, by software programs performing multiple, automated, successive queries, provided that nothing in this Order shall prohibit Verio from accessing Register.com's WHOIS database in accordance with the terms and conditions thereof"; and (4) using any data currently in Verio's possession that will enable the transmission of unsolicited commercial email, telephone calls, or direct mail.

The Second Circuit upheld the district court's findings that (1) Verio was bound by the restrictions Register imposed on the registrant data, (2) Reigster was likely to prevail on a claim that Verio's use of automated search software constituted trespass of chattels, and (3) that there was no abuse of discretion in finding that Verio's allegedly misleading sales warranted injunctive relief.

The Second Circuit first noted that Verio knew of the restrictions Register placed on the use of the WHOIS data, and violated its agreement with Register by its use of the data. In its defense, Verio argued that Register was in violation of the ICANN agreement and was thus prohibited from imposing such restrictions. The Court found that Verio's attempt, as a third party beneficiary to enforce Register's agreement with ICANN, failed to show under California law that the contract was made expressly for the benefit of a third person (Verio). The Court recognized that that the ICANN Agreement explicitly provided for redress of third party grievances through ICANN, and not through the courts.

On appeal, Verio also attempted to argue that it never became contractually bound by Register's additional restrictions as the restrictions did not appear until after Verio submitted its query and received the WHOIS data. The Second Circuit dismissed this argument, stating, "Verio's argument might well be persuasive if its queries addressed to Register's computers had been sporadic and infrequent . . . But Verio was daily submitting numerous queries, each of which resulted in its receiving notice of the terms Register exacted . . . Verio's argument fails." The Court then rejected Verio's argument that, even though it was fully aware of the restrictions imposed by Register, it was not bound by Register's restrictions "because it did not agree to be bound." Utilizing standard contract law the Second Circuit stated, "[w]hen a benefit is offered subject to stated conditions, and the offeree [Verio] makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the

terms, which accordingly become binding on the offeree." The Court affirmed the district court's conclusion that Register showed a likelihood of success on the merits of its contract claim against Verio.

Verio also attacked the granting of a preliminary injunction on Register's trespass to chattels claim. The Court agreed with the lower court that there was a high probability that, should Verio be allowed to utilize its automated search software, other ISPs would devise similar programs to access Register's WHOIS data, overtaxing the system. In its preliminary injunction, the district court also enjoined Verio from using Register's marks in its solicitations and from causing others to believe that Verio was sponsored or endorsed by Register. The Second Circuit found that this injunction was within the scope of the district court's discretion, because Verio's use of Register's mark was misleading.

Fourth Circuit

2003

International Bancorp LLC v. Societe des Bains de Mer et du Cercle des Etrangers a Monaco, No. 02-1364 (4th Cir. 5/19/03). Societe des Bains de Mer et du Cercle des Etrangers a Monaco ("SBM"), has owned and operated a casino under the "Casino de Monte Carlo" trademark since 1863. The mark is registered in Monaco, but not in the United States. For 18 years, SBM has promoted its properties from a New York office staffed with four employees. SBM's promotions within the United States, funded with $1 million annually, include trade show participation, advertising campaigns, charity partnerships, direct mail solicitation, telephone marketing, and solicitation of media coverage.

Appellants, the plaintiff companies, are five companies formed and controlled by a French national, which operate more than 150 web sites devoted to online gambling. Included in this roster are 53 web sites whose domain addresses incorporate some portion of the term "Casino de Monte Carlo."

When SBM learned of the plaintiff companies' web sites and their uses of the "Casino de Monte Carlo" mark, it challenged them in the World Intellectual Property Organization (WIPO). A WIPO panel ruled against the plaintiff companies and ordered the transfer of the 53 domain addresses to SBM. To escape this judgment, the plaintiff companies sued for a declaratory judgment that they were entitled to the disputed domain names. SBM counterclaimed for trademark infringement, trademark dilution, cybersquatting, and unfair competition.

The district court ruled against SBM on its trademark dilution claim, because SBM had not shown actual economic harm, and on its unfair competition claim. But the court ruled in favor of SBM on its trademark infringement claim and on its

cybersquatting claim, awarding SBM $51,000 in statutory damages, and transfer of 43 of the 53 contested domain addresses.

Both parties agreed that the critical question in assessing whether SBM "used its mark in commerce" was whether the services SBM provided under the "Casino de Monte Carlo" mark were rendered in commerce. The Fourth Circuit held that "'commerce' under the Act is coterminous with that commerce that Congress may regulate under the Commerce Clause of the United States Constitution."

> "The plaintiff companies conceded that the record contained evidence that United States citizens went to and gambled at the casino. This concession, when taken together with the undisputed fact that the Casino de Monte Carlo is a subject of a foreign nation, makes unavoidable the legal conclusion that foreign trade was present here, and that as such, so also was "commerce" under the Lanham Act.
>
> > Thus, while SBM's promotions within the United States do not on their own constitute a use in commerce of the "Casino de Monte Carlo" mark, the mark is nonetheless used in commerce because United States citizens purchase casino services sold by a subject of a foreign nation, which purchases constitute trade with a foreign nation that Congress may regulate under the Commerce Clause. And SBM's promotions "use[ ] or display[ ] [the mark] in the sale or advertising of [these] services . . . rendered in commerce."
> >
> > Because SBM used its mark in the sale and advertising of its gambling services to United States citizens; because its rendering of gambling services to United States citizens constitutes foreign trade; because foreign trade is commerce Congress may lawfully regulate; and because commerce under the Lanham Act comprises all commerce that Congress may lawfully regulate, the services SBM renders under the "Casino de Monte Carlo" mark to citizens of the United States are services rendered in commerce, and the "use in commerce" requirement that the Lanham Act sets forth for the mark's protectibility is satisfied."

Fifth Circuit

2004

TMI Inc. v. Maxwell, 70 USPQ2d 1630 (5th Cir. 2004) (reversing and rendering a judgment of $40,000 in statutory damages, and $40,000 in attorneys fees). Maxwell, an unhappy home-buyer, registered "trendmakerhome.com", and used the website as a gripe site. He also included on the website a place called a "Treasure Chest" for readers to share and obtain information about contractors and tradespeople who had done good work, and admitted that he had added that section to attract people to read his gripes about TMI. During the year of the site's existence, the Treasure Chest only

contained one name, that of a man who had performed some work for Maxwell. The site did not contain any paid advertisements. The Fifth Circuit ruled that although some e-mail intended for TMI was sent to Maxwell's site, because did not charge money for viewing the Treasure Chest portion of his site, and had no advertising or links to other sites, his site was not "commercial", and thus there was no liability under the ACPA nor under the dilution statutes. In a footnote, the Fifth Circuit incorrectly distinguished a contrary holding on the issue of "commercial use" of trademarks in *United We Stand America, Inc. v. United We Stand, America New York, Inc.*, 128 F.3d 86, 89-90 [44 USPQ2d 1351] (2d Cir. 1997), stating that such case did not "involve either the anti-dilution provision or ACPA and is, thus, irrelevant to the determination of whether these two sections require commercial use".

Sixth Circuit

2002

Bird v. Parsons, Dotster, & Afternic.com., 289 F.3d 865 (6th Cir. 2002). Since 1983, plaintiff Bird of Dayton, Ohio, had operated a software business using the name Financia Inc. In 1984, he obtained a trademark registration for FINANCIA. He also registered the domain name financia.com. In 2000, defendant Marshall Parsons of California registered the domain name efinancia.com with defendant domain name registrar Dotster Inc. of Longview, Wash. The day after Parsons registered the domain name, Afternic.com Inc. of New York listed efinancia.com on its domain name auction Web site.

Bird sued, alleging liability of the registrar for trademark infringement. The Sixth Circuit held, "A registrar that grants a particular domain name to a registrant simply grants it an address," the court said. "The fact that the registrant can then use its domain name to infringe on the rights of a registered trademark owner does not subject the registrar to liability for trademark infringement or unfair competition." Regarding the alleged liability of the auctioneer for dilution, the Sixth Circuit held "Simply posing a domain name on a Internet auction site …is insufficient to establish the commercial use of a trademark," the court concluded. "This reasoning also applies to an entity, such as Afternic, that operates an online auction site." Thus, there was no basis for a dilution claim.

2003

Taubman Co. v. Webfeats The Sixth Circuit held that a "fan" site that used the plaintiff's registered trademark did not cause a likelihood of confusion, because the defendant included a prominent disclaimer on his website. The Court also held that "gripe" websites did not infringe, and thus reversed the decision of the district court and dissolved a first preliminary injunction that had been entered against using shopsatwillowbend.com, and a second preliminary injunction that had been entered against using 1) taubmansucks.com; 2) shopsatwillowbendsucks.com; 3) theshopsatwillowbendsucks.com; 4) willowbendmallsucks.com; and 5) willowbendsucks.com.

PACCAR Inc. v. TeleScan Technologies LLC The Sixth Circuit held that a disclaimer on an Internet website read "after reaching the web site comes too late" to remedy any "initial interest confusion". The district court properly considered the eight "likelihood of confusion" factors from *Frisch's Restaurants Inc. v. Elby's Big Boy of Steubenville Inc.*, 670 F.2d 642 (6th Cir. 1982), which include: strength of the plaintiff's mark; relatedness of goods or services; similarity of the marks; evidence of actual confusion; marketing channels used; likely degree of purchaser care; intent of the defendant; and likelihood of expansion of product lines. Taking the position of the Ninth Circuit, the Sixth Circuit held that the district court was not clearly erroneous in finding that using the Internet as a marketing channel increases the likelihood of confusion.

Interactive Products Corp. v. A2Z Mobile Office Solutions Inc., No. 01-3590 (6th Cir. 4/10/03). "A website's domain name (e.g., a2zsolutions.com) signifies its source of origin and is, therefore, an important signal to Internet users who are seeking to locate web resources." "Because of the importance of a domain name in identifying the source of a website, many courts have held that the use of another's trademark within the domain name of a website can constitute a trademark violation," citing *Paccar Inc. v. Telescan Technologies LLC*, 319 F.3d 243 (6th Cir. 2003).

"Because post-domain paths do not typically signify source, it is unlikely that the presence of another's trademark in a post-domain path of a URL would ever violate trademark law." "It is enough to find that IPC has not presented any evidence that the presence of 'laptraveler' in the post-domain path of A2Z's portable-computer-stand web page is likely to cause consumer confusion regarding source of the web page or the source of the Mobile Desk product, which is offered for sale on the web page."

Seventh Circuit

Ninth Circuit

2002
D. Nev.

Visa International Service Association v. JSL Corp., 90 Fed.Appx. 484 (9th Cir. 2003). The court granted summary judgment injunctive relief for dilution to Visa, against the use of www.evisa.com for an English language school in Japan.

2004

Playboy Enterprises, Inc. v. Netscape Communications Corp., 354 F.3d 1020 (9th Cir. 2004) (reversing summary judgment in favor of defendants on Playboy's trademark infringement and dilution claims, and remanding for further proceedings). The defendants use a practice called "keying" that allows advertisers to target individuals by linking advertisements to pre-identified terms. When the pre-identified "keyed" terms are entered, a banner ad appears on the search result page. At issue in this case were two terms that the defendants had included in their key lists that are

Playboy's trademarks: "playboy" and "playmate". Whenever either of these words is included in a search, adult-oriented ads linked to these words would appear. Playboy introduced evidence that the adult-oriented banner ads are often graphic in nature and are confusingly labeled or not labeled at all. Playboy sued for trademark infringement and dilution. The district court denied Playboy's request for a preliminary injunction, and granted summary judgment in favor of defendants. Playboy appealed.

The Ninth Circuit examined the defenses in view of the eight-factor test that it uses to determine likelihood of confusion, and held that a fact issue existed as to whether the defendants' practice created a likelihood of initial interest confusion. Regarding the factors in the statutory test for dilution, the Court said that the only contested factor was "the nature and extent of use of the same or similar marks by third parties." The Court concluded that summary judgment was precluded because Playboy had established a genuine issue of material fact as to whether the defendants' practice diluted Playboy's marks. The Ninth Circuit remanded the case to the district court with instructions to re-open discovery. Under the new standard of dilution, to survive summary judgment a party has to show that actual dilution has occurred; the old standard only required a mere likelihood of dilution.

Nissan Motor Co. v. Nissan Computer Corp., No. 02-57148 (9th Cir. 8/6/04) (affirming summary judgment that links on Nissan Computer's website to automobile-related advertisements constituted trademark infringement on the basis of initial interest confusion, and affirming summary judgment that links to sites with disparaging or negative commentary about Nissan Motor did not constitute dilution).

About the links to disparaging websites, the Ninth Circuit said,

> "Although the boundary between commercial and noncommercial speech has yet to be clearly delineated, the core notion of commercial speech is that it does no more than propose a commercial transaction." *Mattel*, 296 F.3d at 906 (quoting *Hoffman v. Capital Cities/ABC, Inc.*, 255 F.3d 1180, 1184 (9th Cir. 2001)) (quotation marks omitted). "If speech is not 'purely commercial'—that is, if it does more than propose a commercial transaction—then it is entitled to full First Amendment protection." *Id*. Negative commentary about Nissan Motor does more than propose a commercial transaction and is, therefore, non-commercial. . . . Therefore, we conclude that the permanent injunction violates the First Amendment to the extent that it enjoins the placing of links on nissan.com to sites with disparaging comments about Nissan Motor."

2. Metatags, Header Tags, and Underline Tags

Don't use others' trademarks or names as metatags, header tags, or underline tags in your website.

Seventh Circuit

2000

Eli Lilly & Co. v. Natural Answers Inc., 233 F.3d 456, 464, 56 U.S.P.Q.2d 1942 (7th Cir. 2000) (affirming the district court's preliminary injunction). "The second fact probative of Natural Answers' wrongful intent is its references to PROZAC® in the source codes of its website. The clear intent of this effort, whether or not it was successful, was to divert Internet users searching for information on PROZAC® to Natural Answers' website [citing *Brookfield Communications* and *New York State Soc. of Certified Public Accountants*]. Because Natural Answers' wrongful intent is so obvious, we weigh it heavily."

2002

Promatek Industries Ltd. v. Equitrac Corp. In October the Court modified its August slip opinion by replacing a sentence with the following: ""The problem here is not that Equitrac, which repairs Promatek products, used Promatek's trademark in its metatag, but that it used that trademark in a way calculated to deceive consumers into thinking that Equitrac was Promatek." In an added footnote the Court stated: "It is not the case that trademarks can never appear in metatags, but that they may only do so where a legitimate use of the trademark is being made."

2003

N.D. Ill

International Star Registry of Illinois, Ltd. v. Bowman-Haight Ventures, Inc., No. 01 C 4687 (N.D. Ill. 07/09/03). The International Star Registry provides a service of assigning a requested name to a distant star. Plaintiff claimed ownership in the trademarks STAR REGISTRY and INTERNATIONAL STAR REGISTRY. Defendant operated a website offering similar services, and put on its website meta tags with the phrase "star registry". Plaintiff sued, and defendant moved for summary judgment on plaintiff's damages claims, arguing that the plaintiff lost no revenue because defendant's use of "star registry" in a meta tag should not, in theory, generate any higher ranking Internet search results than if defendant had merely used "star" and "registry" as separate keywords within the meta tag. Defendant argued that there could be no damages where the same result would be achieved regardless of whether defendant made a permissible or impermissible use of the terms. The court accepted the plaintiff's evidence to the contrary, and denied summary judgment.

Ninth Circuit

1999

Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 50 U.S.P.Q.2d 1545, 1564 (9th Cir. 1999) (reversing the denial of a preliminary injunction, and distinguishing *Playboy Enterprises, Inc. v. Welles*, 7 F. Supp. 2d 1098 (S.D. Cal. 1998), *aff'd*, 162 F.3d 1169 (9th Cir. 1998)). The Ninth Circuit has

followed its California trademark commentator, McCarthy, in his position on "initial interest confusion":

> "Nevertheless, West Coast's use of 'moviebuff.com' in metatags will still result in what is known as initial interest confusion."
>
> "Consistently with Dr. Seuss, the Second Circuit, and the cases which have addressed trademark infringement through metatags use, we conclude that the Lanham Act bars West Coast from including in its metatags any term confusingly similar with Brookfield's mark. ... Unlike the defendant in Holiday Inns, however, West Coast was not a passive figure; instead, it acted affirmatively in placing Brookfield's trademark in the metatags of its web site, thereby creating the initial interest confusion". *Id.* at 1566.
>
> "Preliminary injunctive relief is appropriate here to prevent irreparable injury to Brookfield's interests in its trademark 'MovieBuff' and to promote the public interest in protecting trademarks generally as well. ... When a firm uses a competitor's trademark in the domain name of its web site, users are likely to be confused as to its source or sponsorship. Similarly, using a competitor's trademark in the metatags of such web site is likely to cause what we have described as initial interest confusion. These forms of confusion are exactly what the trademark laws are designed to prevent. *Id.* at 1567.

2002
N.D. Cal.

J.K. Harris v. Kassel, 2002 WL 1303124 (N.D. Cal. March 22, 2002). While the defendants' use of plaintiff's trade name in links to other Web pages and in disseminating truthful information about Harris was nominative fair use, the use of "header tags" and "underline tags" around sentences containing the plaintiff's trade name was not necessary to reasonable identify it, and therefore was likely to cause initial interest confusion.

2003

Horphag Research Ltd. v. Pellegrini d/b/a Healthdiscovery.com, No. 01-56733 (9th Cir. 5/9/03); ***Horphag Research Ltd. v. Garcia d/b/a Healthierlife.com***, No. 02-55142 (9th Cir. 5/9/03). Horphag Research Ltd. is the holder of the trademark Pycnogenol for use in connection with a pine bark extract product. The defendant, Larry Garcia, operated a website having the domain name healthierlife.com, through which he sold pharmaceutical products, including a product that competed with Pycnogenol. The website, in comparing its product to the plaintiff's product, repeatedly used the term "Pycnogenol" in its content and in its metatags. It also labeled its competing product as "Masquelier's: the original French Pycnogenol."

The Ninth Circuit affirmed a finding of infringement, stating, "By using the mark so pervasively, not just in the text of his websites but also in the meta-tags used to link others to his websites, Garcia exceeds any measure of reasonable necessity in using the Pycnogenol mark." "Moreover, the constant use of Horphag's Pycnogenol

trademark and variants thereof, such as 'the Original French Pycnogenol,' likely suggests that Horphag sponsors or is associated with Garcia's websites and products."

N.D. Cal.

J.K. Harris v. Kassel The court vacated its March 22, 2002, preliminary injunction order, substituting a new order withdrawing its analysis of the nominative fair use issue under *New Kids on the Block v. News America Publishing Co.*, 971 F.2d 302 (9th Cir. 1992). It reversed its prior ruling that some of the taxes.com Web site's uses of the J.K. Harris trademark--especially in "header tags" and "underline" tags--were unreasonable. "Similarly, while the evidence submitted to the Court demonstrates that Defendants often made the J.K. Harris name visually obvious, this is not unreasonable, because criticizing J.K. Harris was one of the primary objectives of the web pages. ... Thus, Defendants' referential use of the J.K. Harris trade name, even though frequent and obvious, satisfies the second prong of the *New Kids on the Block* Test."

2003

W.D. Wash.

Flow Control Industries Inc. v. AMHI Inc., No. C02-1101L (W.D. Wash. 3/12/03). The parties are competitors in manufacturing valves. Flow Control put AMHI's federally registered trademark "AMFLO" and the word "amflow" as metatags on Flow Control's website. In retaliation, AMHI put Flow Control's trademarks, including "SKOFLO" as metatags on its website; and it also registered the domain name skoflo.com, and linked that address to its own website. The parties sued each other, and Flow Control moved for summary judgment on its claims of infringement and cybersquatting.

The court found trademark infringement (via "initial interest confusion", even though the customers were sophisticated) and cybersquatting. The court stated: "Defendants do not dispute, however, that the customer base for their products is quite small, such that one or two customers lost or gained per year would make a real difference to the parties. … In short, defendants used plaintiff's mark in such a way as to divert people looking for SKOFLO products to the A&H Web site, thereby improperly benefiting from the goodwill that plaintiff developed in its mark."

B. Domain Names

The "Internet Corporation for Assigned Names and Numbers" ("ICANN") is a non-profit corporation formed in 1998. The U.S. government has recognized it as the technical coordinator of the Internet's domain name system. You can visit its website at www.icann.org. The ICANN Board of Directors, in a meeting in Yokohama, Japan, on July 16, 2000, adopted a resolution calling for the establishment of a policy to introduce new top-level domains (TLDs). As a result, new opportunities in Internet domain names arose, for both clients and their lawyers.

During June and July, 2001, individuals and companies could register domain names associated with two new generic top level domains (gTLD's), which are the last part of the Internet address. Existing gTLD's included .com, .net, and .org (there are others, but these three are the only ones for which anybody can register a domain name). The new gTLD's were .info (completely unrestricted) and .biz (restricted to business/commercial sites).

".info"

The registrar for .info, Afilias, in an effort to protect owners of registered trademarks, had what is called a "Sunrise Period," during which only owners of registered trademarks could register their domain names in advance of the general public. Afilias provided this registration period in an attempt to prevent the problems of cybersquatting and domain name speculation.

During the Sunrise period, Afilias accepted registrations in 5 rounds. A randomized, round-robin processing system limited any one registrant's ability to gain in domain name submissions. Disputes regarding conflicting marks may be raised according to Afilias' Sunrise Challenge policy.

".biz"

There was no "sunrise" period for the .biz gTLD. However the registrar for .biz, Neulevel, Inc., offered a fee-based service that notified trademark owners when someone tried to register a domain name in which they have expressed an interest (a "claimed" domain name). If a person submitted an application for a claimed domain name, they were to be notified that the claim existed. If they registered the name anyway, the claim holder was to be given an opportunity to contest the registration. The service cost $90 per claim. Claim applications were accepted only through July 9, 2001 (later extended), at which point in time (or shortly thereafter) the actual registration of the names began.

ICANN learned from the problems in the offerings of those gTLD's, and later offered additional ones, so that in 2004, the total available gTLD's were:

.**aero**, (restricted to certain members of the global aviation community) sponsored by Societe Internationale de Telecommunications Aeronautiques SC (SITA)

.**biz**, (restricted to businesses), operated by NeuLevel

.**com**, operated by Verisign Global Registry Services

.**coop**, (restricted to cooperatives) sponsored by Dot Cooperation LLC

.**info**, operated by Afilias Limited

.**museum** (restricted to museums and related persons), sponsored by the Museum Domain Management Association (MuseDoma)

.**name**, (restricted to individuals), operated by Global Name Registry

.**net**, operated by Verisign Global Registry Services

.**org**, operated by Public Interest Registry

.**pro**, (restricted to licensed professionals) operated by RegistryPro

Although it would be interesting to detail all the various problems encountered in issuing new gTLD's, this article is not about the mere history of Internet domain names, but rather the history of Internet domain name disputes.

1. Arbitrator For Disputes Involving .biz gTLD

Gene Logic v. Cho Kyu Bock, Claim Number: FA0112000103042, March 4, 2002. Gene Logic Inc. of Gaitherburg, Md., had registered the mark GENE LOGIC in the United States, Japan, and in the European Community in connection with its work in genomics research and related software development, and had a web site, genelogic.com. Cho Kyu Bock of South Korea registered the domain name genelogic.biz. Gene Logic complained under the Start-up Trademark Opposition Policy ("STOP") to NeuLevel Inc., the administrator of the .biz gTLD.

The STOP, which applies to all .biz domain name registrants by contract, authorizes an administrative arbitrator to cancel or transfer a domain name registration upon finding that 1) the domain name is identical to a mark in which the complainant has rights, 2) the registrant has no rights or legitimate interests in the domain name, and 3) the domain name has been registered or is being used in bad faith.

The arbitrator noted that NeuLevel's procedures permitted a mark owner to file an IP Claim with regard to a domain name. When Bock filed his application for a domain name, he was notified of Gene Logic's IP Claim filed with regard to Bock's registration. Consequently, the arbitrator found, "in the instant case of Respondent Cho Kyu Bock and his selection of the domain <genelogic.biz>, he did so with full knowledge that his intended business use of this domain name was in direct conflict with a registered trademark of a known competitor in exactly the same field of business." Thus, the arbitrator found bad faith by Bock, and ordered the transfer of genelogic.biz to Gene Logic.

2. Domain Name Disputes

As the Internet continues to grow in popularity, so do disputes involving domain names. For example, here in the U.S, it generally appears that when a domain name incorporates a trademark, the trademark owner usually prevails over the other party when the goods and services of the trademark are related to the goods and services offered on website associated with the domain name at issue. Courts, however, have

considered factors such as whether there is commercial use of the domain name, and whether the domain name owner's intent is to confuse the consuming public.

Below is a subset of the seminal cases in each circuit.

First Circuit

2000

Hasbro, Inc. v. Clue Computing, Inc., 232 F.3d 1, 56 U.S.P.Q.2d 1766 (1st Cir. 2000) (affirmed per curium). Clue Computing, Inc., of Colorado, provides computer consulting and Internet access services, and obtained the domain name "clue.com" for its business web site. In 1996, Hasbro notified Network Solutions, Inc. that Hasbro owned a trademark on the word "clue". Network Solutions then informed Clue Computing that its use of the "clue.com" domain name would soon be terminated. Clue Computing responded by suing Network Solutions in Colorado state court, and won a preliminary injunction against the threatened termination. Hasbro then sued Clue Computing in federal district court in Massachusetts, charging Clue Computing with infringement and dilution of the Clue® trademark. The district court granted judgment in favor of Clue Computing on Hasbro's trademark infringement claim (seeing very little similarity between Hasbro's products and services and those of Clue Computing), and on Hasbro's federal and state dilution claims, finding that the Clue mark was not famous, that Clue Computing's use of the domain name did not blur or tarnish Hasbro's mark, and that in any event the equities would not justify an injunction.

Second Circuit

1997

Planned Parenthood Fed'n. of America Inc. v. Bucci, 1997 WL 133313, 42 U.S.P.Q.2d 1430 (S.D.N.Y. March 19, 1997), (*aff'd*, 152 F.3d 920, *cert. denied*, 119 S. Ct. 90). The court granted a preliminary injunction against the defendant, an outspoken opponent of the plaintiff, who had registered the domain name "plannedparenthood.com" citing *inter alia* a significant likelihood of confusion with the plaintiff.

Toys R Us, Inc. v. Abir, 45 U.S.P.Q.2d 1944 (S.D.N.Y. 1997). The district court granted a preliminary injunction against Abir to stop his use of toysareus.com, citing *inter alia* dilution of plaintiff's mark.

2001

TCPIP Holding Co., Inc. v. Haar Communications Inc., 244 F.3d 88 (2d Cir. 2001) (vacating a preliminary injunction against the use of 81 domain names, based on dilution, and affirming it for some of the domain names, based on infringement). For approximately 30 years, plaintiff operated a chain of retail stores selling children's clothing and accessories under the federally registered trademark THE CHILDREN'S PLACE. Plaintiff's chain of more than 200 stores had annual revenues of almost $300 million.

In the fall of 1998, defendant developed the idea of creating an Internet portal for children that would provide information and links about a broad array of child-related products and services. Shortly thereafter, defendant registered the domain name "thechildrensplace.com." In early 1999, plaintiff sent defendant a letter demanding that defendant transfer this domain name to plaintiff. Defendant then registered at least 66 more domain names containing variations of the words "children" and "place." After negotiations to purchase the domain name failed, plaintiff sued, alleging trademark infringement, dilution, and unfair competition, and filed a motion for a preliminary injunction, which the court granted.

The Second Circuit held that descriptive marks like plaintiff's mark THE CHILDREN'S PLACE, "which possessed no distinctive quality, or at best a minimal degree, do not qualify for the Act's protection," even if the mark had acquired secondary meaning. The Second Circuit further held that protection was available only if the marks "carried a substantial degree of fame".

Assuming for sake of argument that descriptive marks could be protected under the FTDA, the Second Circuit held that because plaintiff failed to provide statistics for any years earlier than 1994, and failed to submit consumer surveys, press accounts, or other evidence of fame, it did not demonstrate the requisite degree of fame.

The Court affirmed the preliminary injunction as to nine domain names that were virtually identical to plaintiff's mark. Because of the weak, descriptive nature of plaintiff's mark, the court held that the injunction was inappropriate as to any domain names that differed somewhat from plaintiff's mark (e.g., achildplace.com, yourchildsplace.com, mychildsplace.com, ourchildrensplace.com).

Third Circuit

1998

Jews for Jesus v. Brodsky, 993 F. Supp. 282, 46 U.S.P.Q.2d 1652, 1656 (D.N.J. 1998), aff'd, 159 F.3d 1351 (3d Cir. 1998). "Jews for Jesus" ("JFJ") is a non-profit, international outreach ministry that was founded in 1973. It teaches that Jesus is the Messiah of Israel, and the Savior of the World. Its mission includes advocacy, education, and religious camaraderie for both Gentiles and Jews. In 1998 it had 145 staff members, twelve permanent branches worldwide, and an additional 68 chapters.

JFJ "has expended a substantial amount of money publishing ads in national publications like the *New York Times*, the *Washington Post*, the *Wall Street Journal*, *Newsweek*, *Parade*, and *TV Guide*." In March 1995, the JFJ opened a website with the domain name "jews-for-jesus.org."

Brodsky is a professional Internet site developer, an attorney, and a vocal opponent of JFJ. In December 1997, Brodsky opened a web site with the address "jewsforjesus.org", which had one page of text, referred to JFJ, and contained a hyperlink to the Outreach Judaism Organization's Internet site. The Outreach Judaism Organization is also a vocal opponent of JFJ.

JFJ asked Brodsky to stop using its name as his web site address. In response, Brodsky registered a second domain name, "jews-for-jesus.com". After getting no response to a second letter, JFJ sued for a preliminary injunction, which the court granted, finding a likelihood of infringement and dilution.

The Third Circuit affirmed, stating, "considering the vastness of the Internet and its relatively recent availability to the general public, many Internet users are not sophisticated enough to distinguish between the subtle difference in the domain names of the parties." The Court also stated, "a reading of the Defendant['s] Internet site will not eliminate the likelihood of confusion between the Defendant's Internet site and the mark and/or the name of the Plaintiff's organization. This is so even with the addition of the [Defendant's] Disclaimer. . . . The Defendant also stated he intended to use "deceit and trickery" to direct persons to his Internet site." *Id*. at 1669.

The website "jewsforjesus.org" is now owned and operated by the "Jews For Jesus" organization.

2001

Checkpoint Systems Inc. v. Check Point Software Techs., 269 F.3d 270 (3rd Cir. 2001). Initial interest confusion may be a legitimate factor to be considered in a trademark infringement case involving two companies in different sectors of the corporate security industry, but it is only one factor in considering the likelihood of confusion in the marketplace, and may be outweighed by other factors.

Fourth Circuit

1997

CardService International, Inc. v. McGee, 950 F. Supp. 737, 42 U.S.P.Q.2d 1850, 1852 (E.D. Va. 1997), aff'd, 129 F.3d 1258 (4th Cir. 1997) (granting a permanent injunction against the cybersquatter). Cardservice International provides credit and debit card processing, and owns the registered trademark "Cardservice International". McGee registered "cardservice.com" with NSI, refused to relinquish his domain name, and represented himself, instead of hiring a lawyer. The court ruled,

> "McGee cites Network Solutions' policy of granting domain names on a first-come-first-served basis. Such a policy cannot trump federal law. Holders of valid trademarks under federal law are not subject to company policy, nor can the rights of those trademark holders be changed without congressional actions. If trademark laws apply to domain names, anyone who obtains a domain name under Network Solutions' 'first-come-first-served' policy must do so subject to whatever liability is provided for by federal law."

1999

Washington Speakers Bureau, Inc. v. Leading Auths., Inc. 33 F. Supp. 2d 488, 49 U.S.P.Q.2d 1893, 1895-96 (E.D. Va. 1999), *aff'd*, 217 F.3d 843 (4th Cir. 2000); *see also* 51 USPQ2d 1478, for order vacating prior order staying the judgment. Washington Speakers Bureau ("WSB") did not have a registration for its "Washington Speakers Bureau" trademark, when Leading Authorities obtained the domain names "washingtonspeakers" and "washington-speakers". The Court held:

> While knowledge of a senior user's mark "does not necessarily give rise to a presumption of bad faith," in light of the evidence suggesting that other domain names were selected expressly because of their similarity to competitors' names,

the washingtonspeakers names were more likely than not chosen in part because of this very similarity in a "bad faith" attempt to attract business that might otherwise have gone to WSB and to place barriers in the path of WSB's use of the Internet to attract customers.

While the record otherwise suggests that the phrase "Washington Speakers" is a weak segment of the "Washington Speakers Bureau" mark provoking limited consumer association with WSB, Leading Authorities' behavior in intentionally appropriating the mark constitutes conclusive evidence to the contrary.

Although the court found a likelihood of confusion, and thus infringement, it did not find enough "fame" in the mark to qualify for dilution. The court ordered the defendant to relinquish the four domain names:

www.washingtonspeakers.com;
www.washington-speakers.com;
www.washingtonspeakers.net ; and
www.washington-speakers.net.

E.D. Va.

Porsche Cars North America, Inc. v. Porsch.com, 51 F. Supp. 2d 707 (E.D. Va. 1999) (dismissing Porsche's in rem action against 128 domain names as not permitted under the federal dilution statute). Porsche tried, and temporarily failed, to solve the logistical and practical problems involved in pursuing all those using the Porsche names, by suing the actual domain name registrations. *Porsche Cars North America, Inc. v. Porsch.com*, 51 F. Supp. 2d 707, 51 U.S.P.Q.2d 1461 (E.D. Va. 1999) (dismissing Porsche's in rem action against 128 domain names as not permitted under the federal dilution statute).

HQM, Ltd. v. Hatfield, 71 F. Supp. 2d 500 (D. Md. 1999). Plaintiff makes meat products, owns a Hatfield mark used since 1946, and a Hatfield design mark used since 1956. Defendant William Hatfield registered hatfield.com in 1995. He rented it to others to use as part of their e-mail address. In 1999, the plaintiff sued for trademark infringement, unfair competition, and dilution. On December 2, 1999, the court dismissed the complaint, stating that mere registration of the name, and using it for email, was not "commercial use". Thus, there were no sufficient allegations that the defendant was using the mark in connection with any goods or services. Further, the court held that the potential failure of consumers to continue searching for plaintiff's website was not dilution. Unfortunately for the plaintiff, the court then requested "materials addressing attorney's fees and costs within 14 days".

2001

America Online, Inc. v. AT & T Corp., 243 F.3d 812 (4th Cir. 2001) (affirming summary judgment that "YOU HAVE MAIL" and "IM" were generic, but vacating and remanding for further consideration the ruling that "BUDDY LIST" was generic).

AOL sued AT&T, claiming that AT&T's use of the phrases "You Have Mail", "I'm Here", and "Buddy List" for e-mail and Internet messaging-related services infringed and diluted AOL's rights in the marks YOU HAVE MAIL, BUDDY LIST, and IM for identical services. (IM are the initials of instant messaging.) The district court found all three marks to be generic.

The Fourth Circuit ruled that AOL's registration for "Buddy List" was not only prima facie evidence of the validity of the mark, but also prima facie evidence that the mark was suggestive. The district court's acceptance of the registration certificate into evidence was sufficient to establish a question of material fact that could not be resolved on summary judgment.

MicroStrategy Inc. v. Motorola, Inc., 245 F.3d 335 (4th Cir. 2001) (affirming denial of a preliminary injunction). Motorola filed an intent-to-use application for "Intelligence Everywhere", for a lot of its products and services. Motorola then registered the domain name "intelligenceeverywhere.com" with Network Solutions, Inc. MicroStrategy, a producer of communication software, later sued Motorola for trademark infringement, trademark dilution, and cyber squatting, and asked for a preliminary injunction to prevent Motorola from launching its planned global advertising campaign around the "Intelligence Everywhere" mark, scheduled to begin the week of March 19, 2001.

The court denied the motion for a preliminary injunction. The Fourth Circuit affirmed, stating that Microstrategy "has presented a record of limited, sporadic, and inconsistent use of the phrase 'Intelligence Everywhere.'"

Sixth Circuit

1998

Data Concepts, Inc.v. Digital Consulting, Inc., 150 F.3d 620, 47 U.S.P.Q.2d 1672, 1677 (6th Cir. 1998). In 1987, Digital Consulting, Inc. ("Digital") obtained a federal trademark registration for the mark "DCI". In 1993, Data Concepts, Inc. ("Data") registered "dci.com" with NSI. The district court adopted the magistrate judge's findings of a likelihood of confusion, and granted summary judgment. The Sixth Circuit reversed and remanded for trial on the issue of infringement, stating, "The record indicates that Data really was unaware of Digital at the time it decided to use DCI as part of its Internet address. Such evidence usually militates in favor of finding no intent, which weighs against a finding of a likelihood of confusion."

Seventh Circuit

1996

Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1240, 40 U.S.P.Q.2d 1412, 41 U.S.P.Q.2d 1223 (N.D. Ill. 1996) (finding dilution in Toeppen's use of intermatic.com. as a domain name, because such use "lessens the capacity of Intermatic to identify and distinguish its goods and services by means of the Internet").

1997

Juno Online Servs., L.P. v. Juno Lighting, Inc., 979 F. Supp. 684, 44 U.S.P.Q.2d 1913 (N.D.Ill. 1997) (denying money damages to the plaintiff ISP for defendant's attempt to stop plaintiff's use of the "juno.com" domain name, and for defendant's registration of "juno-online.com" domain name).

Ninth Circuit

1996

Comp Exam'r Agency, Inc. v. Juris, Inc., No. 96-213, 1996 WL 376600 (C.D. Cal. Apr. 26, 1996) (granting a preliminary injunction against using juris.com as a domain name, because it would likely confuse consumers). The "consumers" are lawyers -- I guess we are easily confused???.

Hasbro, Inc. v. Internet Entertainment Group, Ltd., 40 U.S.P.Q.2d 1479 (W.D. Wash. 1996) (granting a preliminary injunction against using candyland.com as a domain name for a sexually explicit web site, because it would dilute plaintiff's trademark, "Candyland", for a children's game).

1997

Academy of Motion Picture Arts & Sciences v. Network Solutions, Inc., 989 F. Supp. 1276, 45 U.S.P.Q.2d 1463 (C.D. Cal. 1997) (denying a motion for a preliminary injunction against Network Solutions, for the registration of "Academy"- and "Oscar" derived Internet domain names) The court found that because Network Solutions does not market its registration service or the quality of its service by displaying or otherwise exploiting the mark in question, the domain name is not a "good or service". Therefore, the court held that the mere registration of a domain name by Network solutions does not constitute commercial use).

Lockheed Martin Corp v. Network Solutions, Inc., 985 F. Supp. 949, 44 U.S.P.Q. 2d 1865 (C.D. Cal. 1997), aff'd, 194 F.3d 980 (granting NSI's motion for summary judgment, holding that NSI was not liable for trademark infringement based on its granting registrations of domain names that included plaintiff's service mark "Skunk Works").

Lozano Enter. v. La Opinion Publ'g Co., 44 U.S.P.Q.2d 1764 (C.D. Cal. 1997) (granting plaintiff's motion for summary judgment for defendant's use of the domain name laopinion.com, finding a likelihood of confusion with plaintiff's trademark "La Opinion").

Playboy Enterprises Inc. v. Calvin Designer Label, 985 F. Supp. 1220 (N.D. Cal. 1997) (granting a preliminary injunction for trademark infringement, against using "Playboyxxx" and "Playmatelive" as domain names or as hidden search terms).

Teletech Customer Care Mgt., Inc. v. Tele-Tech Co., 977 F. Supp. 1407 (C.D. Cal. 1997) (granting a preliminary injunction under dilution statutes against using the trademark "TeleTech" as a domain name).

1998

Panavision Int'l L.P. v. Toeppen, 141 F.3d 1316, 46 U.S.P.Q.2d 1511, 1518 (9th Cir. 1998). Toeppen did not challenge the famousness prong of the dilution tests, and did not challenge the factual assertion that he sought to profit by arbitrage with famous trademarks. Instead, he argued that his use of Panavision's marks as domain names was not "commercial". The Ninth Circuit held that his business was to "act as a spoiler", by grabbing domain names, and then selling them to the trademark owners, and thus, commercial use.

The Ninth Circuit found dilution, quoting from the *Jews for Jesus* case: "Prospective users of plaintiff's services who mistakenly access defendant's web site may fail to continue to search for plaintiff's own home page, due to anger, frustration or the belief that plaintiff's home page does not exist." *Id.* at 1521.

No Mayo -- San Francisco v. Memminger, 1998 WL 544974, 1998 U.S. Dist. LEXIS 13154 (N.D. Cal. August 19, 1998) (finding no jurisdiction over the defendant despite an allegation that he registered the domain name nomayo.com with the intent of selling it to the plaintiff).

1999

Avery Dennison Corp. v. Sumpton, 189 F.3d 868, 51 U.S.P.Q.2d 1801, 1805 (9th Cir. 1999) (quoting *I.P. Lund Trading ApS v. Kohler Co.*, 163 F.3d 27, 46 (1st Cir. 1998) (quoting 3 McCarthy, S 24.91)). Mailbank.com is an online service that sells personalized e-mail and Web addresses to individuals. Free View Listings Ltd., which operates Mailbank.com, registered avery.net and dennison.net domain names for use by people with those as first or last names. Avery Dennison sued, claiming dilution of its trademarks. The U.S. District Court for the Central District of California ruled in Avery Dennison's favor, and ordered the president of Free View, Jerry Sumpton, to transfer the domain name registrations to the company in exchange for $300 each).

> "[I]njunctive relief is available under the Federal Trademark Dilution Act if a plaintiff can establish that (1) its mark is famous; (2) the defendant is making commercial use of the mark in commerce; (3) the defendant's use began after the plaintiff's mark became famous; and (4) the defendant's use presents a likelihood of dilution of the distinctive value of the mark."

Avery Dennison Corp. v. Sumpton, 189 F.3d 868, 51 U.S.P.Q.2d 1801, 1805 (9th Cir. 1999) (citing *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1324 (9th Cir. 1998) (interpreting 15 U.S.C. S 1125(c)(1))).

In August 1999, the Ninth Circuit reversed, holding that the Avery and Dennison trademarks are not famous enough to prevent another company from registering them with the .net domain name. The Ninth Circuit ordered summary judgment for Sumpton, and ordered the district court to consider Sumpton's request for attorneys' fees). "[T]o meet the 'famousness' element of protection under the dilution statutes, a mark [must] be truly prominent and renowned".

In its reasoning, the Ninth Circuit stated, "Applying the famousness factors from the Federal Trademark Dilution Act to the facts of the case at bench, we conclude that Avery Dennison likely establishes acquired distinctiveness in the 'Avery' and 'Dennison' trademarks, but goes no further." *Id*. at 1806. The Court also stated, "All relevant evidence on the record tends to establish that both 'Avery' and 'Dennison' are commonly used as trademarks, both on and off of the Internet, by parties other than Avery Dennison."

2000

GoTo.com Inc. v. Walt Disney Co., 202 F.3d 1199, 53 U.S.P.Q.2d 1652, 1659 (9th Cir. 2000) (confirming its January 27 order lifting the stay of a preliminary injunction, and reinstating the original order enjoining the Walt Disney Co. from using its "Go Network" logo). In this case involving two Internet search engines using similar logos, the Ninth Circuit found that "the logos are glaringly similar," and "it is precisely the identical colors that create the confusion: white script in a green circle on a yellow square." The Ninth Circuit also stated that the "Securities and Exchange Commission required a disclaimer on the cover of GoTo's prospectus for its initial public offering, disavowing any connection between Disney and GoTo . . . which suggests to us that the Commission's concern was with the similarity of these two logos."

The Ninth Circuit then commented on the effect of the Internet on the "likelihood of confusion":

> "We now reiterate that the Web as a marketing channel, is particularly susceptible to a likelihood of confusion." . . . "It allows for competing marks to be encountered at the same time, on the same screen." "Navigating amongst web sites involves practically no effort whatsoever, and arguments that Web users exercise a great deal of care before clicking on hyperlinks are unconvincing."

2002

***Entrepreneur Media Inc. v. Smith.*, 279** F.3d 1135 (9th Cir. 2002). The Ninth Circuit held that the domain name entrepreneurpr.com does not infringe the descriptive mark ENTREPRENEUR finding, *inter alia*, that the addition of the letters "PR" serves effectively to signal an important distinction between it and the mark in question. The Court also found it unlikely that Internet users would unintentionally access the entrepreneurpr.com web site when trying to find the trademark owner's website, via the trademark owner's domain names entrepreneur.com and entrepreneurmag.com.

Interstellar Starship Servs., Ltd. v. Epix, Inc., 64 USPQ2d 1514 (9th Cir. 2002). Epix manufactures and sells a wide variety of electronic imaging hardware and software products, and has a registration for EPIX for use with "printed circuit boards and computer programs for image acquisition, processing, display, and transmission." In 1995, Tchou, the sole founder, officer, director, shareholder, and employee of Interstellar Starship Services ("ISS"), registered the domain name www.epix.com with Network Solutions. Epix demanded that Network Solutions cancel ISS's epix.com

registration. When informed by Network Solutions of Epix's demand, ISS filed for a declaratory judgment of non-infringement.

The Ninth Circuit repeated its prior statement that "the three most important *Sleekcraft* factors in evaluating a likelihood of confusion are (1) the similarity of the marks, (2) the relatedness of the goods or services, and (3) the parties' simultaneous use of the Web as a marketing channel." The Court affirmed the district court determinations that EPIX is a weak mark, and that ISS's primary purpose — the promotion of the Clinton Street Cabaret — did not compete with Epix's electronic imaging products, although ISS's incidental purpose — digital image processing and computer-related services — appeared, "at least superficially," to be the same as services offered by Epix. Accordingly, the Ninth Circuit refused to hold that all uses of www.epix.com would generate initial interest confusion with the EPIX mark.

Tenth Circuit

1996

Network Solutions, Inc. v. Clue Computing Inc., 946 F. Supp. 858, 41 U.S.P.Q.2d 1062 (D. Colo. 1996) (dismissing NSI's interpleader action to resolve the dispute between Hasbro and Clue Computing over the right to use "clue.com" as a domain name).

2000

Creative Gifts, Inc. v. UFO., 235 F.3d 540 (10th Cir. 2000) (affirming the transfer of "levitron.com" to plaintiff, and enjoining defendant's future use of the LEVITRON mark). In 1995, plaintiff obtained a federal registration for the mark LEVITRON & design for antigravity tops. Shortly thereafter, plaintiff and defendants entered into a business relationship under which defendant purchased and sold LEVITRON antigravity tops. In October 1996, the parties reached an oral agreement for defendants to register the domain name "levitron.com" to operate a website to sell LEVITRON tops. After negotiations broke down over formalizing a trademark license for defendants to use the LEVITRON mark and the "levitron.com" domain name, plaintiff withdrew permission for defendants to use the mark in the domain name, and then sued defendants.

The district court held that the term LEVITRON was not generic, and that defendants' use of the "levitron.com" domain name infringed the LEVITRON mark. The court also dismissed all 23 of defendants' counterclaims with prejudice as a Rule 37 sanction for numerous discovery violations.

The Tenth Circuit affirmed, noting that the defendants did not offer any of the typical evidence on the issue of genericness: "They elicited no consumer testimony or consumer surveys. Nor did they, on the basis of the record before us, proffer any listings in dictionaries, trade journals or newspapers."

3. Anticybersquatting Consumer Protection Act ("ACPA")

Effective November 29, 1999, we have a law that allows you to sue the actual domain name, rather than the owner of the domain name. Remember Porsche's failed attempt to do that in 1999 against 128 domain names? The "Anticybersquatting Consumer Protection Act" ("ACPA") gives remedies against one who with bad faith uses another's trademark as her own domain name. After this law passed, and Porsche appealed its dismissal by the district court, the appeals court vacated the dismissal. *See below*, under the year 2000 cases.

The ACPA is found at 15 U.S.C. 1125(d). The elements include: a bad faith intent to profit, by one who registers, traffics in, or uses a name which is identical or confusingly similar to, or dilutes, a famous mark. The ACPA added to the laws of infringement and dilution by making it possible to find liability without regard to the goods or services of the parties.

> (d) Cyberpiracy prevention
> (1)
> (A) A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person—
>
> > (i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and
> > (ii) registers, traffics in, or uses a domain name that—
> >
> > > (I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;
> > > (II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or
> > > (III) is a trademark, word, or name protected by reason of section 706 of title 18 or section 220506 of title 36.

The non-exhaustive list of factors to be considered in deciding whether the defendant had a bad faith intent include:

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 goods or services;
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 the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of 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 in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section.

Most of these factors are easily measurable, except for numbers 4, 5, and 9. Thus, factors 4, 5, and 9 are the ones that occupy the attention of many courts.

The ACPA allows in rem actions against the domain name, in the judicial district of the registrar or registry, if 1) the domain name infringes or dilutes, and 2) in personam jurisdiction is impossible, or, with due diligence the plaintiff can't find the defendant after sending snail mail and e-mail, and publishing a notice if the court requires it. . In 2004, there were over 300 accredited registrars. You can see the list at: http://www.icann.org/registrars/accredited-list.html. The most popular ones are NSI, located in Virginia, and register.com, located in New York.

First Circuit

2001

Northern Light Tech., Inc. v. Northern Lights Club, 236 F.3d 57, 57 USPQ2d 1277 (1st Cir. 2001) (affirming a preliminary injunction that required defendant to post a disclaimer on defendant's search site). Plaintiff registered its "northernlight.com" domain name in September, 1996, and began operating its NORTHERN LIGHT search engine at that domain name in August, 1997. Defendant is a one-person unincorporated association owned by Jeff Burgar, the contact person for several thousand domain names. Burgar has been associated with many vanity e-mail services, including FlairMail.com, which register and license domain names as part of e-mail addresses. Defendant registered the domain name "northernlights.com" in October, 1996, and began using it as a vanity e-mail address shortly thereafter.

In April, 1999, defendant began using the "northernlights.com" domain name as an Internet search site. In addition, that site provided a list of businesses using the

name “Northern Light,” including plaintiff’s search engine, and provided links to various sites, including the FlairMail site. Plaintiff’s search site began receiving several thousand referrals per day from defendant’s search site.

Plaintiff obtained a preliminary injunction, requiring defendant to post a specified disclaimer on defendant’s search site. The First Circuit affirmed, noting the defendant’s “well-established pattern of registering multiple domain names containing famous trademarks, such as rollingstones.com, evinrude.com, and givenchy.com.” The First Circuit speculated in a footnote that the defendant “likely hoped to cash in on the confusion surrounding the sponsorship of the websites by finding famous trademark holders willing to pay defendants to end the diversion of Internet traffic from their website to defendants’ sites.”

Sallen v. Corinthians Licenciamentos, 273 F.3d 14 (1st Cir. 2001). After losing control of the domain name “corinthians.com” in a UDRP proceeding, the registrant of the domain name sued to recover control from the Brazilian licensee of the soccer team Corinthiao. The First Circuit held that a domain name registrant who lost an arbitration proceeding under the UDRP can sue under the ACPA to reclaim the domain name.

2002

D. Mass.

Toronto Dominion Bank v. Karpachev, 188 F. Supp. 2d 110 (D. Mass. 2002). The intentional use of confusingly similar domain names, incorporating misspellings and alternative spellings of the plaintiff’s mark, to draw customers away from the plaintiff’s own web site to a critical web site, was bad faith under the ACPA. The use of those domain names was evidence of an intent to “tarnish or damage” the plaintiff’s mark.

Second Circuit

2000

Sporty’s Farm L.L.C. v. Sportsman’s Market Inc., 53 U.S.P.Q.2d 1570 (2d Cir. 2000), *cert. denied*, 120 S. Ct. 2719 (2000). The first appellate ruling on the ACPA has an interesting procedural posture: the ACPA came into existence while the appeal was pending. Arthur Hollander’s company Omega started an aviation catalog in late 1994 or early 1995 and soon thereafter registered the domain name sportys.com with Network Solutions, Inc. (NSI). Nine months later, Omega formed a subsidiary called Sporty’s Farm, and sold it the rights to sportys.com. Sporty’s Farm marketed Christmas trees on the website. Hollander was an aviator who had been receiving aviation equipment catalogs entitled “Sporty’s” from a company called Sportsman’s.

Sportsman’s had registered the trademark sporty’s with the U.S. Patent and Trademark Office (PTO) in 1985. “Sporty’s” is on the cover of all of its catalogs, its toll free phone number is 1-800-Sporty’s, and it spends $10 million annually to advertise the “Sporty’s” logo. In March 1996, Sportsman’s realized that Hollander had registered its trademark as a domain name, and contacted him. Sporty’s Farm quickly instituted a declaratory action to secure its rights to the name. Sportsman’s counterclaimed, and won at the trial court level on a trademark dilution claim. The court issued an injunction requiring Sporty’s Farm to give up the domain name, but ruled that no damages were

available because Omega did not exhibit a willful intent to dilute the Sportsman's trademark.

The Second Circuit asked the parties to brief the applicability of the ACPA. Deciding that the ACPA was applicable, the Second Circuit also found that the elements were present to show that the ACPA had been violated: (1) Sporty's is a "distinctive" mark; (2) the marks Sporty's and sportys.com are "confusingly similar"; and (3) Hollander had a bad faith intent to profit. *Id.* at 1573. The court pointed out that Sporty's Farm did not acquire the domain name from its parent company Omega, or use the website, until after litigation had commenced, the domain name did not contain the name of the company that registered it (Omega), and most importantly, Omega planned to directly compete with Sportsman's. Further, the court accused Hollander and Omega of creating Sporty's Farm only so that it might "keep the name away from Sportsman's." The court was particularly not amused by Hollander's story that he picked the name "Sporty's Farm" from the name of the land that Omega operated on, "Spotty's Farm", which name allegedly came from the name of the childhood dog of Omega's CEO Ralph Michael, "Spotty". The court noted that there was no evidence that Hollander even knew Michael's dog Spotty when Hollander registered the domain name.

Cello Holdings, L.L.C. v. Lawrence-Dahl Companies, 89 F. Supp. 2d 464, 54 U.S.P.Q.2d 1645 (S.D.N.Y. March 30, 2000) Plaintiff Cello had used the "Cello" mark to market high-end stereo systems since 1985, and registered the "Cello" in 1995. In 1997 the defendant registered numerous domain names, including gotmilk.com, stereo.com, and cello.com. The defendant offered to sell cello.com to the plaintiff for $5,000. Cello sued in 1997. Both parties moved for summary judgment. In 1999, the court asked for briefing in view of the *ACPA*, and the *Sporty's* case.

The court found that "Cello" was "famous" only in the limited market of purchasers that spend $20,000-$500,000 for audio equipment. The court also found that "Cello" was widely used as part of registered marks owned by third parties. Because the defendant tried to register "guitar.com," "drums.com," and "violin.com", the court held that it was not clear that he acted with bad faith, although he did intend to profit. Regarding dilution, the court held that Cello's customers "are not likely to be confused." The court denied cross-motions for summary judgment.

2002

Mattel Inc. v. barbie-club.com. A court may obtain in rem jurisdiction over a domain name only in a district in which the domain name registrar or other domain-name authority is located. The 57 domain names that Mattel sued had mostly been registered with domain name registrars located in Maryland, Virginia, and California. Mattel brought its suit in the U.S. District Court for the Southern District of New York, and then sought for "registrar's certificates" for the domain names to be deposited with the district court, hoping by that trick to get in rem jurisdiction in New York over all the 57 names. No such luck.

2003

Storey v. Cello Holdings LLC, 68 USPQ2d 1641 (2nd Cir. 2003) (vacating a judgment that had ordered a re-transfer of the domain name "cello.com" back to Storey, after a UDRP decision had ordered that the domain name “cello.com” be transferred to Cello). "Because a domain-name registrant’s claim under §1114(2)(D)(v) does not involve review of a UDRP decision, the district court’s inquiry should have been on Cello’s right in the Instant Action to contest the lawfulness of Storey’s use of “cello.com” directly under the ACPA."

Third Circuit

2001

Shields v. Zuccarini, 54 U.S.P.Q.2d 1166, 1168 (E.D. Pa. 2000), *affirmed*, 59 U.S.P.Q.2d 1207 (3rd Cir. 2001). Newly-discovered political or moral purposes in creating a website will not suffice to counter a charge of cybersquatting. Plaintiff Joseph Shields creates and sells cartoons that are printed on shirts, and sells other “Joe Cartoon” items that are sold at gift stores. He exhibits and sells his works (such as his “frog blender” and “lemmings competing for diving medals,” which Judge Dalzell refers to as “rather cute”) on his website www.joecartoon.com.

Zuccarini registered the domain sites joescartoon.com, joecarton.com, joescartons.com, joescartoons.com, and cartoonjoe.com, filling them with paid advertisements for credit card companies and other websites. Once litigation ensued, Zuccarini changed the content radically: now web-surfers saw a message extolling the evils of Joe Cartoon. Zuccarini claimed that the sites were registered not in bad faith, but to wage a political protest against Shields’ work because it “desensitizes children to killing animals, [and] makes it seem like great fun and games.” *Id.* at 1168.

Despite Zuccarini’s purported newfound moral indignation, the district court found that he acted with a bad faith intent to profit. The court noted that if Zuccarini was so mortified by Joe Cartoon’s treatment of animals, he probably wouldn’t maintain some of the other domain names that he owns, including www.sexwithanimal.com and www.girlwithanimal.com.

On appeal, the Third Circuit rejected Zuccarini’s contention that registering domain names that are intentional misspellings of distinctive or famous names are not actionable under the ACPA, stating, that a “reasonable interpretation of conduct covered by the phrase ‘confusingly similar’ is the intentional registration of domain names that are misspellings of distinctive or famous names, causing an Internet user who makes a slight spelling or typing error to reach an unintended site.” *Shields*, 59 U.S.P.Q.2d at 1212.

2003

Schmidheiny v. Weber, No. 02-1668 Under the ACPA, a plaintiff may sue to transfer a domain name registration even when it was originally registered prior to the effective date of the statute, if it was re-registered with a new registrar after the law took effect. “[W]e conclude that the language of the statute does not limit the word ‘registration’ to the narrow concept of ‘creation registration’.”

Fourth Circuit

2000

Porsche Cars North America Inc. v. allporsche.com, 215 F.3d. 1320 (4th Cir. 2000). On June 9, 2000, the Fourth Circuit vacated the dismissal of the lower court, in light of the newly-enacted ACPA, and remanded the case to the district court for further proceedings. Some of the defendants might actually have legitimate purposes. What do you think? Here's a partial list:

offering repair - Porscheservice.com
advertising used cars - Usedporsche.com
running enthusiasts' club -Porschephiles.org
selling accessories - Porscheaccessories.com
selling books - Porsche-books.com

On August 23, 2002, the Fourth Circuit vacated part of the new order, and affirmed another part of the new order . ***Porsche Cars North America, Inc. v. Porsche.net***, 302 F.2d 248 (4th Cir. 2002).

Caesars World v. Caesars-Palace.com, 112 F.Supp.2d 502, 54 U.S.P.Q.2d 1121 (E.D. Va. 2000) Plaintiff Caesars World brought an action against domain names containing numerous derivatives of its trademark. Defendants filed a motion to dismiss, contending, *inter alia*, that the in rem provisions of the ACPA are unconstitutional. The court denied the motion, ruling that minimum contacts are necessary for a court to have valid jurisdiction over a defendant only when the underlying cause of action is unrelated to the property which is located in the forum state. Here the property, that is, the domain name, is not only related to the cause of action but is its entire subject matter. Accordingly, it is unnecessary for minimum contacts to meet personal jurisdiction standards.

Lucent Technologies, Inc. v. Lucentsucks.Com, 95 F. Supp. 2d 528, 54 U.S.P.Q.2d 1653 (E.D. Va. 2000). Lucent (a telephone equipment company) notified defendant lucentsucks.com (a porn site) of its intent to sue. Eight days later, Lucent filed an in rem action under the ACPA. The court dismissed the suit, stating that Lucent had not shown due diligence in searching for the defendant. In dicta, the court stated that if the defendant website were parody or critical commentary, the plaintiff's case would be seriously undermined.

2001

Virtual Works, Inc. v. Volkswagen of America, Inc., 238 F.3d 264, 268 (4th Cir.2001) (affirming a judgment requiring plaintiff to give the domain name "vw.net" to Volkswagen). Virtual Works was an Internet service provider unaffiliated with defendant Volkswagen. Virtual Works registered the domain name vw.net with Network Solutions Inc. ("NSI").

For the next two years, Virtual Works used the vw.net domain name in connection with the operation of its ISP business. After aggressive actions by Virtual

Works, Volkswagen responded by invoking NSI's dispute resolution procedure, and challenging Virtual Works' right to the domain name.

Virtual Works then sued for a declaratory judgment confirming its rights to the vw.net domain name. Volkswagen counterclaimed for violation of the ACPA, infringement, and dilution. The district court granted Volkswagen's motion for summary judgment.

The Fourth Circuit affirmed, relying on "(1) the famousness of the VW mark; (2) the similarity of vw.net to the VW mark; [and] (3) the admission that Virtual Works never once did business as VW nor identified itself as such". In addition, the Fourth Circuit ruled that two pieces of evidence showed that Virtual Works had bad faith: 1) "Virtual Works chose vw.net over other domain names not just because 'vw' reflected the company's own initials, but also because it foresaw the ability to profit from the natural association of vw.net and the VW mark", and 2) Virtual Works had threatened to auction the site to the highest bidder if Volkswagen did not elect to purchase it.

People For Ethical Treatment of Animals (PETA) v. Doughney, 263 F.3d 359 (4th Cir. 2001) (finding bad faith intent to profit, even though defendant had done no commercial activity on his website). The Fourth Circuit found that he had "made statements on his website and in the press recommending that PETA attempt to 'settle' with him and 'make him an offer'", and that he had "registered other domain names that [were] identical or similar to the marks or names of other famous people and organizations." *Id*. at 369.

V&S Vin & Sprit Aktiebolag v. Hanson, 60 USPQ2d 1310 (E.D. Va. 2001) (denying Australian defendants' motion to dismiss Swedish corporation's action for infringement of trademark ABSOLUT, cybersquatting, and dilution, on grounds of forum non conveniens grounds, holding that "A trademark holder seeking to enforce its U.S. – registered marks against infringing domain name registrants should not be penalized in the exercise of those rights merely because the parties involved are not United States citizens.").

2002

Harrods Ltd. v. 60 Internet domain names, 302 F.3d 214 (4th Cir. 2002). In rem suits against Internet domain names do not violate due process by permitting suits in which the defendant does not have minimum contacts with the forum. In proving bad faith registration under the anticybersquatting law, the plaintiff's evidence must meet merely the preponderance of the evidence standard, not the higher standard of clear and convincing evidence. The in rem provision applies both to ACPA suits and also to claims of trademark infringement and dilution. *See also* ***Porsche Cars North America, Inc. v. Porsche.net***, 302 F.2d 248 (4th Cir. 2002).

2003

Barcelona.com Inc. v. Excelentisimo Ayuntamiento de Barcelona, 67 U.S.P.Q.2d 1025 (4th Cir. 2003) (reversing the judgment of the district court denying

Bcom, Inc. relief under the ACPA, vacating its memorandum opinion and its order to transfer the domain name "barcelona.com" to the Barcelona City Council, and remanding for further proceedings to grant the appropriate relief under §1114(2)(D)(v)).

The defendant, the city council of Barcelona, Spain (the Ayuntamiento de Barcelona), had brought an action under the UDRP to get the domain name registration for barcelona.com from Joan Nogueras Cobo and his wife, Concepcio Riera Llena, residents of Spain. An administrative arbitration panel of WIPO ordered the transfer of the domain name registration to the city. However, the clever husband and wife team had already formed a corporation under the laws of Delaware, Barcelona.com Inc., and had transferred ownership of the registration to it. Therefore, Barcelona.com Inc. sued in the Eastern District of Virginia, asking for a declaratory judgment that its registration of the domain name was not unlawful.

The district court ordered the transfer of the domain name to the city of Barcelona. The Fourth Circuit reversed and vacated the judgment, stating that the plain text of the ACPA demands application of the U.S. Trademark law, not Spanish law, and that proper application of Spanish law would also have resulted in the husband/wife team keeping their domain name, because the city council could not claim trademark rights to the purely geographical descriptive term “Barcelona”.

"When we apply the Lanham Act, not Spanish law, in determining whether Bcom, Inc.’s registration and use of 'barcelona.com' is unlawful, the ineluctable conclusion follows that Bcom, Inc.’s registration and use of the name 'Barcelona' is not unlawful."

Hawes v. Network Solutions, Inc. and L’Oreal, S.A., 337 F.3d 377 (4th Cir. 2003). In April 1999, Hawes registered the domain name “lorealcomplaints.com” with Network Solutions, Inc. (“NSI”) in Herndon, Virginia, and, as required by NSI, signed a Domain Name Registration Agreement. Sometime after Hawes registered his domain name, L’Oreal sued Hawes in a French court, alleging infringement of L’Oreal’s French trademarks, because of his domain name. Upon learning of this French litigation, NSI transmitted a “Registrar Certificate” for the domain name to counsel for L’Oreal in Paris, tendering control and authority over the registration of the domain name to the French court, in accordance with Network Solutions’ “standard service agreement with its registrants and the dispute policy incorporated therein.”

Hawes failed to appear before the French court, so the court entered judgment in favor of L’Oreal, and ordered the domain name to be transferred to L’Oreal. NSI transferred the name to L’Oreal, so Hawes sued NSI and L’Oreal under the ACPA, asking for a declaration that his use of the domain name was lawful, and asking that it be transferred back to him. The district court dismissed the case on several grounds, including that it possessed discretion under the Declaratory Judgment Act to decline to grant declaratory relief. The Fourth Circuit vacated the dismissal as to L’Oreal, and held that although a district court possesses discretion in deciding whether to grant a declaratory judgment under 28 U.S.C. § 2201, the Declaratory Judgment Act, “a district court possesses no similar discretion in adjudicating an action brought under 15 U.S.C. § 1114(2)(D)(v), in which Congress created a new and independent cause of action

and, unlike in § 2201, used no language indicating that a district court may exercise discretion regarding whether to grant declaratory relief."

E.D. Va.

Globalsantafe Corp. v. globalsantafe.com, No. 01-1541-A, (E.D. Va. 2/5/03). Global Marine Inc. and Santa Fe International Corp. decided in 2001 to merge into a new company Globalsantafe Corp. Less than one day after the announced merger, the Korean domain name registrar, Hangan, registered the domain name globalsantafe.com for Jongsun Park. That domain name was transferred to Fanmore Corp., a Korean entity, with Jong Ha Park listed as the contact.

In October 2001, Global Marine and Santa Fe filed an in rem action against the globalsantafe.com domain name under the ACPA. In November 2001, the companies' merger became effective, and the new Globalsantafe filed a trademark application for GLOBALSANTAFE. The Korean registrar deposited the domain name certificate with the district court, but the registrant failed to appear in court to defend its right to use the domain name.

The court ordered the domain name registry VeriSign to transfer the domain name to Globalsantafe, and later extended that order to the Korean registrar. In September 2002, Park obtained from a court in Korea an injunction barring the Korean registrar from transferring the domain name as ordered by the U.S. district court. Globalsantafe moved for an amended judgment to direct Verisign to cancel the infringing domain name until it is transferred to Globalsantafe.

The court noted that cancellation of a domain name can be achieved by 1) the registrar's cancellation order to the registry, 2) by the registry's disabling of the domain name by placing it on "hold" status, or 3) by the registry's unilateral act of deleting the registration information without the cooperation of the registrar. Verisign's contractual agreements with ICANN and Hangan may not limit Globalsantafe's trademark rights and remedies under the Lanham Act and the ACPA:

> To be sure, it is normally appropriate to direct a cancellation order primarily at the current domain name registrar and to direct that cancellation proceed through the usual channels. However, in situations, where, as here, such an order has proven ineffective at achieving cancellation, it becomes necessary to direct the registry to act unilaterally to carry out the cancellation remedy authorized under the ACPA. In this regard, a court is not limited merely to the disabling procedure envisioned by Verisign's contractual agreements, but may also order the registry to delete completely a domain name registration pursuant to the court's order, just as the registry would in response to a registrar's request. Indeed, in order to vindicate the purposes of the ACPA, disabling alone in many cases may not be sufficient, for it does not oust the cybersquatter from his perch, but rather allows the cybersquatter to remain in possession of the name in violation of the trademark holder's rights.

Because Globalsantafe requested only an amendment of the order to direct Verisign to cancel the domain name by disabling it, the court decided that it did not have to decide whether complete cancellation of the domain name by Verisign was appropriate. The court ordered Verisign not to cancel, but to disable, the domain name by eliminating the domain name IP address from its database.

The court further ruled that there was no basis for abstention on comity grounds because: (1) the U.S. and Korean proceedings were not concurrent; (2) the foreign court proceeding was intended to frustrate the judgment of the U.S. court; and (3) the U.S. judgment supported significant trademark policies under U.S. law.

The court noted "there is a significant gap in the ACPA's trademark enforcement regime for domain names registered under top-level domain names, such as the foreign country code domain names, whose registry is located outside the United States."

E.D. Va.

America Online Inc. v. aol.org, No. 02-1116-A, (E.D. Va. 4/23/03). AOL held the U.S. registrations for the marks AOL and AOL.COM. AOL sued under the in rem provisions of the ACPA. The court issued an order directing the registrar, OnlineNIC, a company based in China, to execute the transfer. However, the registrar instead transferred the registration to another registrar, Netpia.com Inc., based in South Korea. Meanwhile, the registrant had also been changed twice and was now under a presumably fictitious name and controlled by a Korean entity.

AOL then requested an order directing Public Interest Registry to execute the transfer. Public Interest Registry, a Pennsylvania corporation headquartered in Reston, Va., is the operator of the .org registry, a function it took over from Verisign Global Registry Services Inc. at the beginning of the year, under a contract with the ICANN.

Following his prior ruling in the *Globalsantafe* case, Judge Ellis stated, "These jurisdictional provisions weigh strongly against any notion that the transfer and cancellation remedies authorized by the ACPA ... are somehow limited to orders directed at registrar, but not registries. ... Congress deliberately and sensibly provided for jurisdiction where the registry is located so there would be no doubt that courts had the power to direct the registry to carry out the authorized ACPA remedies of transfer and cancellation. ... By choosing to register a domain name in the popular '.org' top-level domain, these foreign registrants deliberately chose to use a top-level domain controlled by a United States registry. ... They chose, in effect, to play Internet ball in American cyberspace." The court issued the transfer order.

2004

Retail Servs., Inc. v. Freebies Pub., Nos. 03-1272 and 03-1317, 2004 WL 771417 (4th Cir. April 13, 2004) (affirming a declaratory judgment of no infringement, and of no cybersquatting). Customer relationship management services company sued a trademark owner seeking a declaration that service company's "freebie.com" domain

name did not constitute infringement or cybersquatting of trademark owner's stylized "Freebies" trademark. The Fourth Circuit looked to the ACPA in analyzing whether a stated cause of action under the ACPA exists if the trademark in question is found to be generic, and thus not capable of trademark protection. In doing so, the Court stated that "a prerequisite for bringing a claim under the ACPA is establishing the existence of a valid trademark and ownership of that mark".

2005

Lamparello v. Jerry Falwell Ministries, No. 04-2011 (4th Cir. August 24, 2005) (reversing a holding of trademark infringement based on the use of a domain name spelled "Fallwell", rejecting the "initial interest confusion" analysis, and following the 5th Circuit to find no cybersquatting because the defendant had no intent to make a profit).

Fifth Circuit

2002

Ernest and Julio Gallo Winery v. Spider Webs Ltd.**,** 286 F.3d 270 (5th Cir. 2002). The plaintiff, Ernest and Julio Gallo Winery, had registered the federal trademark ERNEST & JULIO GALLO in 1964. The defendants—Spider Webs Ltd. and its principals—ran an operation whose business was to "develop" domain names. They registered more than 2,000 names, including about 300 that included trademarks of existing companies, including the domain name ernestandjuliogallo.com. The defendants argued that they were merely holding on to ernestandjuliogallo.com with a plan to sell it should the federal anticybersquatting statute be declared unconstitutional. The Fifth Circuit held that such was evidence of bad faith.

2004

TMI Inc. v. Maxwell, 70 USPQ2d 1630 (5th Cir. 2004) (reversing and rendering a judgment of $40,000 in statutory damages, and $40,000 in attorneys fees). Maxwell, an unhappy home-buyer, registered "trendmakerhome.com", and used the website as a gripe site. He also included on the website a place called a "Treasure Chest" for readers to share and obtain information about contractors and tradespeople who had done good work, and admitted that he had added that section to attract people to read his gripes about TMI. During the year of the site's existence, the Treasure Chest only contained one name, that of a man who had performed some work for Maxwell. The site did not contain any paid advertisements. The Fifth Circuit ruled that although some e-mail intended for TMI was sent to Maxwell's site, because did not charge money for viewing the Treasure Chest portion of his site, and had no advertising or links to other sites, his site was not "commercial", and thus there was no liability under the ACPA nor under the dilution statutes. In a footnote, the Fifth Circuit incorrectly distinguished a contrary holding on the issue of "commercial use" of trademarks in *United We Stand America, Inc. v. United We Stand, America New York, Inc.*, 128 F.3d 86, 89-90 [44 USPQ2d 1351] (2d Cir. 1997), stating that such case did not "involve either the anti-

dilution provision or ACPA and is, thus, irrelevant to the determination of whether these two sections require commercial use".

Sixth Circuit

2003

Ford Motor Company v. Catalanotte, 342 F.3d 543, 68 U.S.P.Q.2d 1050 (6th Cir. 2003) (affirming an award of $5,000 and injunctive relief under the ACPA). Catalanotte, a Ford employee since 1978, registered "fordworld.com" in 1997, and three years later offered to sell it to Ford. Catalanotte's lawyer argued that because Catalanotte registered the domain name before the date of enactment of the ACPA (November 29, 1999), the district court incorrectly awarded damages to Ford. However, the Sixth Circuit found that because Catalanotte offered to sell the domain name to Ford after November 29, 1999, such offer was "trafficking in" the domain name after the enactment date, and thus the district court correctly awarded damages.

2004

In ***Lucas Nursery and Landscaping v. Michelle Grosse*** (March 5, 2004), the Sixth Circuit affirmed a grant of summary judgment to Grosse, who had started a website www.lucasnursery.com to complain about the plaintiff. The Sixth Circuit expressly refused to consider "whether the ACPA covers non-commercial activity", focusing instead on whether there was "bad faith intent to profit", even though the statutory "bad faith" factors 4 and 5 clearly refer to commercial activity:

> 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

(emphasis added) However, the Sixth Circuit did say, "The fourth factor cuts in Grosse's favor because the site was used for noncommercial purposes." Also, the court pointed out that the nursery did not have a website.

In conclusion, the Sixth Circuit stated:

> Although Grosse's actions would arguably satisfy three of the four aforementioned factors, she does not fall within the factor that we consider central to a finding of bad faith. **She did not register multiple web sites; she only registered one.** Further, it is not clear to this Court that the presence of simply one factor that indicates a bad faith intent to profit, without more, can satisfy an imposition of liability within the meaning of the **ACPA.** The role of the

reviewing court is not simply to add factors and place them in particular categories, without making some sense of what motivates the conduct at issue. The factors are given to courts as a guide, not as a substitute for careful thinking about whether the conduct at issue is motivated by a bad faith intent to profit. Perhaps most important to our conclusion are, Grosse's actions, which seem to have been undertaken in the spirit of informing fellow consumers about the practices of a landscaping company that she believed had performed inferior work on her yard. One of the **ACPA's** main objectives is the protection of consumers from slick internet peddlers who trade on the names and reputations of established brands. The practice of informing fellow consumers of one's experience with a particular service provider is surely not inconsistent with this ideal (emphasis added).

Seventh Circuit

2002

Ty Inc. v. Perryman, 306 F.3d 509, 64 U.S.P.Q.2d 1689 (7th Cir. 2002) (vacating a summary judgment and injunction against the defendant, and remanding). Ms. Ruth Perryman operated a website www.bargainbeanies.com where she sold "second-hand beanbag stuffed animals, primarily but not exclusively Ty's Beanie Babies." The Seventh Circuit held that there was no dilution, and no violation of the ACPA, but that there could be confusion by Perryman's calling other plush toys "other beanies", stating that such was a "misdescription, in fact false advertising, and supports the last prohibition in the injunction, the prohibition against using 'Beanie' or 'Beanies' 'in connection with any non-Ty products.'"

Eighth Circuit

2004

Coca-Cola Co. v. Purdy, Nos. 02-2894 etc. (8th Cir. 9/1/04) (affirming preliminary injunctions and dismissing appeals of a contempt order and sanctions, for lack
of jurisdiction). Purdy, a pro-life advocate, registered domain names such as drinkcoke.org, mycoca-cola.com, mymcdonalds.com, mypepsi.org, and my-washingtonpost.com. Purdy linked the domain names to abortionismurder.com. He also linked my-washingtonpost.com to a Web site that mimicked the appearance of the actual washingtonpost.com Web site. The site displayed statements such as "The Washington Post proclaims 'Abortion is Murder' " and "Things Don't Always Go Better With Coke. Abortion is Murder -- 'The Real Thing' ", as well as images of aborted fetuses and links to Purdy's anti-abortion Web site.

After receiving requests to stop from the trademark owners, Purdy offered to give up the my-washingtonpost.com domain name if the Washington Post would publish one of Purdy's writings on its editorial page. He then registered more domain names, and began using the E-mail address dontkillyourbaby@washingtonpost.cc. Despite a court

order forbidding him to use those domain names, and ordering him to transfer those names to the trademark owners, Purdy registered a further 60 domain names. The judge found Purdy in contempt. The court issued a second order prohibiting Purdy from using the names in question, and ordering him to transfer the domain name registrations. Purdy then registered more domain names, and the court issued a supplemental contempt order imposing fines.

As is usual in these cases, Purdy argued that there was no evidence that he had the requisite bad faith intent to profit. The 8th Circuit considered the nine statutory factors regarding a defendant's alleged bad faith intent to profit. In so doing, the Court stated:

> "The fact that confusion about a website's source or sponsorship could be resolved by visiting the website is not relevant to whether the domain name itself is identical or confusingly similar to a plaintiff's mark. . . . Moreover, the record indicates that Purdy intended to capitalize on the similarity between his domain names and plaintiffs' marks to attract unwitting Internet users to antiabortion websites. . . .
>
> Furthermore, the record shows that just days after Purdy began registering and using the domain names at issue in this case, he apparently offered to stop using the Washington Post domain names in exchange for space on the editorial page in that newspaper. A proposal to exchange domain names for valuable consideration is not insignificant in respect to the issue of bad faith intent to profit.

The 8th Circuit distinguished *Lucas Nursery* and *TMI*, stating that "[n]either customer in those cases had registered multiple infringing domain names or offered to transfer the names in exchange for valuable consideration. Neither had linked the names to websites about issues other than the company's business or to websites that solicited donations or sold merchandise."

Purdy argued that the First Amendment entitled him to use the domain names at issue to attract Internet users to websites containing political expression and criticism of the plaintiffs. The Court held, "While Purdy has the right to express his message over the Internet, he has not shown that the First Amendment protects his appropriation of plaintiffs' marks in order to spread his protest message by confusing Internet users into thinking that they are entering one of the plaintiffs' websites."

Ninth Circuit

2002

Nissan Motor Co. v. Nissan Computer Corp., 204 F.R.D. 460 (C.D. Cal. 2001); (original case: 89 F. Supp. 2d 1154 (C.D. Cal. 2000), *aff'd*, 246 F.3d 675 (9th Cir. 2002)). The purchase of search engine keywords ("Nissan" and "Nissan.com" from search engine operators) that are identical to Internet domain names registered by

another party does not violate any trademark-related rights belonging to the domain name registrant.

C.D. Cal.

Nissan Motor Co. v. Nissan Computer Corp. Nissan Computer obtained the Internet domain names nissan.com and nissan.net. Nissan Motor sued Nissan Computer in 1999 for trademark infringement, dilution, and cybersquatting. Nissan Computer Corp. is a North Carolina company, incorporated in 1991 by its president, Uzi Nissan, to sell and service computers.

In March, 2000, the court rejected Nissan Computer's motion to dismiss for lack of personal jurisdiction, and granted Nissan Motor's motion for a preliminary injunction. In March, 2002, the court issued a partial summary judgment for Nissan Motor on its claims of infringement and cybersquatting. *Nissan Motor Co. v. Nissan Computer Corp.,* 180 F.Supp. 2d 1089, 61 U.S.P.Q.2d 1839 (C.D. Cal. 2002).

The court quoted *Mattel Inc. v. MCA Records Inc.*, 296 F.3d 894, 63 U.S.P.Q.2d 1715 (9th Cir. 2002), stating that the FTDA is not intended to prohibit or threaten "noncommercial expression, such as parody, satire, editorial and other forms of expression that are not a part of a commercial transaction." However, the court held that the noncommercial exemption does not apply to critical commentary when the goodwill represented by the trademark is exploited to injure the trademark owner. Thus, the court granted Nissan Motor's motion for a permanent injunction, but limited the injuction to merely barring Mr. Uzi Nissan from using his websites nissan.com and nissan.net for commercial purposes, including any disparaging remarks or negative commentary about Nissan Motors.

2003

Kremen v. Cohen, Network Solutions Inc., et al., No. 01-15899 (9th Cir. 7/25/03). Kremen registered the domain name sex.com in 1994 without a written contract, and without having to pay anything for it. "Con man Stephen Cohen, meanwhile, was doing time for impersonating a bankruptcy lawyer. He, too, saw the potential of the domain name. Kremen had gotten it first, but that was only a minor impediment for a man of Cohen's boundless resource and bounded integrity."

Stephen Cohen sent a forged letter to NSI that he claimed he received from Online Classifieds, Kremen's company, informing Cohen that Online Classifieds had fired Kremen, was no longer interested in the domain name, and consented to its transfer to Cohen. NSI accepted the letter as valid and transferred the domain name to Cohen. When Kremen complained, NSI told him it was too late to undue the transaction. Cohen went on to turn sex.com into a lucrative online porn empire. Kremen sued Cohen, and received a judgment of $65 million. Cohen ignored the judgment, wired his money overseas, and went to Mexico to escape an arrest warrant.

> "Then things started getting really bizarre. Kremen put up a 'wanted' poster on the sex.com site with a mug shot of Cohen, offering a $50,000 reward

> to anyone who brought him to justice. Cohen's lawyers responded with a motion to vacate the arrest warrant. They reported that Cohen was under house arrest in Mexico and that gunfights between Mexican authorities and would-be bounty hunters seeking Kremen's reward money posed a threat to human life. The district court rejected this story as 'implausible' and denied the motion. Cohen, so far as the record shows, remains at large."

Unable to reach Cohen, Kremen sued NSI for breach of contract, breach of third party contract, and conversion. The district court granted summary judgment in favor of Network Solutions on all claims. *Kremen v. Cohen*, 99 F. Supp. 2d 1168 (N.D. Cal. 2000). The Ninth Circuit affirmed no breach of contract, and no breach of a third party contract with the National Science Foundation. However, the Ninth Circuit disagreed with the district court's holding that intangible property was not subject to conversion, and instead held that "Kremen's domain name is protected by California conversion law", and remanded the case.

2005

Bosley Medical Institute Inc. v. Kremer, 74 U.S.P.Q.2d 1280, 1282 (9th Cir. 2005). The Ninth Circuit at first appeared to rule again in favor of "First Amendment" cybersquatters when it stated: (it's a long quote, but the puns are worth it)

> Defendant Michael Kremer was dissatisfied with the hair restoration services provided to him by the Bosley Medical Institute, Inc. In a bald-faced effort to get even, Kremer started a website at www.BosleyMedical.com, which, to put it mildly, was uncomplimentary of the Bosley Medical Institute. The problem is that "Bosley Medical" is the registered trademark of the Bosley Medical Institute, Inc., which brought suit against Kremer for trademark infringement and like claims. Kremer argues that noncommercial use of the mark is not actionable as infringement under the Lanham Act. Bosley responds that Kremer is splitting hairs.
>
> Like the district court, we agree with Kremer. We hold today that the noncommercial use of a trademark as the domain name of a website — the subject of which is consumer commentary about the products and services represented by the mark — does not constitute infringement under the Lanham Act.

Fortunately for trademark owners, the Ninth Circuit then held that such use **could** violate the ACPA, and followed the Eighth Circuit to correct the prior faulty thinking by the Fifth and Sixth Circuits:

> The ACPA makes it clear that "use" is only one possible way to violate the Act ("registers, traffics in, or uses"). Allowing a cybersquatter to register the domain name with a bad faith intent to profit but get around the law by making noncommercial use of the mark would run counter to the purpose of the Act. "[T]he use of a domain name in connection with a site that makes a

noncommercial or fair use of the mark does not necessarily mean that the domain name registrant lacked bad faith."

72 U.S.P.Q.2d at 1287, quoting from *Coca-Cola Co. v. Purdy*, 382 F.3d 774, 778 , 72 U.S.P.Q.2d 1305 (8th Cir. 2004).

2006

Pebble Beach Company v. Caddy, No. 04-15577 (9th Circuit, July 12, 2006).

The Ninth Circuit, in a trademark infringement suit brought by the operator of the Pebble Beach golf resort, refused to take personal jurisdiction over a British bed and breakfast that used the term "Pebble Beach" in its passive website advertising and in its domain name. The Court held that these were not acts aimed at the state of California. In so ruling, the Court clarified the Calder "effects test" for personal jurisdiction, holding that expressly aiming at the forum state was required. For similar reasons, the Court also held that the defendant's acts were insufficient to subject him to personal jurisdiction under the federal long-arm rule. The Court noted that although the bed and breakfast operator had formerly lived in California and was familiar with the golf resort, he was not a cybersquatter trying to obtain money from the resort's operator, and did not write a letter to force the resort operator to act.

4. International Arbitration Panels For Domain Name Disputes

First, a few definitions, which you can find at various places, including http://en.wikipedia.org/wiki/Main_Page, and at http://gnso.icann.org/drafts/pdp-dec05-draft-fr.htm#glosdef.

Domain Name System	On the Internet, the **domain name system** (**DNS**) stores and associates many types of information with domain names; most importantly, it translates domain names (computer hostnames) to IP addresses. It also lists mail exchange servers accepting e-mail for each domain. In providing a worldwide keyword-based redirection service, DNS is an essential component of contemporary Internet use.
Root server	A **root nameserver** is a DNS server that answers requests for the root namespace domain, and redirects requests for a particular top-level domain to that TLD's nameservers. Although any local implementation of DNS can implement its own private root nameservers, the term "root nameserver" is generally used to describe the thirteen well-known root nameservers that implement the root namespace domain for the Internet's official global implementation of the Domain Name System. (Most of these are in the United States.) All domain names on the Internet can be regarded as ending in a full stop character e.g. "en.wikipedia.org.". This final dot is

	generally implied rather than explicit, as modern DNS software does not actually require that the final dot be included when attempting to translate a domain name to an IP address. The empty string after the final dot is called the root domain, and all other domains (i.e. .com, .org, .net, etc.) are contained within the root domain. http://en.wikipedia.org/wiki/Root_server
ICANN	The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. ICANN is responsible for coordinating the management of the technical elements of the DNS to ensure universal resolvability so that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique technical identifiers used in the Internet's operations, and delegation of Top-Level Domain names (such as .com, .info, etc.). Other issues of concern to Internet users, such as the rules for financial transactions, Internet content control, unsolicited commercial email (spam), and data protection are outside the range of ICANN's mission of technical coordination. Ensuring predictable results from any place on the Internet is called "universal resolvability." It is a critical design feature of the Domain Name System, one that makes the Internet the helpful, global resource that it is today. Without it, the same domain name might map to different Internet locations under different circumstances, which would only cause confusion.
The Generic Names Supporting Organization (GNSO) of ICANN	The successor to the responsibilities of the Domain Name Supporting Organization that relate to the generic top-level domains. ICANN's by-laws outline three supporting organizations, of which the GNSO belongs. The SOs help to promote the development of Internet policy and encourage diverse and international participation in the technical management of the Internet. Each SO names three Directors to the ICANN Board.

From ICANN’s website comes the following:

ICANN Welcomes Participation

Participation in ICANN is open to all who have an interest in global Internet policy as it relates to ICANN's mission of technical coordination. ICANN provides many online forums which are accessible through ICANN's website, and the Supporting Organizations and Advisory Committees have active mailing lists for participants. Additionally, ICANN holds public meetings throughout the year. Recent meetings have been held in Bucharest, Montreal, Shanghai, Rio de Janeiro, and Accra. For more information on the Supporting Organizations and Advisory Committees, please refer to their websites:

Address Supporting Organization (ASO) - www.aso.icann.org

Country Code Domain Name Supporting Organization (CCNSO) - www.ccnso.icann.org

Generic Names Supporting Organization (GNSO) - www.gnso.icann.org

At-Large Advisory Committee - www.alac.icann.org

Governmental Advisory Committee - www.gac.icann.org

More information on ICANN can be found on ICANN's website: http://www.icann.org

As of March, 2007, here are the existing top level domain names:

TLD	Introduced	Sponsored/ Unsponsored	Purpose	Sponsor/ Operator
.aero	2001	Sponsored	Air-transport industry	Societe Internationale de Telecommunications Aeronautiques SC, (SITA)
.biz	2001	Unsponsored	Businesses	NeuLevel
.cat	2005	Sponsored	Catalan linguistic & cultural community	Fundació puntCAT
.com	1995	Unsponsored	Unrestricted (but intended for commercial registrants)	VeriSign, Inc.
.coop	2001	Sponsored	Cooperatives	DotCooperation,

				LLC
.edu	1995	Sponsored	United States educational institutions	EDUCAUSE
.gov	1995	Sponsored	United States government	US General Services Administration
.info	2001	Unsponsored	Unrestricted use	Afilias Limited
.int	1998	Unsponsored	Organizations established by international treaties between governments	Internet Assigned Numbers Authority
.jobs	2005	Sponsored	International community of human resource managers	Employ Media LLC
.mil	1995	Sponsored	United States military	US DoD Network Information Center
.mobi	2005	Sponsored	Mobile content providers and users community	mTLD Top Level Domain, LTD.
.museum	2001	Sponsored	Museums	Museum Domain Management Association, (MuseDoma)
.name	2001	Unsponsored	For registration by individuals	Global Name Registry, LTD
.net	1995	Unsponsored	Unrestricted (but intended for network providers, etc.)	VeriSign, Inc.
.org	1995	Unsponsored	Unrestricted (but intended	Public Interest Registry. Until 31

			for organizations that do not fit elsewhere)	December 2002, .org was operated by VeriSign Global Registry Services.
.pro	2002	Unsponsored	Accountants, lawyers, physicians, and other professionals	RegistryPro, LTD
.tel	2006	Sponsored		Telnic Ltd.
.travel	2005	Sponsored	Travel and tourism community	Tralliance Corporation

In 2005-2006, four new TLDs (.cat, .jobs, .mobi, and .travel) were launched. ICANN's GNSO is currently developing policy recommendations for introduction of additional gTLDs. We will continue to see new top level domain names, because the GNSO website states the following:

Principle 1	New generic top-level domains (gTLDs) must be introduced in an orderly, timely and predictable way.
Principle 2	Some new generic top-level domains may be internationalised domain names (IDNs) subject to the approval of IDNs being available in the root.
Principle 3	The reasons for introducing new top-level domains include that there is demand from potential applicants for new top-level domains in both ASCII and IDN formats and that the new TLD process promotes competition, consumer choice and geographical and service-provider diversity.

In addition to the continuing increase in generic TLD's, there are also several hundred country codes that serve as TLD's.

ac – Ascension Island	.ad – Andorra	.ae – United Arab Emirates
.af – Afghanistan	.ag – Antigua and Barbuda	.ai – Anguilla
.al – Albania	.am – Armenia	.an – Netherlands Antilles
.ao – Angola	.aq – Antarctica	.ar – Argentina
.as – American Samoa	.at – Austria	.au – Australia
.aw – Aruba	.ax – Aland Islands	.az – Azerbaijan
.ba – Bosnia and Herzegovina	.bb – Barbados	.bd – Bangladesh
.be – Belgium	.bf – Burkina Faso	.bg – Bulgaria

.bh – Bahrain	.bi – Burundi	.bj – Benin
.bm – Bermuda	.bn – Brunei Darussalam	.bo – Bolivia
.br – Brazil	.bs – Bahamas	.bt – Bhutan
.bv – Bouvet Island	.bw – Botswana	.by – Belarus
.bz – Belize	.ca – Canada	.cc – Cocos (Keeling) Islands
.cd – Congo, The Democratic Republic of the	.cf – Central African Republic	.cg – Congo, Republic of
.ch – Switzerland	.ci – Cote d'Ivoire	.ck – Cook Islands
.cl – Chile	.cm – Cameroon	.cn – China
.co – Colombia	.cr – Costa Rica	.cu – Cuba
.cv – Cape Verde	.cx – Christmas Island	.cy – Cyprus
.cz – Czech Republic	.de – Germany	.dj – Djibouti
.dk – Denmark	.dm – Dominica	.do – Dominican Republic
.dz – Algeria	.ec – Ecuador	.ee – Estonia
.eg – Egypt	.eh – Western Sahara	.er – Eritrea
.es – Spain	.et – Ethiopia	.eu – European Union
.fi – Finland	.fj – Fiji	.fk – Falkland Islands (Malvinas)
.fm – Micronesia, Federated States of	.fo – Faroe Islands	.fr – France
.ga – Gabon	.gb – United Kingdom	.gd – Grenada
.ge – Georgia	.gf – French Guiana	.gg – Guernsey
.gh – Ghana	.gi – Gibraltar	.gl – Greenland
.gm – Gambia	.gn – Guinea	.gp – Guadeloupe
.gq – Equatorial Guinea	.gr – Greece	.gs – South Georgia and the South Sandwich Islands
.gt – Guatemala	.gu – Guam	.gw – Guinea-Bissau
.gy – Guyana	.hk – Hong Kong	.hm – Heard and McDonald Islands
.hn – Honduras	.hr – Croatia/Hrvatska	.ht – Haiti
.hu – Hungary	.id – Indonesia	.ie – Ireland
.il – Israel	.im – Isle of Man	.in – India
.io – British Indian Ocean Territory	.iq – Iraq	.ir – Iran, Islamic Republic of
.is – Iceland	.it – Italy	.je – Jersey
.jm – Jamaica	.jo – Jordan	.jp – Japan
.ke – Kenya	.kg – Kyrgyzstan	.kh – Cambodia
.ki – Kiribati	.km – Comoros	.kn – Saint Kitts and Nevis
.kp – Korea, Democratic People's Republic	.kr – Korea, Republic of	.kw – Kuwait
.ky – Cayman Islands	.kz – Kazakhstan	.la – Lao People's Democratic Republic
.lb – Lebanon	.lc – Saint Lucia	.li – Liechtenstein
.lk – Sri Lanka	.lr – Liberia	.ls – Lesotho

.lt – Lithuania	.lu – Luxembourg	.lv – Latvia
.ly – Libyan Arab Jamahiriya	.ma – Morocco	.mc – Monaco
.md – Moldova, Republic of	.me – Montenegro	.mg – Madagascar
.mh – Marshall Islands	.mk – Macedonia, The Former Yugoslav Republic of	.ml – Mali
.mm – Myanmar	.mn – Mongolia	.mo – Macao
.mp – Northern Mariana Islands	.mq – Martinique	.mr – Mauritania
.ms – Montserrat	.mt – Malta	.mu – Mauritius
.mv – Maldives	.mw – Malawi	.mx – Mexico
.my – Malaysia	.mz – Mozambique	.na – Namibia
.nc – New Caledonia	.ne – Niger	.nf – Norfolk Island
.ng – Nigeria	.ni – Nicaragua	.nl – Netherlands
.no – Norway	.np – Nepal	.nr – Nauru
.nu – Niue	.nz – New Zealand	.om – Oman
.pa – Panama	.pe – Peru	.pf – French Polynesia
.pg – Papua New Guinea	.ph – Philippines	.pk – Pakistan
.pl – Poland	.pm – Saint Pierre and Miquelon	.pn – Pitcairn Island
.pr – Puerto Rico	.ps – Palestinian Territory, Occupied	.pt – Portugal
.pw – Palau	.py – Paraguay	.qa – Qatar
.re – Reunion Island	.ro – Romania	.rs – Serbia
.ru – Russian Federation	.rw – Rwanda	.sa – Saudi Arabia
.sb – Solomon Islands	.sc – Seychelles	.sd – Sudan
.se – Sweden	.sg – Singapore	.sh – Saint Helena
.si – Slovenia	.sj – Svalbard and Jan Mayen Islands	.sk – Slovak Republic
.sl – Sierra Leone	.sm – San Marino	.sn – Senegal
.so – Somalia	.sr – Suriname	.st – Sao Tome and Principe
.su – Soviet Union (being phased out)	.sv – El Salvador	.sy – Syrian Arab Republic
.sz – Swaziland	.tc – Turks and Caicos Islands	.td – Chad
.tf – French Southern Territories	.tg – Togo	.th – Thailand
.tj – Tajikistan	.tk – Tokelau	.tl – Timor-Leste
.tm – Turkmenistan	.tn – Tunisia	.to – Tonga
.tp – East Timor	.tr – Turkey	.tt – Trinidad and Tobago
.tv – Tuvalu	.tw – Taiwan	.tz – Tanzania
.ua – Ukraine	.ug – Uganda	.uk – United Kingdom

.um – United States Minor Outlying Islands	.us – United States	.uy – Uruguay
.uz – Uzbekistan	.va – Holy See (Vatican City State)	.vc – Saint Vincent and the Grenadines
.ve – Venezuela	.vg – Virgin Islands, British	.vi – Virgin Islands, U.S.
.vn – Vietnam	.vu – Vanuatu	.wf – Wallis and Futuna Islands
.ws – Samoa	.ye – Yemen	.yt – Mayotte
.yu – Yugoslavia	.za – South Africa	.zm – Zambia
.zw – Zimbabwe		

1. ICANN'S Domain Name Dispute Resolution Policy

According to ICANN's website in March 2007, "ICANN implemented a Uniform Domain Name Dispute Resolution Policy (UDRP), which has been used to resolve more than 5000 disputes over the rights to domain names. The UDRP is designed to be efficient and cost effective." Also, "The Uniform Domain-Name Dispute Resolution Policy (UDRP) has been adopted by ICANN-accredited registrars in all gTLDs (.aero, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel and .travel). Dispute proceedings arising from alleged abusive registrations of domain names (for example, cybersquatting) may be initiated by a holder of trademark rights. The UDRP is a policy between a registrar and its customer and is included in registration agreements for all ICANN-accredited registrars."

You can find the UDRP at http://www.icann.org/udrp/. The UDRP requires the aggrieved party to show: 1) the domain name is identical or confusingly similar to the aggrieved party's mark; 2) the domain name holder has no legitimate rights or interests; and 3) bad faith on the part of the domain name holder.

ICANN has three approved arbitration organizations. From the ICANN website comes the following:

> Complaints under the Uniform Dispute Resolution Policy may be submitted to any approved dispute-resolution service provider listed below. Each provider follows the Rules for Uniform Domain Name Dispute Resolution Policy as well as its own supplemental rules. To go to the web site of a provider, click on its name below:
>
> - Asian Domain Name Dispute Resolution Centre [ADNDRC] (approved effective 28 February 2002). It has three offices:
>   - Beijing click here to see its supplemental rules.
>   - Hong Kong click here to see its supplemental rules.
>   - Seoul click here to see its supplemental rules.
> - The National Arbitration Forum [NAF] (approved effective 23 December 1999). Click here to see its supplemental rules.
> - World Intellectual Property Organization [WIPO] (approved effective 1 December 1999). Click here to see its supplemental rules.

Also from the WIPO website comes this explanation of what resolution the litigants can expect to receive:

A domain name is either **cancelled**, **transferred**, or **sustained** (i.e., the complaint is denied and the respondent keeps the domain name). Some examples of cases that received significant media attention include juliaroberts.com and jimihendrix.com, which were transferred to the individuals or their families. A complaint involving sting.com, filed by the singer known as Sting, was denied for a variety of reasons, principally that the domain name registrant was also known by the same nickname, as well as the fact that the name is a common word in the English language and is not necessarily an exclusive trademark.

There are no monetary damages applied in UDRP domain name disputes, and no injunctive relief is available. The accredited domain name registrars - which have agreed to abide by the UDRP - implement a decision after a period of ten days, unless the decision is appealed in that time.

The resolutions offered by WIPO are mandatory in the sense that accredited registrars are bound to take the necessary steps to enforce a decision, such as transferring the name concerned. **However, under the UDRP, either party retains the option to take the dispute to a court of competent jurisdiction for independent resolution.** (emphasis added)

The list of country code top-level domains that have agreements with ICANN can be found at: http://www.icann.org/cctlds/agreements.html. Unfortunately, in 2007 the number was less than thirty.

The following cases involve a few instances where either the UDRP litigants have ended up in U.S. courts, or the litigants names seemed interesting enough to this author to include in this brief history.

Third Circuit

2003

Dluhos v. Strasberg, 321 F.3d 365 (3d Cir. 2003). UDRP Arbitrations are not arbitrations within the meaning of the Federal Arbitration Act. Therefore, UDRP determinations are not entitled to deferential judicial review. The ACPA, 15 U.S.C. §1114(2)(D)(v), provides registrants with an affirmative cause of action to recover domain names lost in UDRP proceedings. The statute provides that a registrant whose domain name has been "suspended, disabled, or transferred" may sue for a declaration that the registration does not violate the ACPA, as well as for an order to return the domain name.

Fourth Circuit

2001
E.D. Va.

Parisi v. Netlearning Inc., 59 USPQ2d 1051 (E.D. Va. 2001) (denying defendant Netlearning's motion to dismiss a declaratory judgment action of non-infringement). Following a UDRP panel ruling against the plaintiff Parisi, the Virginia District Court held that the Federal Arbitration Act's (9 U.S.C. §1 et seq.) restrictions on judicial review of arbitration awards do not apply to civil actions challenging UDRP panel decisions.

WIPO Arbitration Panel

2000

Roberts v. Boyd, WIPO Administrative Panel Decision, Case No. D2000-0210, May 29, 2000. An early case involving the UDRP involves an alleged "fan" of Julia Roberts, a man named Russell Boyd, who registered the URL juliaroberts.com in 1998. Boyd listed the domain name for sale with Web auctioneer Ebay.com, and received and rejected a $2,500 bid. On March 25, 2000, the lawyers for Julia Roberts filed a complaint with WIPO. A WIPO arbitration panel heard the case, mostly via email. About two months later, on May 29, 2000, the panel issued its decision. Boyd had argued that he was "merely operating a fan site". The panel found that the site became a "fan site" only after Julia filed her complaint. Therefore, the panel found the requisite "bad faith". The panel also found that the "Julia Roberts" name has secondary meaning. The panel ordered Boyd to transfer the domain name to Julia.

However, Boyd sued her within ten days of the panel's decision. Thus, under the UDRP, precluding ICANN from canceling his web site that used her name. His website continued to exist for a brief period of time after he sued Julia. At that website, he was pleading with Julia to call off her lawyers, claiming that he was merely her fan. However, his web site no longer exists.

2003

Pierce Brosnan v. Network Operations Center, WIPO Administrative Panel Decision, Case No. D2003-0519, August 27, 2003. The Respondent registered the domain name piercebrosnan.com, and redirected it to the website "www.celebrity1000.com". Network Operations Center is a pseudonym for the infamous cybersquatter Jeff Burgar. Burgar, doing business as "Alberta Hot Rods" and the "Stefanie Seymour Club", has engaged in a practice of registering domain names (about 75 of them) comprised of celebrities' names. In a prior UDRP proceeding against Mr. Burgar, the panel noted, "it has been clearly demonstrated, partly through Respondent's admissions, that he obtained a succession of celebrity.com domain names and this gives rise to an evident pattern of conduct in which he stockpiled similar registrations." *Celine Dion v. Jeff Burgar*, WIPO Case No. D2000-1838 (February 13, 2001) at 3.

Multiple proceedings under the UDRP have been successfully prosecuted against Burgar by celebrities who have obtained transfer or cancellation of domain names registered and used in bad faith by Burgar, including proceedings involving Kevin Spacey, Michael Andretti, Stephanie Seymour, and Dr. Michael Crichton.

The WIPO Arbitration and Mediation Center (the "Center") appointed Dawn Osborne as the sole panelist for this matter on August 13, 2003. Burgar did not respond to Pierce Brosnan's complaint. Ms. Osborne ordered the domain name transferred to Mr. Brosnan. On September 8, 2003, the website www.piercebrosnan.com was still directed to Burgar's website www.celebrity1000.com.

5. The European Union's Domain Name Dispute Resolution Policy

I The European Commission selected EURid to operate the .eu top level domain. EURid is a not-for-profit organization, established in Belgium. EURid was established in a partnership between the operators of the country-code top level domain registries for Belgium (.be), Italy (.it) and Sweden (.se). Later the registry for .si (Slovenia) and .cz (Czech Republic) joined as members. EURid has its headquarters in Diegem, Belgium and a regional office in Stockholm, and is in the process of setting up regional offices in Prague and Italy to support four geographical regions to provide support in local languages for .eu registrars and registrants in the European Union. The EURid website is http://www.eurid.eu/ .In March, 2007, there were several hundred accredited registrars for the .eu domain, including about 200 in the U.S., but only one was in Houston. About 150 of those listed as being in the United States were located in either Oregon or Washington. What's with that??

EURid offers an Alternative Dispute Resolution (ADR) for resolving disputes about .eu domain names. The ADR is facilitated by the Prague-based Arbitration Court in the Czech Republic. It administers ADR Proceedings in line with the Public Policy Rules for .eu of the European Commission (EC Regulation 874/2004). On the website of the Czech arbitration Court (www.adr.eu) you will find the ADR rules, fees and all other relevant information. ADR proceedings are carried out in the language selected by the holder of the disputed domain name.

In 2007, one of my clients received an email from a cybersquatter, who had a domain name ending in .eu, using one of my client's famous marks. Because the TLD was .eu, we could not use the UDRP of ICANN; we had to arbitrate under the ADR rules, and the first big issue was "In what language will the arbitration be?" The ADR rules require that if you are not happy with the language that the cybersquatter selected when he registered your trademark as a domain name, then before you file your complaint, you must first file a request to change the language to be the language that you desire. That request initiates a "Language Trial".

6. Fighting Overly-Aggressive Attempts to Cancel Domain Names

In January, 2001, the WIPO labeled at least two overly aggressive attempts to cancel domain names as "reverse domain name hijacking". Unfortunately, the UDRP

has no provisions to compensate rightful owners for their costs in defending against reverse domain name hijacking.

WIPO Arbitration Panel

2001

Deutsche Welle v. Diamondware Ltd. WIPO Administrative Panel Decision, Panelists Willoughby, Bettinger, and Cabell, Case No. D 2000-1202, January 2, 2001. In July, 2000, Deutsche Welle (a radio & TV broadcaster) sued Diamondware Ltd. (software developer) under the UDRP to cancel the registration of dw.com, which the Arizonians had registered in 1994. On January 2, 2001, WIPO refused to cancel the domain name registration, calling the Germans' actions "reverse domain name hijacking".

Goldline Int'l v.Gold Line, WIPO Administrative Panel Decision, Panelists Bernstein, Kelly, and Limbury, Case No. D2000-1151, January 4, 2001. Goldline Int'l (a coin dealer) sued Gold Line (provider of Internet community services) under the UDRP to cancel goldline.com, which Gold Line had registered in 1997. Gold Line had even added a disclaimer to its website after the coin dealer griped. On January 4, 2001, WIPO refused to cancel the domain name registration, calling the coin dealer's actions "reverse domain name hijacking".

Loren Stocker, Managing Director for Del Mar Internet noted, "Egregious behavior like that of Goldline International goes unpunished thanks to a flawed ICANN policy. Am I now to defend myself against the 40 other trademark holders?"

G.A. Modafine S.A. v. Mani.Com, WIPO Administrative Panel Decision, Panelists Hon. Sir Ian Barker, Reinhard Schanda, and David Perkins, Case No. D2001-0388, May 30, 2001. Modefine owns the mark "MANI". Saresh Mani of Quincy, MA in 1998 developed the concept of creating a website to locate and foster communications with and among the dispersed members and descendants of the "mani" family from northern India (now Pakistan) by offering them free e-mail services. He then purchased the domain name "mani.com" (which had been registered by another party) for the sum of $1,000 in December, 1998. In January, 1999, he directed a web programmer to create a website located at the "mani.com" URL through which he would offer free e-mail services to all members and descendants of the "Mani" family. The panel dismissed the complaint.

G.A. Modefine S.A. v. Anand Ramnath Mani, WIPO Administrative Panel Decision, Nick Gardner, Sole Panelist, Case No. D2001-0537, July 20, 2001. Modefine owns the mark "ARMANI". Canadian graphic designer Mani had used "armani.com" since 1994 as an email address. Modefine offered him $750 and an Armani suit, but Mani refused, offering instead to change his email address to merely "amani.com". The WIPO judge Nick Gardner said Modefine had "been guilty of abusing the process", and ruled that Mani could keep his domain name.

Citizen Groups

At least two different organizations have existed to help small businesses defend themselves against overly aggressive attempts to cancel domain names.

Domain Defense Advocate (no longer existing)

AltaVista's assistant general counsel warned a California computer technician named Lawrence Tolliver, that his use of www.www-shopping.com infringed the trademark rights of Compaq, owner of Alta Vista, owner of shopping.com, and demanded that Tolliver give up his domain name by June 10, 1999.

To combat Compaq, Tolliver got help from the Domain Defense Advocate, which organized e-mail campaigns from Internet users on behalf of domain holders, against trademark owners. The DDA stated on its web page:

> "When, in September of 1998, Colgate-Palmolive attempted to wrestle the proud name of ajax.org from its rightful owners, we were overcome with the feeling that not only had Network Solutions, Inc. created a system that left the little guys shit outta luck, but that there were very few organizations or bureaus outside of NSI to assist domains in attempting to fend off attacks from large and well-monied corporations that, in reality, had no legal right to the domain-names in question. When the netizens of slashdot.org came to our rescue with a conscientious outpouring of letters and feedback, we were saved. We at ajax.org reaped the benefits of the battle we waged, but to no greater benefit than the salvation of one domain."

Tolliver kept his domain name, and temporarily included the following warning on the first page of his site: "Please note: This web site is not Shopping.com (http://www.shopping.com), and has no business connections whatsoever with it, but you are welcome to shop here at www-Shopping.com (http://www.www-shopping.com) anytime!"

Domain Name Rights Coalition (http://www.domain-name.org/)

The Domain Name Rights Coalition (http://www.domain-name.org/) represents small businesses and Internet users in domain name disputes with trademark holders. The President, Mikki Barry, advises clients threatened by trademark owners to file a petition to cancel with the Trademark Office. His web page originally stated: "Have you received a threat from a trademark owner who wants you to give them your domain name? See our summary page on the NSI dispute policy and a quick overview of your possible rights to stop reverse domain name hijacking." As of June 12, 2002, it stated, "Have you received a threat from a trademark owner who wants you to give them your domain name? See our quick overview of your possible rights to stop reverse domain name hijacking."

A more effective way to fight may be through public opinion.

Verizon thought it could avoid the “sucks.com” problem by registering “verizonsucks.com” itself, which it did. Unfortunately, the online hacker magazine 2600.com then registered “verizonreallysucks.com”. When Verizon then sent a “desist” letter to 2600.com, 2600.com then registered: “VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com”.

C. Copyrights

1. Clickwrap and Browse-Wrap Licensing

First Circuit

2005

Campbell v. General Dynamics Government Systems Corp., 407 F.3d 546 (1st Cir. 2005) (affirming the striking of the employer's affirmative defense, and affirming the denial of the employer's motion to compel arbitration). A company-wide e-mail announced a new dispute resolution policy, which was accessed by links in the e-mail and required discrimination claims to be submitted to arbitration. The First Circuit held that enforcement of the arbitration policy was not appropriate because the e-mail did not provide minimally sufficient notice to a reasonably prudent employee of the contractual nature of the e-mailed policy and the concomitant waiver of the employee's right to access a judicial forum. The Court also held that the mass e-mail, which did not require an affirmative response but requested the recipient to review the materials, was not a traditional means for conveying contractually binding terms of employment, and did not state directly that the policy contained a mandatory arbitration agreement that would become the employee's exclusive remedy for all claims.

> The e-mail made no mention of whether (or how) the Policy would affect an employee's right to access a judicial forum with respect to workplace disputes. Moreover, it neither specified that the Policy contained an agreement to arbitrate that would become binding upon continued em-ployment nor indicated whether the term "workplace disputes" included those giving rise to federal statutory claims. The text of the Policy was not part of the e-mail proper, although the company posted the Policy on its intranet (its internal corporate network).
>
> The e-mail did state that the Policy would become effective on May 1, 2001 (the day following its transmission). It also urged recipients to "review the enclosed materials carefully, as the [Policy] is an essential element of your employment relationship." Those with questions were invited to con-tact the company's vice-president of human resources. The phrase "enclosed materials" was an apparent reference to two embedded links located at the bottom of the e-mail. Each link provided access to a document that the recipient could view by moving a cursor over the link and clicking on it. The first link was labeled "Brochure: http://csconnect.gd-cs.com/hr/dispute_resolution.htm"; clicking on it would have provided access to a two-page brochure that detailed how the Policy worked. Upon reading the second page of that brochure, the recipient would have learned that company employees who "continue [their] current employment after the effective date of the [Policy's] adoption" would be "covered" by its terms and that the Policy would encompass, among other things, "employment discrimination and harassment claims, based on, for example, age, race, sex, religion, national origin, veteran status, citizenship, disability or other characteristics protected by law." In a

shaded box in the lower right-hand corner of that page, the recipient would have found the following statement:

> The Company has adopted this four-step policy as the exclusive means of resolving workplace disputes for legally protected rights. If an employee files a lawsuit against the Company, the Company will ask the court to dismiss the lawsuit and refer it to the [Policy].

Clicking on the second link, entitled "Handbook: http://csconnect.gd-cs.com/hr/DRP_Handbook_2.doc," would have provided access to a dispute resolution handbook, which contained the full text of the Policy (designated as "Human Resources Policy 402"), a flow chart illustrating how the Policy worked, forms for filing claims at each of the four levels, and a compendium of questions that the company thought might arise. No part of the e-mail communication required a response acknowledging receipt of the Policy or signifying that a recipient had read and understood its terms. Although General Dynamics set up a tracking log to monitor whether each of its employees opened the e-mail -- the record indicates that the plaintiff opened the e-mail two minutes after it was sent -- it did not take any steps to record whether its employees clicked on the embedded links to peruse either the brochure or the handbook. Moreover, General Dynamics has not supplied any evidence to contradict the plaintiff's claim that he never read or saw the brochure, the handbook, or the Policy prior to his termination.

Second Circuit

2001

Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002) (*affirming* the trial court's decision, found at 150 F. Supp. 2d 585 (S.D.N.Y. 2001)). The court found a proposed "browse-wrap" contract to be unenforceable, because, in part, the software user was not required to indicate assent to the contract as a precondition to downloading the software.

2002

N.Y. Sup. Ct.

Moore v. Microsoft., 293 A.D.2d 587 (N.Y. App. Div. 2002). A cause of action for deceptive trade practices was barred by the terms of a "clickwrap" software licensing agreement that was displayed to the plaintiff before the software was downloaded, and before it was installed on his computer.

2. Infringement

Second Circuit

2004

MyWebGrocer LLC v. Hometown Info Inc., No. 03-7909 (2d Cir. 7/13/04) (affirming the denial of a preliminary injunction). MyWebGrocer, a web developer, produced product descriptions for an online grocery, which did not renew its contract. The next web developer copied verbatim those descriptions. Although it affirmed the denial of a preliminary injunction, the Second Circuit stated that the first web developer might have some narrow copyright protection, "at least from wholesale verbatim copying", explaining:

> "if the selection process imbues a compilation with the requisite creative spark, the compilation may be protected so long as there are indicia that principles of selection (other than all-inclusiveness) have been employed." *Silverstein v. Penguin Putnam, Inc.*, 368 F.3d 77, 83 (2d Cir. 2004). When the record is complete, a trier of fact might conclude that the various providers have different concepts of the most attractive and useful product description -- brevity versus completeness, bare physical essentials versus essentials plus puffery, full product names versus abbreviations, for example. A trier might conclude that MyWeb made creative choices about what to include or exclude in its product descriptions -- e.g. advertising slogans, sub-brands, product colors, and phrases from product packaging -- for the purpose of facilitating and encouraging online shopping. . . . MyWeb may therefore have a narrow copyright in its product descriptions that protects them from wholesale copying.

Fourth Circuit

2003

Xoom Inc. v. Imageline Inc., No. 02-1121 (4th Cir. 3/21/03). Copyright registrations of compilations of clip-art images is sufficient to permit a copyright infringement action against an infringer on the underlying preexisting works. "Where an owner of a collective work also owns the copyright for a constituent part of that work, registration of the collective work is sufficient to permit an infringement action of the constituent part." *Morris v. Business Concepts Inc.*, 259 F.3d 65 (2d Cir. 2001); *In re Independent Service Organizations Antitrust Litigation*, 964 F. Supp. 1469 (D. Kan. 1997). However, statutory damages are limited to damages for just two works, not for each of the underlying 1,580 clip-art images.

Fifth Circuit

2004

General Universal Systems Inc. v. Hal Inc., No. 01-21114 (5th Cir. 7/20/04) (affirming in part, reversing in part, and remanding). The plaintiff, GUS, had no copy of

the software for which it claimed literal copyright infringement; only a copyright registration for the software. In a footnote, the Fifth Circuit noted:

> GUS claimed in filings to the district court that it submitted a copy of the software source code as well as copies of data entry screens, reports, and record layouts to the Copyright Office when it obtained a copyright registration for the system. The Copyright Office, however, apparently misplaced the source code print-outs and GUS did not retain a copy of the code as it existed in 1983.

So, GUS tried to use indirect evidence (directory listings from both programs, and printouts created by both programs) to prove 1) the "probative similarity" element of the two-part circumstantial proof of copying, and 2) that the copying is legally actionable by showing that the allegedly infringing work is substantially similar to protectable elements of the infringed work.

The district court dismissed the non-literal copyright infringement claims, based on the "abstraction-filtration-comparison" test first outlined by the Second Circuit in *Altai*, refined by the Tenth Circuit in *Gates Rubber,* and adopted by the Fifth Circuit in *Engineering Dynamics, Inc. v. Structural Software, Inc.*, 26 F.3d 1335, 1340 (5th Cir. 1994). The district court awarded summary judgment of non-infringement of the literal copyright infringement claims, awarded a total of $448,928.73 in costs, attorneys' fees, and expenses incurred in successfully defending the copyright cause of action, and later granted HAL's motion for turnover and sale of GUS's Lopez COBOL software.

The Fifth Circuit affirmed the dismissal, the summary judgment, and the award of fees, stating about the summary judgment:

> GUS's difficulty stems, ultimately, from the muddled nature of its infringement claims. As the district court noted, when GUS first filed its infringement suit, it claimed only that HAL misappropriated nonliteral elements of CHAMPION PACKER, like its structure, sequence, and organization. GUS broadened its claims in its summary judgment motion, asserting that HAL directly copied source code from CHAMPION. The exhibits that GUS attached as evidence of source code copying, however, did not reflect the change in the nature of its claims.
>
> GUS had the MEPAW and LOPEZ COBOL source codes at its disposal; it should have supported its assertions with tangible references to these materials rather than with empty and conclusory statements. In short, GUS presented insufficient evidence of source code copying to survive summary judgment. When GUS filed its motion for summary judgment, it did not need to marshal all its facts to support its infringement claims. But when HAL responded with an allegation that GUS could produce no evidence on basic elements of its claims, GUS was required to come forward with tangible evidence. It failed to do so, and summary judgment for HAL was appropriate.

Seventh Circuit

2003

In re Aimster Copyright Litigation, No. 02-4125 (7th Cir. 6/30/03). The Seventh Circuit affirmed the preliminary injunction on the grounds of contributory and vicarious liability, stating that Aimster's own software tutorial was an "invitation to infringement" by its users, and because Aimster could not produce any evidence that it has substantial noninfringing uses. See the discussion of the injunction under the "Fair Use" section below.

Ninth Circuit

2002

Kelly v. Arriba Soft, 280 F.3d 934 (9th Cir. 2002). Clicking on a thumbnail, a user was presented with a page containing a full-sized image that was imported directly from Kelly's Web page. The image was surrounded on the page by a link to the originating Web site, an Arriba banner, and Arriba advertising. The thumbnails were exact replicas of the original image, but they were much smaller, or poorer quality. The Ninth Circuit ruled that the thumbnails were fair use, stating, "Because Arriba's use is not superseding Kelly's use but, rather, has created a different purpose for the images, Arriba's use is transformative.

2004

Metro-Goldwyn-Mayer Studios v. Grokster Ltd., No. 03-55894 (9th Cir. 8/19/04) (affirming a partial grant of summary judgment of no contributory and no vicarious copyright infringement for distributing peer-to-peer file-sharing computer networking software). The plaintiffs included most of the major motion picture studios and recording companies. Defendant StreamCast's software used the type of architecture used by the Gnutella software system, which broadcasts a search request to all the computers on the network, conducts a search of the individual index files, and routes the collective results back to the requesting computer..

Defendants Grokster and StreamCast initially used FastTrack Technology, a type of peer-to-peer file-sharing network (the "supernode" model), in which a number of select computers on the network are designated as indexing servers. The "supernode" architecture was developed by KaZaa BV, a Dutch company, and licensed under the name of "FastTrack" technology. The user initiating a file search connects with the most easily accessible supernode, which conducts the search of its index and supplies the user with the results. Any computer on the network could function as a supernode if it met the technical requirements, such as processing speed.

Contributory Copyright Infringement

The following two of the three elements required to prove a defendant liable under the theory of contributory copyright infringement were in dispute: (1) knowledge of the infringement, and (2) material contribution to the infringement. (The element of direct infringement was undisputed.) Because the software was capable of substantial noninfringing uses, in order to show that the defendants had the requisite knowledge, the plaintiffs had to prove that the defendants had specific knowledge of infringement **at a time at which they contributed to the infringement**, and that the defendants failed to act upon that information. The Ninth Circuit found no "knowledge", stating,

> "Indeed, at present, neither StreamCast nor Grokster maintains control over index files. As the district court observed, even if the Software Distributors "closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption."

The Ninth Circuit also found no "material contribution", in spite of the following:

> "Stream-Cast maintains an XML11 file from which user software periodically retrieves parameters. These values may include the addresses of websites where lists of active users are maintained. The owner of the FastTrack software, Sharman, maintains root nodes containing lists of currently active supernodes to which users can connect. Both defendants also communicate with users incidentally, but not to facilitate infringement. . . . While Grokster and StreamCast in particular may seek to be the "next Napster," *Grokster I*, 259 F. Supp. 2d at 1036, the peer-to-peer file-sharing technology at issue is not simply a tool engineered to get around the holdings of Napster I and Napster II."

Vicarious Copyright Infringement

Only the third element was in dispute, of the following three elements required to prove a defendant vicariously liable for copyright infringement: (1) direct infringement by a primary party, (2) a direct financial benefit to the defendant, and (3) the right and ability to supervise the infringers. The Ninth Circuit found no right and ability to supervise, stating:

> However, given the lack of a registration and log-in process, even Grokster has no ability to actually terminate access to filesharing functions, absent a mandatory software upgrade to all users that the particular user refuses, or IP address blocking attempts. It is also clear that none of the communication between defendants and users provides a point of access for filtering or searching for infringing files, since infringing material and index information do not pass through defendants' computers. In the case of StreamCast, shutting down its XML file altogether would not prevent anyone from using the Gnutella network. In the case of Grokster, its licensing agreement with KaZaa/Sharman does not give it the ability to mandate that root nodes be shut down.

3. Fair Use

The following cases involving the defense of "fair use" are in no way exhaustive. They are merely some that interested this author.

Second Circuit

2004

NXIVM Corp. v. The Ross Institute, 364 F.3d 471 (2d Cir. 2004) (affirming the denial of a preliminary injunction, even though the alleged infringers knew that their access to the copyrighted material was unauthorized). "Because the Harper & Row Court did not end its analysis of the fair use defense after considering and ascertaining the defendants' bad faith there, we believe that the bad faith of a defendant is not dispositive of a fair use defense. Instead, we agree with the court in *Religious Tech. Ctr. v. Netcom On-Line Communication Services, Inc.*, 923 F. Supp. 1231, 1244 n.14 (N.D. Cal. 1995), that '[n]othing in Harper & Row indicates that [the defendants'] bad faith [is] itself conclusive of the fair use question, or even of the first factor [the purpose and character of the use].'"

Third Circuit

2002

Dun & Bradstreet Software Services Inc. v. Grace Consulting Inc., 307 F.3d 197 (3d Cir. 2002). Grace offered software maintenance services to D&B's customers, at prices far below what D&B charged. D&B sued for copyright infringement and misappropriation of trade secrets. Grace argued that it used "copy and call" commands to access D&B's software, and thus any copying, if performed, was inadvertent and de minimis. (Programmers use "copy and call" commands to retrieve data or execute code from another program stored on the computer without independently booting up that second program.) In response, the Third Circuit stated:

> In supporting its de minimis defense, Grace asserts that the quantitative infringement amounted to only twenty-seven lines out of 525,000 lines. This argument is irrelevant as a matter of law and we therefore will not tarry on the disputed factual element. The unrefuted trial testimony was that if one considers Grace's use of Copy and Call commands to gain access to PAYTXABR and the Geac code, the CNR W-2 program actually consists of 62% Geac code, and the GMI W-2 program possesses approximately 43% of Geac's code. Much more significant, however, than the quantity of copy is the quality of the material purloined.
>
> A de minimis defense does not apply where the qualitative value of the copying is material. Kremin, Geac's technical expert, and Dr. Dewar, Grace's expert, both

agree that Geac's software would not work if PAYTXABR were removed from it and that Grace's infringing W-2 software would not work without its copies of PAYTXABR. Thus, the information Grace copied was highly critical.

The Third Circuit also rejected the argument that interoperability was an external factor that justified copying the software:

> Both Altai and Mitel clearly held that in determining aspects of the program not entitled to protection because of external factors, we examine the program from the viewpoint of the creator. … Dewar's testimony regarding external factors, including interoperability, is wholly misplaced. As Dewar admitted on cross-examination, he focused on externality from the viewpoint of Grace's W-2 program, not Geac's. He looked at externalities from the eyes of the plagiarist, not the eyes of the program's creator. As explained, in determining whether certain aspects of an allegedly infringed software are not protected by copyright law, the focus is on external factors that influenced the choice of the creator of the infringed product.

Finally, the Third Circuit considered the issue of copyright preemption of trade secret claims for the first time, holding that the trade secret claims related to both the customer lists and the software were not subject to copyright preemption because a state law misappropriation of trade secrets claim that requires a proof of breach of duty of trust or confidence to the plaintiff through the improper disclosure of confidential materials is qualitatively different from copyright infringement because it is not an element of copyright infringement.

Seventh Circuit

Ninth Circuit

2001

A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001). The Recording Industry Association of America ("RIAA") sued Napster on December 7, 1999, alleging contributory and vicarious copyright infringement. Napster allows online users to trade audio tracks directly from their PCs. The Napster website stated: "Welcome to Napster Join the largest, most diverse online community of music lovers in history by downloading and installing Napster. It's fun, simple and free."

In a press release on July 3, 2000, Napster CEO Hank Barry stated: "This case is about whether it is legal to share MP3 versions of sound recordings over the Internet. "We say yes--the major labels say no." The general counsel for the RIAA has stated in

a press release, “Napster is about facilitating piracy and trying to build a business on the backs of artists and copyright owners.”

The trial court entered a preliminary injunction. Two Ninth Circuit judges then granted a stay of the injunction, pending appeal. On February 12, 2001, the Ninth Circuit affirmed that Napster would probably lose on the issues of direct infringement by the users of Napster, and on Napster’s contributory and vicarious copyright infringement. The Ninth Circuit affirmed the preliminary injunction, but remanded for a hearing on the scope of the injunction. Regarding direct infringement, the Ninth Circuit concluded that **Napster users did not have a valid fair use defense**, and concerning one of the factors, stated:

> “We conclude that the district court did not err when it refused to apply the "shifting" analyses of Sony and Diamond. Both Diamond and Sony are inapposite because the methods of shifting in these cases did not also simultaneously involve distribution of the copyrighted material to the general public; the time or space-shifting of copyrighted material exposed the material only to the original user.” *Id.* at 1019.

Regarding contributory infringement, the Ninth Circuit ruled:

> “Under the facts as found by the district court, Napster materially contributes to the infringing activity. Relying on Fonovisa, the district court concluded that ‘[w]ithout the support services defendant provides, Napster users could not find and download the music they want with the ease of which defendant boasts.’”

Regarding vicarious copyright infringement, the Ninth Circuit ruled:

> “Our review of the record requires us to accept the district court's conclusion that plaintiffs have demonstrated a likelihood of success on the merits of the vicarious copyright infringement claim. Napster's failure to police the system's "premises," combined with a showing that Napster financially benefits from the continuing availability of infringing files on its system, leads to the imposition of vicarious liability.”

2002

A&M Records Inc. v. Napster Inc., 62 USPQ2d 1221 (9th Cir. 2002). Napster appealed the district court's order forcing Napster to disable its file transferring service until certain conditions were met, to achieve full compliance with the modified preliminary injunction. The Ninth Circuit affirmed both the district court's modified preliminary injunction and shut down order.

On June 3, 2002, Napster filed for Chapter 11 bankruptcy protection, agreeing to sell its assets to Bertelsmann for $8 million. The rumor was that Napster would emerge as a wholly-owned subsidiary of Bertelsmann, complying with the copyright laws as a subscription music service. In September, 2002, Napster died: it closed its doors, and

put a “Dead Kitty” sign with a tombstone on the home page of its website. On December 11, 2002, Napster stuff was auctioned off. Napster had filed for bankruptcy earlier in 2002. Santa Clara-based software maker Roxio bought the brand name and intellectual property after Napster's bankruptcy. Since Napster fell off the map, other free online music trading services have taken its place, including Kazaa and Gnutella networks. Apparently the subscription services have fewer than 500,000 users combined, whereas in early 2003 Kazaa had about 3.5 million users online at any given time.

In late July, 2003, Roxio's chairman and chief executive, Chris Gorog, announced plans to shelve its current online music service, pressplay, and roll out Napster 2.0 by Christmas. Napster 2.0 supposedly will offer the option of either paying a la carte to download music, or paying a monthly subscription fee.

2003

Kelly v. Arriba Soft Corp.,67 USPQ2d 1297 (9th Cir. 2003). The Ninth Circuit affirmed its earlier ruling that thumbnail images were fair use, but withdrew the part of its prior opinion regarding whether Arriba’s display of the full-sized images was a fair use, because on that issue the district court had made a summary judgment ruling without a motion for summary judgment from the parties. Therefore, the Ninth Circuit reversed the district court’s summary judgment as to the display of the full-sized images, and remanded the case for further proceedings.

2007

Perfect 10 v. Google, Inc., 2007 U.S. App. LEXIS 11420, No. 04-57143 (9th Cir., March 29, 2007 (rehearing denied). The Ninth Circuit vacated a preliminary injunction for displaying thumbnail versions of the owner’s photographs of nude models, stating, “Google has provided a significant benefit to the public. … We conclude that Perfect 10 is unlikely to be able to overcome Google's fair use defense”. However, the Ninth Circuit remanded. …

4. Linking & Framing

Here’s some food for thought, from the CIO magazine website, at www.cio.com: “Linking to Us: We invite you to link to any/all of our web pages. We do not view this as duplication.” Just as with the domain name cases, there are a lot of these cases. At one time you could find some of them at:
http://www.gigalaw.com/library/copyrightcases.html.

Ninth Circuit

2001

Kelly v. Arriba Soft, 280 F.3d 934 (9th Cir. 2002). Clicking on a thumbnail, a user was presented with a page containing a full-sized image that was imported directly from Kelly's Web page. The image was surrounded on the page by a link to the originating Web site, an Arriba banner, and Arriba advertising. The Ninth Circuit ruled that the unauthorized online linking to images residing on Kelly's web site violated Kelly's right of public display.

5. Crawling

Ninth Circuit

2000
N.D. Cal.

Ebay v. Bidder's Edge On May 24, 2000, a U.S. District Court in the Northern District of California issued a preliminary injunction to stop Bidder's Edge from using an automated program to search eBay's website for information. Bidder's Edge had accessed eBay's site as much as 100,000 times a day over a ten-month period. The court said that such searches, using "software robots" that carry out thousands of instructions per minute, can slow down a computer system's operations. The court held that Bidder's Edge had "trespassed" on eBay's computer system without permission.

C.D. Cal.

Ticketmaster Corp., et al. v. Tickets.Com, Inc., 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000). On August 10, 2000, the judge denied Ticketmaster's request for a preliminary injunction to stop Tickets.com from crawling Ticketmaster's site and posting information about (and links to pages about) tickets for sale on Ticketmaster's site. The judge relied on the Supreme Court's Feist opinion that factual information is not copyrightable, stated that the copying is protected by fair use, and stated that the reasoning on trespass in the recent eBay "crawling" case was inapplicable, because the crawling did not interfere with Ticketmaster's web site.

6. Audio Home Recording Act ("AHRA")

The Audio Home Recording Act of 1992 required manufacturers of digital audio recording devices to implement code systems to curb serial re-recordings of copyrighted music. At the same time, the law explicitly barred copyright suits from being brought "based on the noncommercial use by a consumer" of a digital or analog recording device. See 17 U.S.C. § 1008.

Ninth Circuit

1999

Recording Industry Ass'n of America v. Diamond Multimedia Systems, Inc., 180 F.3d 1072, 51 U.S.P.Q.2d 1115 (9th Cir. 1999). In 1998, the Recording Industry Association of America ("RIAA") sued Diamond Multimedia. Diamond's Rio PMP300 player allows users to download songs from the Internet in the MP3 (MPEG 1, Audio Layer 3) format and replay them on home stereos.

The Ninth Circuit held that Diamond's Rio PMP300 player does not fall within the "digital recording device" definition used in the Audio Home Recording Act, and that the act applies to recordings made from digital audio tapes or CDs, but not to recordings made from the hard drives of computers**.**

2001

A&M Records, Inc. v. Napster, Inc., 57 USPQ2d 1729, 1743 (9th Cir. 2001). Regarding one of Napster's defenses, the Ninth Circuit said, "[T]he Audio Home Recording Act does not cover the downloading of MP3 files to computer hard drives."

7. Digital Millennium Copyright Act ("DMCA")

Fearful that the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material, Congress sought to combat copyright piracy in its earlier stages, before the work was even copied. The Digital Millennium Copyright Act (DMCA) prohibits the circumvention of technological measures (such as encryption and passwords) used to protect copyrighted material. 17 U.S.C. §1201(a)(1)). The clause dealing with circumvention went into effect October 28, 2000, two years after the October 28, 1998, signing of the legislation. Additionally, the DMCA prohibits buying or selling a technology primarily designed to circumvent a digital wall (the "anti-trafficking provisions," contained in 17 U.S.C. §1201(a)(2), (b)(1)). Also, the DMCA prohibits transmission of copyrighted material that has had "copyright management information" (e.g. author's name, copyright notice) removed. This provision was effective when the legislation was passed. See 17 U.S.C. §§ 1201-05. When the DMCA is violated willfully and for purposes of profit, felony punishment is permissible.

The DMCA also added §512 to 17 U.S.C., to limit the liability of ISP's. The DMCA established certain "safe harbors" to provide protection from liability for: (1) transitory digital network communications; (2) system caching; (3) information residing on systems or networks at the direction of users; and (4) information location tools. 17 U.S.C. §§ 512(a)-(d).

Gnutella

At one time the old website http://gnutella.wego.com/ stated:

> "Gnutella is a real-time search, peer-based file-sharing client that allows a user running a Gnutella client to search for and download files from other Gnutella users. Gnutella was originally conceived, authored and released by Justin Frankel and Tom Pepper of Nullsoft in March 2000."

As of September, 2007, Gnutella was still operating at http://www.gnutella.com, and stated at http://www.gnutella.com/news/4210:

> Where did Gnutella come from? The evil-geniuses at Nullsoft (creators of Winamp) first developed the protocol in late 1999. Since Nullsoft had recently been acquired by AOL (soon to be AOL-Time Warner), the problems that would arise remain obvious. Nullsoft basically had to cease using the company's resources to develop this technology because the record labels saw (and still see) it as a threat to their industry.
>
> However, what the technology really accomplishes is not a threat to any industry; rather, it creates a revamped atmosphere on the Internet, enabling users to share information like never before. To put it simply, Gnutella puts the personal interaction back into the Internet. When you run Gnutella software and connect to the Gnutella Network, you bring with you the information you wanted to make public. And you choose what information to share. You can choose to share nothing; you can choose to share one file, a directory, or your entire hard drive (we do not recommend this option).
>
> One of the major differences between Gnutella and Napster-like software is that those applications are centralized. That means the technology uses central servers where the government agencies can spy on you and infringe on your freedom to search the net.
>
> So Gnutella allows you to search for information anonymously, and it allows you to search for information in a setting that differs from traditional search engines like Yahoo! because unlike search engines like that, the information is not controlled or fed to you. Nothing is pushed at you; you control what you look for.

In March, 2007, the Gnutella website had very few posts on it since 2006, and one of the discussion threads was "Is Gnutella dying?". As of September 1, 2007, there had been only about fifteen posts of user comments on the main page of Gnutella. ..

Second Circuit

2000

S.D.N.Y.
UMG Recordings, Inc., et al. v. MP3.com, Inc., 92 F.Supp.2d 349 (S.D.N.Y. May 04, 2000). The Recording Industry Association of America ("RIAA") sued My.MP3.com on January 21, 2000, because of the "Beam-It" and "Instant Listening" software services

provided by MP3.com that allowed users to insert into their My.Mp3.com Music Manager (i.e. personal locker) copies of CDs they already own.

On May 4, 2000, Judge Rakoff of the District Court in New York, N.Y., granted summary judgment of copyright infringement.

On June 9, 2000, Time Warner and BMG settled with MP3.com, each granting a license to MP3.com. BMG also licensed rights to its music library to MusicBank, a start-up online music storage service. MP3.com issued a joint press release with Time Warner and BMG, stating:

> MP3.com allows users to access, manage, and listen to their personal music collection anytime and anywhere in the world, using any web-enabled device or application. MP3.com enables more than 67,000 artists to distribute and promote their music worldwide, while enabling consumers to conveniently access this expanding music catalog. Consumers can search for, listen to, and download music free of charge.

On August 21, 2000, Sony Music settled with MP3.com. UMG Recordings, Inc. (Universal Music Group), the largest record company in the world, had still not settled with MP3.com. Then, on August 23, 2000, the court ruled that the damages should be based on the CD's, and not on the individual songs on the CD's. *UMG Recordings, Inc. v. MP3.COM, Inc.*, 109 F.Supp.2d 223 (S.D.N.Y. Aug 23, 2000). People then speculated that MP3.com would get off easy. However, on September 6, 2000, the court ruled that the damages would be $25,000 for each CD. *UMG Recordings, Inc. v. MP3.Com, Inc.*, 2000 WL 1262568, 56 U.S.P.Q.2d 1376 (S.D.N.Y. Sep 06, 2000). The speculation then became that MP3.com would soon cease to exist.

However, on September 1, 2007, the site still existed, and had the following statements on its home page:

> **Musicians Wanted.**
> Sign up for a free mp3.com artist account
> and get exposed to millions of fans.
>
> **Download free music**
> Sign up for a fan account Free Account Signup

2001

Universal City Studios Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (affirming an injunction prohibiting posting on the Internet, or creating hyperlinks to, DeCSS). "CSS is an encryption scheme that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. The algorithm is a type of mathematical formula for transforming the contents of the movie file into gibberish; the "keys" are in actuality strings of 0's and 1's that serve as values for the mathematical formula. Decryption in the case of CSS requires a set of "player keys" contained in compliant DVD players, as

well as an understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the contents of a DVD. With the player keys and the algorithm, a DVD player can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content of the DVD."

"In September 1999, Jon Johansen, a Norwegian teenager, collaborating with two unidentified individuals he met on the Internet, reverse–engineered a licensed DVD player designed to operate on the Microsoft operating system, and culled from it the player keys and other information necessary to decrypt CSS. The record suggests that Johansen was trying to develop a DVD player operable on Linux, an alternative operating system that did not support any licensed DVD players at that time. In order to accomplish this task, Johansen wrote a decryption program executable on Microsoft's operating system. That program was called, appropriately enough, "DeCSS." If a user runs the DeCSS program (for example, by clicking on the DeCSS icon on a Microsoft operating system platform) with a DVD in the computer's disk drive, DeCSS will decrypt the DVD's CSS protection, allowing the user to copy the DVD's files and place the copy on the user's hard drive. The result is a very large computer file that can be played on a non–CSS–compliant player and copied, manipulated, and transferred just like any other computer file. DeCSS comes complete with a fairly user–friendly interface that helps the user select from among the DVD's files and assign the decrypted file a location on the user's hard drive. The quality of the resulting decrypted movie is "virtually identical" to that of the encrypted movie on the DVD. And the file produced by DeCSS, while large, can be compressed to a manageable size by a compression software called "DivX," available at no cost on the Internet. This compressed file can be copied onto a DVD, or transferred over the Internet (with some patience)."

The district court entered an injunction, prohibiting posting on the Internet, or creating hyperlinks to, DeCSS. The Second Circuit held that the injunction did not violate the First Amendment right of free speech.

A professor at Carnegie Mellon, Dr. David S. Touretzky, in the Computer Science Department, has a website devoted to this issue:

http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/.

There he states: "If code that can be directly compiled and executed may be suppressed under the DMCA, as Judge Kaplan asserts in his preliminary ruling, but a textual description of the same algorithm may not be suppressed, then where exactly should the line be drawn? This web site was created to explore this issue, and point out the absurdity of Judge Kaplan's position that source code can be legally differentiated from other forms of written expression."

Third Circuit

2003

Bonneville Int'l Corp. v. Peters, 347 F.3d 485 (3d Cir. 2003) (affirming summary judgment for the Copyright Office). An Association of radio station owners

sued the Register of Copyrights, seeking to invalidate a rule promulgated by the Copyright Office excluding simultaneous Internet "streaming" of station broadcasts from statutory exemption of copyright coverage. The Third Circuit held that the statutory exemption of "nonsubscription broadcast transmissions" from digital audio transmission performance copyright coverage implicates only over-the-air radio broadcast transmissions, and does not cover a station's simultaneous Internet streaming of its AM/FM broadcast signals. The Court reasoned that there are no affirmative grounds to justify expansion of the protections offered by the DPRA into a region about which the DMCA is silent, and stated, "We have already noted that the exemptions the DPRA afforded to radio broadcasters were specifically intended to protect only traditional radio broadcasting, and did not contemplate protecting AM/FM webcasting."

Fourth Circuit

2001

ALS Scan, Inc. v. RemarQ Communities, Inc, 239 F.3d 619 (4th Cir. 2001) (reversing a summary judgment that had been granted summary in favor of RemarQ). ALS Scan, Inc., ("ALS") creates and markets copyrighted "adult" photographs which it makes available online or on CD-ROMs to subscribers for a fee. RemarQ Communities, Inc. ("RemarQ"), an Internet service provider, provides its subscribers with access to newsgroups, two of which contained infringing copies of ALS's images posted by subscribers to the newsgroups. ALS contacted RemarQ, alleging that through these newsgroups RemarQ had provided access to more than 10,000 images belonging to ALS over a several-month period. ALS demanded the removal of the images, but RemarQ did not comply.

ALS sued RemarQ, alleging violations of the DMCA, as well as unfair competition. The district court granted summary judgment in favor of RemarQ on the ground that ALS failed to comply with the DMCA notice requirements because it did not specifically identify the infringing works in its notice to RemarQ.

The Fourth Circuit reversed and remanded, holding that an ISP which receives "substantial" notice of infringing materials on its system cannot ignore such notice, and still avail itself of the DMCA's safe harbor for ISP's.

Ninth Circuit

2004

Ellison v. Robertson, 357 F.3d 1072 (9th Cir. 2004) (affirming in part a summary judgment for the ISP, reversing in part, and remanding). The owner of copyrighted works sued for copyright infringement against an Internet service provider which allowed a third party to post several of the owner's short stories on the network. In order for a provider to be eligible for DMCA's safe-harbor provisions, providers must implement a policy that provides for the termination of service access for repeat copyright infringers in appropriate circumstances and must inform subscribers of that policy. In this case, the Internet service provider did post a brief summary of its policy

as to repeat infringers, but it changed the e-mail address to which infringement notifications were to be sent, and failed to forward messages sent to the old address or notify the senders that the old address was inactive. The court stated this inaction which allowed notices of potential copyright infringement to go completely unheeded was sufficient for a reasonable jury to conclude that the provider had not reasonably implemented its policy against repeat offenders.

The Court also determined that the provider's storage of the infringer's posts on its servers for fourteen days constituted "intermediate" and "transient" storage that was not "maintained on system or network…for a longer period than is reasonably necessary for the transmission, routing, or provision of connections," within the meaning of DMCA's safe-harbor provisions. The Court affirmed the district court's holdings as to vicarious and contributory infringement, but remanded, finding that there were "triable issues of material fact concerning whether AOL meets the threshold requirements, set forth in § 512(i), to assert the safe harbor limitations of liability of §§ 512(a-d)."

2007

Perfect 10, Inc. v. CCBILL LLC, 488 F.3d 1102 (9th Cir. 2007) (holding that the defendants were eligible for CDA immunity for state law claims of unfair competition, false advertising, and right of publicity claims). Perfect 10, the publisher of an adult entertainment magazine and the owner of the subscription website perfect10.com, alleged that CCBill and CWIE were not entitled to the "safe harbor" provisions of the DMCA for providing services to websites that posted images stolen from Perfect 10's magazine and website. The Court quoted the district court in stating that the DMCA safe harbors limit liability but do not affect the question of ultimate liability under the various doctrines of direct, vicarious, and contributory liability. Regarding those safe harbor provisions, the Court held:

> [A] service provider "implements" a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications. …
>
> To identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement. …
>
> Permitting a copyright holder to cobble together adequate notice from separately defective notices also unduly burdens service providers. …
>
> Since Perfect 10 did not provide effective notice, knowledge of infringement may not be imputed to CCBill or CWIE based on Perfect 10's communications. …
>
> We do not place the burden of determining whether photographs are actually illegal on a service provider. …
>
> Password-hacking websites are thus not per se "red flags" of infringement. …
>
> Because CWIE does not receive a direct financial benefit, CWIE meets the requirements of § 512(c).

D.C. Circuit

2003

Recording Industry Ass'n of America Inc. v. Verizon Internet Services Inc., Nos. 03-7015, 03-7053 (D.C. Cir. 6/4/03). The D.C. Circuit denied a request for a stay pending appeal of an order by the U.S. District Court for the District of Columbia requiring Verizon, as an Internet service provider, to disclose information about users to the RIAA, which was seeking to enforce a subpoena under the authority of the DMCA.

Recording Industry Ass'n of America Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003) (reversing and remanding to vacate an order enforcing a subpoena, and to grant a motion to quash another subpoena).

The RIAA served Verizon with two subpoenas pursuant to the subpoena provision of the DMCA, seeking the identity of two ISP subscribers whom it believed were infringing its members' copyrights by trading large numbers of digital files of copyrighted music using file sharing programs (such as P2P). The D.C. Circuit determined that a subpoena may be issued to only an ISP that is engaged in storing copyright infringing material on its servers. The statute does not authorize the issuance of subpoenas to an ISP that merely transmits infringing material, but does not store any such material on its servers. Because Verizon does not store the material on its servers, the D.C. Circuit vacated the district court's order enforcing the subpoena.

Federal Circuit

2004

The Chamberlain Group, Inc. v. Skylink Technologies, Inc., No. 04-1118 (Fed. Cir. 8/31/04). Under the DMCA, a charge of trafficking in a device that circumvents technology and provides "access" to a copyrighted work requires proof that the access was unauthorized. The DMCA prohibits only those forms of access that reasonably relate to copyright protections that are otherwise available. The statute defines "circumvent" as a set of acts taken "without the authority of the copyright owner." DMCA liability under 17 U.S.C. §1201(a)(2) requires proof of unauthorized access as part of the plaintiff's case in chief. Congress could not have intended that merely accessing copyrighted software would be a per se violation of the DMCA's anti-circumvention provision. "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." 17 U.S.C. §1201(c)(1). The Court stated:

> Under Chamberlain's proposed construction, explicated at oral argument, disabling a burglar alarm to gain "access" to a home containing copyrighted books, music, art, and periodicals would violate the DMCA; anyone who did so would unquestionably have "circumvent[ed] a technological measure that effectively controls access to a work protected under [the Copyright Act]." …

> In a similar vein, Chamberlain's proposed construction would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial "encryption" scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products. In other words, Chamberlain's construction of the DMCA would allow virtually any company to attempt to leverage its sales into aftermarket monopolies—a practice that both the antitrust laws … and the doctrine of copyright misuse … normally prohibit.

8. Webcasting

On December 11, 2000, the Copyright Office amended its regulations to clarify that transmissions of an AM/FM broadcast signal over the Internet are subject to a sound recording copyright owner's exclusive right to perform his or her work publicly by means of digital audio transmissions. Broadcasters who choose to transmit their radio signals over the Internet may do so under a compulsory license. The Copyright Office relied on its interpretation of 17 U.S.C. § 114(d).

In response, a radio station sued the Register of Copyrights, seeking to invalidate that rule, which interpreted the statutory exemption from copyright coverage for sound recordings to not encompass "streaming," occurring when a licensed radio station transmitted a sound recording over its Internet website while simultaneously broadcasting the sound recording over air. The RIAA intervened as a defendant, and both parties moved for summary judgment. The court held in favor of the Register of Copyrights. *Bonneville Intern. Corp. v. Peters*, 153 F.Supp.2d 763 (E.D. Pa. 2001).

On February 7, 2002, the U.S. Copyright Office issued a notice of a proposed rulemaking on the requirements for giving sound recording copyright owners reasonable notice of the use of their works in connection with the section 114 statutory license for certain digital transmissions of public performances of sound recordings, and on the requirements for how records of such use will be kept and made available to copyright owners. The rates for webcasting are set forth in 37 CFR 261.

9. Electronic Databases

2001

U.S. Supreme Court

New York Times Co. v. Tasini, 59 USPQ2d 1001 (U.S. Sup.Ct. 2001)**.** Absent written permission from the author of an article that is part of a collective work, 17 U.S.C. §201(c) permits the copyright owner of the collective work to reproduce and distribute individual contributions to the collective work "as part of" any "revision" of that work. The Court held that reproduction of periodical articles in electronic databases, without

the consent of the articles' authors, is not protected by the privilege set forth in 17 U.S.C. §201(c).

The Court reasoned that databases present each contribution to a searcher as a separate item within the search result, without the context provided by the original periodical editions or by any revision of those editions. The entire database cannot be a "revision" of each constituent edition of a periodical, because the massive whole of the database is not recognizable as a new "version" of its every small part, and because, if databases are viewed as simply presenting individual articles individually, such reproduction and distribution would violate the authors' exclusive rights under 17 U.S.C. §106.

After the decision by the Supreme Court ("Tasini I"), the New York Times posted a notice on its website stating that any freelance writer's work affected by the Tasini I decision would be removed from the electronic databases unless the writer executed a release of all claims arising out of the New York Times' infringement in connection with that work. To that end, the notice contained a document (the "Release Agreement" or "Restoration Request") pursuant to which freelance writers could release their claims for compensation. All told, the New York Times intends to remove each of the affected articles, numbering approximately 115,000. Tasini sued, alleging that the Release Agreement was unlawful and unenforceable. *Tasini v. New York Times Co., Inc.*, 184 F.Supp.2d 350 (S.D.N.Y. 2002). The court granted the defendant's motion to dismiss.

10. Copyrights in Government Works

2001-2002

Fifth Circuit

Works created by the federal government are not copyrightable. 17 U.S.C. § 105. On February 2, 2001, the Fifth Circuit, as a matter of first impression, held that copyright protection for privately authored model building codes does not "evanesce" when the codes are adopted by local governments. As long as citizens have reasonable access to the codes, the copyrights remain enforceable. Thus, copying by a noncommercial Internet website infringes copyrights in those codes. *Veeck v. Southern Bldg. Code Congress Int'l Inc.*, 241 F.3d 398 (5th Cir. 2001).

Upon a motion for rehearing, the *en banc* Court reversed. The Court stated that when Veeck copied only "the law" of Anna and Savoy, Texas, which he obtained from SBCCI's publication, and when he reprinted only "the law" of those municipalities, he did not infringe SBCCI's copyrights in its model building codes. *Veeck v. Southern Bldg. Code Congress Int'l, Inc.*, 293 F.3d 791 (5th Cir. 2002).

D. Defamation, Privacy & Child Protection

1. Communications Decency Act ("CDA") 47 U.S.C. § 230

47 U.S.C. § 230. Protection for private blocking and screening of offensive material.

(a) Findings

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy

It is the policy of the United States—

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children’s access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for “Good Samaritan” blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in [sub]paragraph [(A)].

(d) Obligations of interactive computer service

A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

(e) Effect on other laws

(1) No effect on criminal law

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

(2) No effect on intellectual property law

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. **No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.**

(4) No effect on communications privacy law

Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

(f) Definitions

As used in this section:

(1) Internet

The term “Internet” means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service

The term “interactive computer service” means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

The term “information content provider” means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

(4) Access software provider

The term “access software provider” means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

Supreme Court

1997

Reno v. ACLU, 521 U.S. 844 (1997). The ACLU sued, challenging the constitutionality of CDA provisions that sought to protect minors from harmful material on the Internet. The Court held that the challenged provisions were facially overbroad, thus in violation of the First Amendment. However, the provisions would be saved from facial overbreadth challenge by severing the phrase "or indecent" from the statute, pursuant to its severability clause.

First Circuit

2007

Universal Communication Systems Inc. v. Lycos Inc., 478 F.3d 413 (1st Cir. 2007) (affirming the dismissal of all claims, and holding that Lycos is immune to claims arising from user posts made on its Raging Bull message boards). Plaintiffs Universal Communication Systems, Inc. and its chief executive officer, Michael J. Zwebner, sued Lycos, objecting to a series of allegedly false and defamatory postings made under pseudonymous screen names on an Internet message board operated by Lycos.

Third Circuit

2003

Green v. America Online, 318 F.3d 465 (3d Cir. 2003). An ISP subscriber sued an ISP for negligent failure to properly police its network after two other subscribers transmitted allegedly defamatory information about the subscriber to an Internet chat room, and later transmitted a program to the subscriber's computer that caused it to shut down. The Court held that the tort claims were barred by AOL's immunity under 47 U.S.C. 230. Section 230 provides immunity to an ISP "as a publisher or speaker of information originating from another information content provider". Section 230 further provides that no cause of action may be maintained under state law that would be inconsistent with its provisions. The Court further noted that a program is "information" within the meaning of the Act, and the transmission of the "punter" program to the subscribers' computer was likewise within the scope of the Act, and thus, AOL was immune.

Fourth Circuit

1997

Zeran v. America Online, 129 F.3d 327 (4th Cir. 1997) (affirming judgment for AOL). The plaintiff alleged that AOL had "unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar posting thereafter." The district court granted judgment for AOL on the grounds that Section 230 bars Zeran's claims. In affirming, the Court of Appeals stated:

> By its plain language, §230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third party user of the service. Specifically, §230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for the exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred. *Zeran v. American Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (finding that failure to remove defamatory statements was an act shielded from liability by section 230(c)).

Immunity under the CDA requires proof of three elements. Defendant must establish (1) that it is an interactive computer services provider; (2) that it is not an

information content provider with respect to the disputed activity; and (3) that plaintiff seeks to hold defendant liable for information originating with a third-party user of its service.

1998
E.D. Va.
Mainstream Loudoun v. Board of Trustees of Loudoun County Library, 2 F.Supp.2d 783 (E.D. Va. 1998).

The CDA did not provide immunity to a county library board of trustees, and its individual members, in a § 1983 action brought by library patrons who alleged that the board's enforcement of its policy of blocking access to adult-oriented Internet sites from library computers violated their First Amendment free speech rights.

Sixth Circuit

2001
E.D. Mich.

Ford Motor Co. v. GreatDomains.Com, 60 USPQ2d 1446 (E.D. Mich. 2001) (holding that this law does not immunize a defendant from liability for trademark infringement, even if the defendant is considered to be provider of an "interactive computer service"). The Zeran quotation, in context, refers to defamation and other forms of tort liability. This statute states, "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. §230(e)(2). Courts have uniformly held that this law does not immunize a defendant from liability for trademark infringement or copyright infringement. *Gucci America Inc. v. Hall & Associates*, 60 USPQ2d 1714 (S.D.N.Y. 2001).

Ninth Circuit

2000
California Superior Court

Stoner v. eBay, 56 USPQ2d 1852 (Calif Super Ct 2000) (holding that eBay was an interactive service provider, but not a content provider.). The CDA also provides immunity from State laws.

2003

Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003). The plaintiff, Ellen Batzel of North Carolina, was an entertainment lawyer. Batzel hired one of the defendants, Robert Smith, also of North Carolina, to paint her house. After Batzel declined to help Smith market a script he wrote, Smith sent messages to Ton Cremers, a resident of the Netherlands. Cremers published in his newsletter, to owners and operators of museums, claims by Smith that Batzel claimed a connection with Heinrich Himmler, and that her personal art collection included pieces stolen by the Nazis from Jews.

Batzel sued Smith, Cremers, the Netherlands Museums Association, Ohio-based Mosler Inc., and 50 "Doe" defendants. Cremers moved to dismiss for lack of personal jurisdiction. Previously, the district court had ruled that the sending of the e-mail newsletter to California subscribers, along with a trip to California for a conference and the republishing of articles from California newspapers, were sufficient to support an exercise of personal jurisdiction over Cremers and his Museum Security Network Cremers also moved to strike under the California anti-SLAPP statute, alleging that Batzel's suit was meritless and that the complaint was filed in an attempt to interfere with his First Amendment rights. However, because Cremers did not timely appeal the court's ruling on the jurisdiction issue, the Ninth Circuit declined to hear his appeal on that issue.

The Ninth Circuit remanded the case, because under the CDA, Section 230(c)(1), "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The Ninth Circuit suggested that the term "interactive computer service" might apply to Cremers because "the definition of 'interactive computer service' on its face covers 'any' information services or other systems, as long as the service or system allows 'multiple users' to access 'a computer server'." The Ninth Circuit also said that the immunity applies on its face to "users" of interactive computer services as well as service providers, and that Cremers was using such services.

Carafano v. Metrosplash.com Inc., 339 F.3d 1119 (9th Cir. 2003). The district court had held that a matchmaker web site is a content provider, and thus not immune from suit. However, it found no liability, because of no proof of actual malice. The Ninth Circuit affirmed, but reversed the "no immunity" holding, stating:

> [S]o long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process.
> The fact that some or the content was formulated in response to Matchmaker's questionnaire does not alter this conclusion. Doubtless, the questionnaire facilitated the expression of information by individual users. However, the selection of content was left exclusively to the user.... Matchmaker cannot be considered an "information content provider" under the statute because no profile has any content until a user actively creates it.

2007

Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, No. 04-56916 (9th Cir. 2007) (holding that the CDA does NOT immunize for allegedly discriminatory roommate preferences supplied by users in response to the service's questionnaire). Roommate operates an online roommate matching website at www.roommates.com. The Fair Housing Councils of San Fernando Valley and San Diego ("the Councils") sued, claiming that Roommate violated the Fair Housing Act. The 9th Circuit held, "By categorizing, channeling and limiting the distribution of users' profiles, Roommate provides an additional layer of information that it is 'responsible' at

least ‘in part’ for creating or developing. … Roommate is therefore not ‘responsible, in whole or in part, for the creation or development of’ its users' answers to the open-ended ‘Additional Comments’ form, and is immune from liability for publishing these responses.”

While holding that the service was a "content provider" with respect to the information solicited by its questionnaires, the Court held that the service was immune with respect to the allegedly discriminatory content of user profiles and unguided "additional comments.").

Perfect 10, Inc. v. CCBILL LLC, 488 F.3d 1102 (9th Cir. 2007) (holding that the defendants were eligible for CDA immunity for state law claims of unfair competition, false advertising, and right of publicity claims). Perfect 10, the publisher of an adult entertainment magazine and the owner of the subscription website perfect10.com, alleged that CCBill and CWIE violated copyright, trademark, and state unfair competition, false advertising and right of publicity laws by providing services to websites that posted images stolen from Perfect 10's magazine and website.

Tenth Circuit

2000

Ben Ezra v. American Online, 206 F.3d 980 (10th Cir. 2000). AOL, which operates an interactive computer service, was not an "information content provider" with respect to information published on its stock quotation service, and thus qualified for immunity, against negligence and defamation claims for providing allegedly inaccurate stock information. The plaintiff did not counter evidence that stock information was created solely by third parties. AOL’s efforts to correct errors through deletions and correction requests to third parties was not development or creation of information.

Eleventh Circuit

2006

(affirming the district court’s grant of summary judgment in favor of Amazon and award of attorney’s fees) In 1991 Almeida’s mother gave written permission for Cabral to take pictures of her 10-year-old daughter Almeida, and to use those pictures in an exhibit, in a book, and in promotional material for the book. Almeida’s image was displayed at Cabral’s two-day exhibit, at which the first edition of Anjos Proibidos (“Forbidden Angels”) was offered for sale, displaying black and white photographs of girls between the ages of ten and seventeen, including a photograph of Almeida inside the book. Two hundred copies of the book were sold before the authorities in Sao Paulo seized the remaining copies. Cabral and the book’s publisher, Itamarati Grafica, were prosecuted for producing a work of child pornography, and both were acquitted. In

2002, Almeida discovered that her picture was being displayed on Amazon.com websites in furtherance of the sale of the second edition of Anjos Proibidos. Amazon's product detail page displayed the second edition cover photograph of Almeida and a quote attributed to a ten-year old Almeida: "I really liked Fabio. He's super-cool. I never felt any shame in making the photos."

On November 14, 2003, Almeida filed suit in Miami-Dade County, Florida asserting claims under: (1) the right of publicity statute, Fla. Stat. § 540.08; (2) the civil theft statute, Fla. Stat. § 772.11; and (3) the Florida common law invasion of privacy doctrine. On January 2, 2004, Amazon invoked diversity jurisdiction and removed the case to federal district court. On July 30, 2004, the district court granted Amazon's motion for summary judgment as to all of Almeida's claims. The district court held that Almeida may not recover under section 540.08 because the subject matter of her claim has been preempted by the CDA. Assuming arguendo that the CDA does not preempt the subject matter of Almeida's section 540.08 claim, the district court concluded that Almeida consented to Cabral's use of her image, and, therefore, section 540.08(3)(b) bars application of the statute. Further, the district court dismissed Amazon's invasion of privacy claim on the same basis as the statutory right of publicity claim. As to Almeida's civil theft claim, the district court determined that Almeida failed to establish Amazon's felonious intent by clear and convincing evidence. Finally, the district court awarded Amazon attorney's fees based on Almeida's civil theft claim.

The 11th Circuit held that Almeida's right of publicity claim based on Fla. Stat. § 540.08 would not withstand a motion to dismiss under the law, and that therefore, it was unnecessary for the district court to determine whether the CDA preempts Almeida's state law right of publicity claim.

2. Children's Online Privacy Protection Act of 1998

The Children's Online Privacy Protection Act ("COPPA", 15 U.S.C. § 6501-6504) became effective on April 21, 2000. The FTC enforces this law. This law protects children's privacy by giving parents the tools to control what information is collected from their children online. Under the Act's implementing Rule (codified at 16 C.F.R. § 312.), operators of commercial websites and online services directed to or knowingly collecting personal information from children under 13 must: (1) notify parents of their information practices; (2) obtain verifiable parental consent before collecting a child's personal information; (3) give parents a choice as to whether their child's information will be disclosed to third parties; (4) provide parents access to their child's information; (5) let parents prevent further use of collected information; (6) not require a child to provide more information than is reasonably necessary to participate in an activity; and (7) maintain the confidentiality, security, and integrity of the information.

In order to encourage active industry self-regulation, the Act also includes a "safe harbor" provision allowing industry groups and others to request Commission approval of self-regulatory guidelines to govern participating websites' compliance with the Rule.

2000

F.T.C. v. Toysmart.Com, LLC., 2000 WL 1523287 (D. Mass. 2000). On July 7, 2000, the Federal Trade Commission sued Toysmart.com, LLC, and Toysmart.com, Inc., a failed Internet retailer of children's toys, in the United States District Court for the District of Massachusetts, seeking injunctive and declaratory relief to prevent the sale of confidential, personal customer information collected on the company Web site in violation of its own privacy policy. The complaint alleged that Toysmart, a Delaware company located in Waltham, Massachusetts, that is now in bankruptcy, had violated Section 5 of the FTC Act by misrepresenting to consumers that personal information would never be shared with third parties, and then disclosing, selling, or offering that information for sale. "Even failing dot-coms must abide by their promise to protect the privacy rights of their customers," said Chairman Robert Pitofsky. "The FTC seeks to ensure these promises are kept." The State of Texas' motion to intervene was denied.

2001

On April 21, 2001, the FTC announced the following:

"The FTC charged Monarch Services, Inc. and Girls Life, Inc., operators of www.girlslife.com; Bigmailbox.com, Inc., and Nolan Quan, operators of www.bigmailbox.com; and Looksmart Ltd., operator of www.insidetheweb.com with illegally collecting personally identifying information from children under 13 years of age without parental consent, in violation of the COPPA Rule. To settle the FTC charges, the companies together will pay a total of $100,000 in civil penalties for their COPPA violations. In addition to the requirement that these companies comply with COPPA in connection with any future online collection of personally identifying information from children under 13, the settlements require the operators to delete all personally identifying information collected from children online at any time since the Rule's effective date. These cases mark the first civil penalty cases the FTC has brought under the COPPA Rule."

2002

On April 22, 2002, the second anniversary of the Children's Online Privacy Protection Rule, the Federal Trade Commission announced its sixth COPPA enforcement case, together with new initiatives designed to enhance compliance with the law.

"The Ohio Art Company, manufacturer of the Etch-A-Sketch drawing toy, will pay $35,000 to settle Federal Trade Commission charges that it violated the Children's Online Privacy Protection Rule by collecting personal information from children on its www.etch-a-sketch Web site without first obtaining parental consent. The settlement also bars future violations of the COPPA Rule. This is the FTC's sixth COPPA law enforcement case."

“The FTC alleges that The Ohio Art Company collected personal information from children registering for "Etchy's Birthday Club." The site collected the names, mailing addresses, e-mail addresses, age, and date of birth from children who wanted to qualify to win an Etch-A-Sketch toy on their birthday. The FTC charged that the company merely directed children to "get your parent or guardian's permission first," and then collected the information without first obtaining parental consent as required by the law. In addition, the FTC alleged that the company collected more information from children than was reasonably necessary for children to participate in the "birthday club" activity, and that the site's privacy policy statement did not clearly or completely disclose all of its information collection practices or make certain disclosures required by COPPA. The site also failed to provide parents the opportunity to review the personal information collected from their children and to inform them of their ability to prevent the further collection and use of this information, the FTC alleged.”

2003

Hershey Foods Corp. and Mrs. Fields Cookies settled Federal Trade Commission charges February 26 that their websites violated the Children’s Online Privacy Protection Act. The settlements contain certain record-keeping requirements to allow the FTC to monitor the companies’ compliance. Also, Hershey will pay civil penalties of $85,000, and Mrs. Fields will pay civil penalties of $100,000. These penalties are the biggest civil penalties imposed for COPPA noncompliance.

Many of Hershey’s websites are candy-related sites directed to children. Hershey instructed children under 13 to have their parents fill in an online parental consent form. The company allegedly took no steps to ensure that a parent or guardian saw or filled out the consent forms. Apparently the company collected personal information--including full name, home address, e-mail address, and age--from children.

Apparently portions of the Mrs. Fields Web sites--mrsfields.com, pretzeltime.com, and pretzelmaker.com--were directed to children. These pages offered birthday clubs for children 12 or under and provided birthday greetings and coupons for free cookies or pretzels. The company allegedly collected personal information--including full name, home address, e-mail address, and birth date--from more than 84,000 children without first obtaining parental consent.

3. Children's Internet Protection Act

This law, known as “CIPA”, is found at 20 U.S.C. § 9134 & 47 U.S.C. 254.

Supreme Court

2003

A group of public libraries, library associations, library patrons, and Web site publishers challenged the constitutionality of the Children's Internet Protection Act (CIPA), which required public libraries to use anti-pornography Internet filters as a condition for receipt of federal subsidies. The Philadelphia district court held that CIPA unconstitutionally induced libraries to violate the First Amendment, and that CIPA's disabling provision was insufficient to cure the constitutional defect. *American Library Ass'n, Inc. v. U.S.*, 201 F.Supp.2d 401 (E.D. Pa. 2002), *cert granted*, November 12, 2002. On November 12, 2002, the Supreme Court agreed to hear the government's appeal. On June 23, 2003, The U.S. Supreme Court, on a 6-3 vote, ruled that public library Internet anti-pornography filters are not a violation of the First Amendment, even if the filters block some legitimate sites, reversing the district court's ruling, stating:

> Most libraries already exclude pornography from their print collections because they deem it inappropriate for inclusion. We do not subject these decisions to heightened scrutiny; it would make little sense to treat libraries' judgments to block online pornography any differently, when these judgments are made for just the same reason.
>
> Like the District Court, the dissents fault the tendency of filtering software to "overblock"--that is, to erroneously block access to constitutionally protected speech that falls outside the categories that software users intend to block. … Assuming that such erroneous blocking presents constitutional difficulties, any such concerns are dispelled by the ease with which patrons may have the filtering software disabled. When a patron encounters a blocked site, he need only ask a librarian to unblock it or (at least in the case of adults) disable the filter. As the District Court found, libraries have the capacity to permanently unblock any erroneously blocked site. … With respect to adults, CIPA also expressly authorizes library officials to "disable" a filter altogether "to enable access for bona fide research or other lawful purposes." … The District Court viewed unblocking and disabling as inadequate because some patrons may be too embarrassed to request them. … But the Constitution does not guarantee the right to acquire information at a public library without any risk of embarrassment.
>
> Because public libraries' use of Internet filtering software does not violate their patrons' First Amendment rights, CIPA does not induce libraries to violate the Constitution, and is a valid exercise of Congress' spending power. Nor does CIPA impose an unconstitutional condition on public libraries. *U.S. v. American Library Ass'n, Inc.,* No. 02-361, 539 U.S. 194 (June 23, 2003).

The Federal Communications Commission then set a July 1, 2004, deadline for libraries to comply with the Children's Internet Protection Act.

4. TLD kids.us

On December 4, 2002, President George W. Bush signed into law the "Dot Kids Implementation and Efficiency Act of 2002," Public Law No. 107-317 ("Dot Kids Act"), requiring the United States Department of Commerce to establish a second level

domain within the ".us" domain to provide access to material that is suitable for, and not harmful to, minors.

On February 13, 2003, NeuStar, Inc. was appointed to be the administrator of the kids.us domain name space by the Department of Commerce, pursuant to Modification No. 7 to the usTLD Agreement between kids.us Administrator and the Department of Commerce (Order No. SB1335-02-W-0175) dated February 13, 2003, to operate a shared registration system, TLD nameservers, and other equipment for the "kids.us" second-level domain.

NeuStar operated a kids.us Sunrise period June 17-August 15, 2003 for owners of existing or pending United States trademarks or service marks to apply for kids.us domain names that exactly match their trademarks or service marks.

NeuStar states the following in its "Kids.Us Administrator-Registrar Agreement", located at www.kids.us:

> Kids.us is an Internet domain that parents--and children under 13--can trust for appropriate online activity. It's the first and only "youth-friendly" Web space to be established by the United States government, and it features advanced technical, policy and operational mechanisms that keep young people informed, entertained, and protected online. …
>
> All Registrants seeking to obtain an Active Registration must also agree to abide by the Content Policy, attached hereto as Exhibit A.

Exhibit A

Specifically, the kids.us domain is designed to restrict access to content that is "harmful to minors", which has been defined by the kids.us Act as:

> "The average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, that it is designed to appeal to, or is designed to pander to, the prurient interest;
>
> The material depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
>
> Taken as a whole, the material lacks serious, literary, artistic, political, or scientific value for minors."

Further, the kids.us Act also states that the domain should have content that is "suitable for minors", or content that:

> "Is not psychologically or intellectually inappropriate for minors; and Serves (1) the educational, informational, intellectual, or cognitive needs of minors; or (2) the social, emotional, or entertainment needs of minors."

KIDS.US GUIDELINES AND RESTRICTIONS

- Compliance with existing rules and regulations regarding indecency on the airwaves
- A commitment to offer some educational and informational content
- Compliance with the children's online privacy protection act (COPPA) requirements 10
- Compliance with children's advertising review unit (CARU) advertising standards [of the BBB]

The following information or content is not permitted within the kids.us domain:

Mature content—actual and/or simulated normal or perverted sexual acts or sexual contact; sexually explicit information that is not of medical or scientific nature which includes

- Discussion or descriptions of sexual techniques or exercises;
- Sexual paraphernalia;
- Explicit discussions of sex and sexuality; and
- Lewd clothing sales.

Pornography—content that is sexually explicit and/or has a purpose of arousing a sexual or prurient interest which includes

- Lewd exhibitions of genitals or post-pubescent female breasts;
- Pornographic fiction or erotica;
- Sex-related phone and video information;
- Adult services (e.g., escort services, exotic dancers);
- Personals or dating services;
- Fetish information or clothing; and
- Sex toys.

Inappropriate language—use of profane, indecent, pornographic or sexually-related language, including the seven words identified in *Federal Communications Commission v. Pacifica Foundation, 438 U.S. 726, 98 S. Ct. 3026, 57 L.Ed.2d 1073 (1978)* in the domain name or content of any kids.us website

Violence—content which advocates or provides instructions for causing physical harm to people, animals or property, which includes

- Information or instructions for injuring or killing people or animals;
- Explosives and bombs – manufacturing, obtaining materials, transport and detonation;
- Graphic images of blood and gore with no medical or scientific purpose;
- Destructive mischief, pranks or practical jokes; and
- Dangerous chemistry, physics and engineering.

Hate speech—content with hostility or aggression toward an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics OR denigrates others on the basis of these characteristics or justifies inequality on the basis of those characteristics. This includes

- Racism;
- Religious-based hate speech, such as anti-Semitism; □
- Misogyny;
- Race-based separatism; and
- Ageism.

Drugs—content that advocates the illegal use of drugs, or abuse of over-the-counter or prescription medications. This includes

- Direct or indirect sale of illegal substances;
- Narcotic paraphernalia;
- Manufacture of illegal substances (organic or chemical);
- Abuse of over-the-counter or prescription drugs or medical treatments;
- Direct or indirect distribution of illegal substances; and
- Use of illegal substances.

Alcohol—content that advocates or contemplates alcohol consumption which includes

- Offers for sale;
- Supplies recipes for creating, encouraging or guidance on consumption;
- Paraphernalia to make or consume; and
- Drinking games or other recreational displays.

Tobacco—content that features smoking or use of other tobacco products, which includes

Retailers or other means of acquiring;
Tobacco products and paraphernalia;
Instructions for using tobacco products; and
Glamorization of tobacco use.

Gambling—content that advocates legal or illegal gambling, which includes

Online Casinos, lotteries, gaming or online betting sites;
Information or tips for placing bets of handicapping; and
Fundraisers that use gambling.

Weapons—content that sells or advocates the use of weapons, which includes

Direct sale or information on the procurement of firearms, ammunition, any firearm accessories, sport knives, and martial arts weapons; and
Information on use or modification of firearms, ammunition, any firearm accessories, sport knives, and martial arts weapons.

Criminal activities—content that advocates or provides information or instruction for engaging criminal activity, which includes

Theft;
Bodily harm;
Property damage; and
Computer-related crimes.

Notwithstanding the list contained above, all content will be reviewed by the Content Manager(s) on the whole prior to being approved for display on a kids.us domain. If such content is deemed by the Content Manager(s) and/or NeuStar as having serious educational, informational, intellectual, literary, artistic, political, or scientific value for minors, we believe that exceptions can be made to allow this content to appear in the kids.us domain.

E. Deceptive Acts 15 U.S.C.§ 45(a)

Section 5(a) of the FTC Act, 15 U.S.C.§ 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce".

1. Hijacking & Mousetrapping Internet Surfers

"Hijacking" works in the following way. Surfers who look for a site but misspell its Web address or invert a term - using cartoonjoe.com, for example, rather than joecartoon.com - are taken to a site to which they had not intended to go.

"Mousetrapping" is using special programming code at a website to obstruct surfers' ability to close their browser or go back to the previous page. Clicks on the "close" or "back" buttons causes new windows to open.

Third Circuit

2002
E.D. Pa.

Federal Trade Commission v. Zuccarini, 2002 WL 1378421, 2002-1 Trade Cases P 73,690 (E.D. Pa. 2002). On September 25, 2001, the Federal Trade

Commission sued John Zuccarini under 15 U.S.C.§ 45(a) for hijacking and mousetrapping. The complaint charged that Zuccarini had set up more than 5,500 websites, using common misspellings of famous names like Victoria's Secret and the Wall Street Journal. (Zuccarini had websites with 41 variations on the name of Britney Spears.) By misspelling a web address, Internet surfers were taken to one of Zuccarini's websites, where they then were bombarded with a rapid series of windows displaying ads for goods and services ranging from Internet gambling to pornography. In some cases, the legitimate Web site the consumer was attempting to access also was launched, so consumers thought the hailstorm of ads to which they were being exposed was from a legitimate Web site. After one FTC staff member closed out of 32 separate windows, leaving just two windows on the task bar, he selected the "back" button, only to watch the same seven windows that initiated the blitz erupt on his screen, and the cybertrap began anew.

The Court entered a permanent injunction, barring the defendant from: redirecting or obstructing consumers on the Internet in connection with the advertising, promoting, offering for sale, selling, or providing any goods or services on the Internet, the World Wide Web or any Web page or Web site; and launching the Web sites of others without their permission. Zuccarini was ordered to pay $1,897,166. The court also ordered certain bookkeeping and record-keeping requirements to allow the FTC to monitor the defendant's compliance with the court's order.

2. Other Unfair & Deceptive Acts

The FTC has also pursued entities for using the Internet for such activities as:

selling fraudulent "kits" to become paralegals, *F.T.C. v. Para-Link Int'l, Inc.*, 2001 WL 1701537, 2001-2 Trade Cases P 73,507 (M.D. Fla. 2001),.

a multi-level marketing scheme involving the sale of a work-from-home business opportunity called a "Web Pak", *F.T.C. v. Skybiz.com, Inc.*, 2001 WL 1673645, 2001-2 Trade Cases P 73,496 (N.D. Okla. 2001),.

billing telephone line subscribers for Internet access, whether or not they actually accessed or authorized access to pornographers' web sites, *F.T.C. v. Verity Int'l, Ltd.,* 194 F.Supp.2d 270, 2002-2 Trade Cases P 73,722 (S.D.N.Y. 2002), and

not giving promised rebates. *Federal Trade Commission v. UrbanQ*, Civ. No. CV-0333147 (E.D.N.Y. 6/26/03).

From the FTC's website, http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm, comes this warning:

> **How Not to Get Hooked by a 'Phishing' Scam**
>
> Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing".

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization that you deal with – for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC, the nation's consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.

- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

- Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.
  A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system

(like Windows or Linux) may offer free software “patches” to close holes in the system that hackers or phishers could exploit.

- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.

- Report suspicious activity to the FTC. If you get spam that is phishing for information, forward it to spam@uce.gov. If you believe you’ve been scammed, file your complaint at www.ftc.gov, and then visit the FTC’s Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.

Also from the FTC's website comes this 2004 announcement about phishing:

In a joint law enforcement initiative, the Federal Trade Commission and the Department of Justice have brought two separate actions to shut down a spam operation that hijacked logos from AOL and Paypal to con hundreds of consumers into providing credit card and bank account numbers. At the request of the FTC, a U.S. District Court ordered the defendant to halt his identity theft scam, known as “phishing.” The Justice Department obtained a criminal conviction and the defendant is awaiting sentencing.

The scam worked like this: Consumers received e-mail that appeared to come from America Online or Paypal. The “from” line identified the sender as “billing center,” or “account
department” and the subject line carried warnings such as “AOL Billing Error Please Read Enclosed Email,” and “Please Update Account Information Urgent!” The text of the message contained a warning that if the consumers did not respond to the e-mail, their account would be cancelled. Some of the spam said, “. . . we have to ask all our members for updated/correct billing information. Please be advised that this is mandatory. If we do not get your updated billing information, your account will be revoked and put under review and may be cancelled.” A hyperlink in the e-mail took consumers to what appeared to be the AOL Billing Center, with AOL’s logo and live links to real AOL Web pages. But the copy-cat Web page belonged to the defendant. The defendant asked consumers to provide information such as their names and mothers’ maiden names, billing addresses, Social Security numbers, dates of birth, bank account numbers, and bank routing numbers. The defendant also asked consumers to provide their AOL screen names and passwords.

F. Crimes

A good lawyer should be aware of these Internet crimes for at least two reasons: first, to counsel your clients against walking too close to the edge of the abyss, and second, to gain insight from the DOJ’s prosecution of certain Internet crimes that have parallel civil causes of action.

The federal government has a website devoted to crimes on the Internet: www.cybercrime.gov. This website is maintained by the U.S. Department of Justice, Criminal Division, Computer Crime & Intellectual Property Section ("CCIPS").

1. Trafficking in Counterfeit Labels: 18 U.S.C. § 2318

18 U.S.C. §2318 provides, in pertinent part:

(a) Whoever, in any of the circumstances described in subsection (c) of this section, knowingly traffics in a counterfeit label affixed or designed to be affixed to a phonorecord, or a copy of a computer program or documentation or packaging for a computer program, or a copy of a motion picture or other audiovisual work, and whoever, in any of the circumstances described in subsection (c) of this section, knowingly traffics in counterfeit documentation or packaging for a computer program, shall be fined under this title [$250,000] or imprisoned for not more than five years, or both.

The DOJ's manual for prosecuting intellectual property crimes states the following about this felony provision, which Congress amended in 1996:

> The current law continues that broad coverage, permitting a case to be proven even without evidence of copyright so long as, for example, the mail or a facility of interstate or foreign commerce is used in the commission of the offense.
>
> Many copyright infringement crimes make use of counterfeit labels. And, in some cases, it can be easier for the government to prove the counterfeit labeling count than the copyright infringement count. For example, the counterfeit labeling crime does not require proof of infringement, i.e., actual copying or distribution; it is enough to show that the defendant was "trafficking." In addition, a counterfeit labeling case requires proof of only a "knowing" mental state, rather than a "willful" mental state.

2. Piracy of Copyrighted Works 18 U.S.C. § 2319

18 U.S.C. §2319 provides, in pertinent part:

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under section 506(a)(1) of title 17--

> (1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution,

including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

3. Trafficking In Counterfeit Goods Or Services

"Whoever intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services shall, if an individual, be fined not more than $2,000,000 or imprisoned not more than 10 years, or both, and, if a person other than an individual, be fined not more than $5,000,000. In the case of an offense by a person under this section that occurs after that person is convicted of another offense under this section, the person convicted, if an individual, shall be fined not more than $5,000,000 or imprisoned not more than 20 years, or both, and if other than an individual, shall be fined not more than $15,000,000." 18 U.S.C. § 2320(a).

The definition of a "counterfeit mark" in Section 2320(e)(1)(A) is based on the definition of "counterfeit" from 15 U.S.C. § 1127: a "spurious mark that is identical with, or substantially indistinguishable from, a mark registered . . ." However, it includes two additional elements: (1) the mark must be "used in connection with trafficking in goods or services"; and (2) the counterfeit mark must be used on those goods or services for which the genuine mark is registered on the Principal Register in the Patent and Trademark Office.

1999

Aoki Lee (Honolulu, 1999). Lee was charged by a federal grand jury on December 9, 1999, with infringing the trademark of the Honolulu Marathon Association (HMA). The HMA maintains a domain name called www.honolulumarathon.org, where residents of the U.S. can register for the marathon. Japanese residents, on the other hand, are told they must register in person at an office in Japan.

Lee took most of the content of the authorized website and placed it at a domain name he registered: www.honolulumarathon.com. He purported to offer Japanese runners the opportunity to register via the website, for a fee $100 more than the actual registration amount. Lee was also charged with selling these services through the use of counterfeit marks which he copied from the authorized website.

(Lee was also charged with selling Viagra over the Internet without a prescription.) The FBI shut down Lee's website after its investigation.

Lee pleaded guilty to one count of wire fraud and one count of selling Viagra without a prescription. The main issue at sentencing was whether the district court could impose the special skills adjustment based on Lee's use of computer skills in creating his phony site. The district court found that Lee "was skilled at accessing and manipulating computer systems" and imposed the special skills enhancement. The adjustment raised the guideline sentencing range from six to twelve months to ten to sixteen months. This increase deprived the district court of the sentencing option of imposing no imprisonment. On appeal, the Ninth Circuit reversed and remanded, holding that imposition of special skills sentencing enhancement was not warranted. *U.S. v. Lee*, 296 F.3d 792 (9th Cir. 2002).

2002

Chan, Chao, Chellberg, Jin, Zheng, Kuo, Lei, Wang, Ly, Zhang, Wu, Yang, Wang, Wu, et. al. (San Jose, CA)

The United States Attorney's Office for the Northern District of California and the Federal Bureau of Investigation announced that 27 people were arrested April 18, 2002, in a coordinated takedown of a large, loosely affiliated group of dealers in counterfeit software in the Bay Area. Eight of the 11 indictments are a direct result of the undercover operation dubbed "Cyberstorm". The undercover operation, which began in 2000, sought to identify dealers in counterfeit software. Each of the defendants listed in Indictments 1-8 are alleged to have sold counterfeit software to an undercover agent. The indictments charge that each of the defendants trafficked in counterfeit goods and committed criminal copyright infringement. (18 U.S.C. §§ 2319 & 2320) In addition, some of the individuals are charged with conspiracy, money laundering or structuring cash transactions to evade reporting requirements.

Affidavits filed in the case allege that the defendants in Indictments 1 through 8 sold counterfeit software such as Microsoft Windows 98 or Microsoft Office 2000. Posing undercover, a police officer held himself out as a businessman engaged in buying and selling computer software and computer components. While legitimate copies of the software sold for between $200 and $600 in stores, the defendants sold the counterfeit software for between $7 and $70. Most of the transactions were done in cash and completed either at the defendants' homes or in parking lots adjacent to shopping centers. Altogether, according to statements made in court, the total retail value of the software purchased from these defendants throughout the course of the undercover operation would have exceeded $5 million, if the software had been legitimate.

4. Computer Fraud And Abuse 18 U.S.C. § 1030

The Computer Fraud And Abuse statute, 18 U.S.C. § 1030, makes it a crime, among other things, if anyone "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030a)(5). Subsection (5)(A)(i) prohibits anyone from knowingly damaging a computer (without authorization) while subsection (5)(A)(ii) prohibits unauthorized users from causing damage recklessly and subsection (5)(A)(iii) from causing damage negligently.

Section 1030(g) allows for civil actions by "any person who suffers damage or loss by reason of a violation of this section" to obtain "compensatory damages and injunctive relief or other equitable relief".

The USA PATRIOT Act, enacted on October 26, 2001, essentially adopted the Ninth Circuit's 2000 *Middleton* definition of loss in 18 U.S.C. § 1030(e)(11). The term "loss" was then defined by that statute to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

First Circuit

2001

EF Cultural Travel BV v. Explorica, 274 F.3d 577 (1st Cir. 2001) (awarding costs of assessing damage). Once the defendant's expert "scraped" all of the plaintiff's prices off of the plaintiff's website, it sent a spreadsheet containing EF's pricing information to Explorica, which then systematically undercut EF's prices. The district court granted a preliminary injunction. On appeal, the court held that use of the "scraper" program "exceeded authorized access" within the meaning of the CFAA, assuming that the program's speed and efficiency depended on the executive's breach of his confidentiality agreement with his former employer.

Second Circuit

2001

United States v. Ivanov, 175 F.Supp.2d 367 (D. Conn. 2001) (proving that the threat was transmitted in interstate or foreign commerce is sufficient). Section 1030(a)(7) does not require proof that the defendant delayed or obstructed commerce. The defendant hacked into the victim's network and obtained root access to the victim's servers. He then proposed that the victim hire him as a "security expert" to prevent further security breaches, including the deletion of all of the files on the server.

2002

***U.S. v. Harris*,** 302 F.3d 72 (2nd Cir. 2002). The defendant was arrested after she gained access to her employer's computer without authorization, in order to obtain the Social Security numbers of individuals who were the targets of a credit-card fraud scheme. Pursuant to a plea agreement, she waived indictment, and pled guilty to a one-count information accusing her of violating 18 U.S.C. § 1030(a)(2)(B). On appeal from her sentence, the Second Circuit held that the district court did not meet the requirement of an affirmative act or statement allowing an inference that the district court had considered the defendant's ability to pay restitution.

2004

Register.com, Inc. v. Verio, Inc., 126 F.Supp.2d 238 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004). A company created an automated program to access its competitor's web server—a publicly available computer—in violation of the competitor's terms of use. Even though the company that created the automated program did not circumvent any security feature and could lawfully have accessed the site if it did so without using automated programs, the court held that this activity constituted "unauthorized access" for purposes of section 1030(a)(5). *Id.* at 251-52.

I.M.S. Inquiry Management Systems v. Berkshire Information Systems, 307 F.Supp.2d 521, 525-26 (S.D.N.Y. 2004) (allegation, that the integrity of copyrighted data system was impaired by defendant's copying it, was sufficient to plead cause of action under CFAA).

Third Circuit

2001

U.S. v. Lloyd, 269 F.3d 228 (3d Cir. 2001). The government alleged that Lloyd, an Omega employee, planted a computer "time bomb" in the central file server of Omega's computer network while employed there, and that the "time bomb" detonated after he was fired from the company. A jury convicted him on one count of computer sabotage, a violation of the CFAA. After one of the jurors advised the court that she had learned from the media during the course of deliberations about off-site computer sabotage, the district court granted Lloyd's motion for a new trial. The government appealed. The Third Circuit found no evidence to suggest that Lloyd was prejudiced substantially by a juror's exposure to the story of the "Love Bug" virus, and concluded that the district court abused its discretion in granting a new trial

2006

HUB Group, Inc. v. Clancy, 2006 WL 208684 (E.D. Pa. 2006) (downloading employer's customer database to a thumb drive for use at a future employer created sufficient damage to state claim under the CFAA).

Fourth Circuit

2002

U.S. v. Sullivan, 40 Fed.Appx. 740, 2002 WL 312773 (4th Cir. 2002). Sullivan, a computer programmer, upon getting upset with his employer, Lance, Inc., inserted a computer code (a "logic bomb") into the software he had prepared for Lance. The code was designed to disable a communication function in Lance's hand-held computers. Sullivan then quit without telling anyone about the bomb. The bomb went off about four months later, disabling 824 hand-held computers used by Lance's sales representatives to communicate with the headquarters. Shortly thereafter, when confronted by the FBI, Sullivan confessed to planting the bomb. Sullivan was convicted for intentionally causing damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A). He appealed the admission of evidence seized from his home, and the denial of his motion for judgment of acquittal. In an unpublished opinion, the Fourth Circuit held that evidence seized from his home computer properly came in under Federal Rule of Evidence 404(b) to show "proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident."

Fifth Circuit

2006

Fiber Sys. Int'l v. Roehrs, 470 F.3d 1150 (5th Cir. 2006).

> In Roehrs, the Fifth Circuit confirmed an expanded view of causes of action available under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"). The dispute involved an hostile family struggle over control of fiber-optic business. The principal parties were Plaintiffs Michael Roehrs/Fiber Systems International, Inc. ("FSI") and Defendants Daniel Roehrs/Optical Cabling Systems ("OCS"). An earlier dispute between the parties was settled with an agreement for FSI to buy out Daniel Roehrs and other minority shareholders' stake in the company. In this case, FSI sued OCS and other individual defendants for violations of the CFFA, which criminalizes acts relating to fraudulent or damaging conduct involving computer use. FSI argued that defendants "stole FSI's confidential business and proprietary information and trade secrets, without authorization, from FSI's computers," misappropriated and stole FSI's computer equipment, and used and disseminated the wrongfullyobtained information through the new company that they formed [OCS]. FSI sought damages and injunctive relief under the CFAA. In response, Defendants (OCS as well as the individual defendants) filed a defamation counterclaim against FSI for falsely accusing them of being thieves.
>
> Among the issues on appeal was the district court's determination that the CFAA's § 1030(a)(4) did not create a civil cause of action. The defendants argued, and the district court agreed, that a civil cause of action did not exist based on the language of the CFAA's damage provision (18 U.S.C. § 1030(g)) which states: Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil

action for a violation of this section may be brought only if the conduct involves one of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B) . . . . The district court interpreted this provision narrowly to mean that only a subsection (a)(5) violation resulted in civil liability.

The Fifth Circuit disagreed, holding that while § 1030(g) refers only to subsection (a)(5), it does not limit CFAA civil suits to subsection (a)(5) violations. Instead, all that is required to maintain a CFAA civil suit is a finding of conduct that violates one of the factors set forth in subsection (a)(5)(B); under the Court's analysis, a section 1030(a)(4) violation could include a violation of one of these factors. In doing so, the court noted that this interpretation as to the scope of civil suits available under the CFAA was consistent with previous decisions of the Third and Ninth Circuits.

2007

Hewlett-Packard Co. v. Byd:sign, Inc., 2007 U.S. Dist. LEXIS 5323 (E.D. Tex. 2007) (denying defendants' motion to dismiss HP's CFAA claims). The individual defendants were at one time either employees or contractors working for HP or for one of its predecessors, Compaq Computer Corporation. HP alleged that they conspired to use their positions of trust and confidence at HP to obtain trade secrets and other proprietary information from HP and then illegally funneled those secrets, and HP's corporate opportunities, to an enterprise founded by several of them. HP further alleged that the defendants acted without authorization, or exceeded their authorized access, when they used HP's computers to further their fraudulent scheme against HP, and attempted to "scrub" their computers, thereby damaging or deleting HP information.

United States v. Phillips, 477 F.3d 215 (5th Cir. 2007) (affirming his conviction for intentionally accessing a protected computer without authorization and recklessly causing damage in excess of $ 5,000).

Phillips entered the University of Texas at Austin ("UT") in 2001 and was admitted to the Department of Computer Sciences in 2003. Like all incoming UT students, Phillips signed UT's "acceptable use" computer policy, in which he agreed not to perform port scans using his university computer account. Nonetheless, only a few weeks after matriculating, Phillips began using various programs designed to scan computer networks and steal encrypted data and passwords. He succeeded in infiltrating hundreds of computers, including machines belonging to other UT students, private businesses, U.S. Government agencies, and the British Armed Services webserver. In a matter of months, Phillips amassed a veritable informational goldmine by stealing and cataloguing a wide variety of personal and proprietary data, such as credit card numbers, bank account information, student financial aid statements, birth records, passwords, and Social Security numbers.

“Port scanning” is a technique used by computer hackers by which an individual sends requests via a worm or other program to various networked computer ports in an effort to ascertain whether particular machines have vulnerabilities that would leave them susceptible to external intrusion. Often used as an initial step in launching an attack on another computer or transmitting a virus, port scanning is a relatively unsophisticated, but highly effective, reconnaissance method, likened at trial by UT's information technology chief as the electronic equivalent of "rattling doorknobs" to see if easy access can be gained to a room.

The scans, however, were soon discovered by UT's Information Security Office ("ISO"), which informed Phillips on three separate occasions that his computer had been detected port scanning hundreds of thousands of external computers for vulnerabilities. Despite several instructions to stop, Phillips continued to scan and infiltrate computers within and without the UT system, daily adding to his database of stolen information.

At around the time ISO issued its first warning in early 2002, Phillips designed a computer program expressly for the purpose of hacking into the UT system via a portal known as the "TXClass Learning Central: A Complete Training Resource for UT Faculty and Staff." TXClass was a "secure" server operated by UT and used by faculty and staff as a resource for enrollment in professional education courses. Authorized users gained access to their TXClass accounts by typing their Social Security numbers in a field on the TXClass website's log-on page. Phillips exploited the vulnerability inherent in this log-on protocol by transmitting a "brute-force attack" program, which automatically transmitted to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized TXClass users.

"Brute-force attack" is term of art in computer science used to describe a program designed to decode encrypted data by generating a large number of passwords.

Initially, Phillips selected ranges of Social Security numbers for individuals born in Texas, but he refined the brute-force attack to include only numbers assigned to the ten most populous Texas counties. When the program hit a valid Social Security number and obtained access to TXClass, it automatically extracted personal information corresponding to that number from the TXClass database and, in effect, provided Phillips a "back door" into UT's main server and unified database. Over a fourteen-month period, Phillips thus gained access to a mother lode of data about more than 45,000 current and prospective students, donors, and alumni.

Phillips's actions hurt the UT computer system. The brute-force attack program proved so invasive -- increasing the usual monthly number of unique requests received by TXClass from approximately 20,000 to as many as 1,200,000 -- that it caused the UT computer system to crash several times in early 2003.

Hundreds of UT web applications became temporarily inaccessible, including the university's online library, payroll, accounting, admissions, and medical records. UT spent over $ 122,000 to assess the damage and $ 60,000 to notify victims that their personal information and Social Security numbers had been illicitly obtained.
After discovering the incursions, UT contacted the Secret Service, and the investigation led to Phillips. Phillips admitted that he designed the brute-force attack program to obtain data about individuals from the UT system, but he disavowed that he intended to use or sell the information.

Seventh Circuit

2000

YourNetDating v. Mitchell, 88 F.Supp.2d 870, 871 (N.D. Ill. 2000) (granting temporary restraining order where defendant installed code on plaintiff's web server that diverted certain users of plaintiff's website to pornography website).

2006

International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 419-20 (7th Cir. 2006). A civil complaint stated a claim when it alleged that the defendant copied a secure-erasure program to his (company-issued) laptop, and even said in dicta that it made no difference if the defendant copied the program over an Internet connection, from an external disk drive, or an internal disk drive.

Eighth Circuit

2006

United States v. Millot, 433 F.3d 1057 (8th Cir. 2006) (affirming a sentence under the CFAA of three months imprisonment, three months home detention, three years supervised release, a $5,000 fine, and restitution in the amount of $20,350). In 2000, Millot worked as a systems analyst in the Information Access Management Group for Aventis Pharmaceuticals. In October of 2000, Aventis Pharmaceuticals outsourced its security functions to IBM. Millot was not offered a job with IBM, and left employment with Aventis in September 2000. When he left employment, he kept the SecureID card he had previously assigned to an ex-employee Fromm. On December 16, 2000, he used the SecureID card and the Fromm account to log onto the Aventis system and delete an account. The person whose account he deleted was the manager of Technical Services for Aventis. Although IBM was able to rebuild the account within a matter of hours, the affected person continued to experience problems with his account for the following three weeks. Investigators later traced the unauthorized remote access back to Millot's personal internet access account, and Millot confessed to what he had done.

Ninth Circuit

2000

Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1126-27 (W.D. Wash. 2000) (accessing and copying private data may cause damage to the data under the CFAA). A self-storage company hired away a key employee of its main competitor. Before the employee left to take his new job, he emailed copies of computer files containing trade secrets to his new employer. In support of a motion for summary judgment as to the section 1030(a)(5) count, the defendant argued that the plaintiff's computer system had suffered no "damage" as a consequence of a mere copying of files by the disloyal employee. The court, however, found the term "integrity" contextually ambiguous, and held that the employee did in fact impair the integrity of the data on the system—even though no data was "physically changed or erased" in the process—when he accessed a computer system without authorization to collect trade secrets.

United States v. Middleton, 231 F.3d 1207, 1213-14 (9th Cir. 2000) (part of the damage consisted of a user increasing his permissions on a computer system without authorization).

2004

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004) (affirming dismissal of a Wiretap Act claim, and reversing a dismissal with prejudice of a Computer Fraud and Abuse Act claim, with instructions to dismiss with leave to amend to allege damages or loss).

During the course of commercial litigation between Integrated Capital Associates (ICA) and Farey-Jones, Farey-Jones ordered his lawyer to subpoena ICA's ISP and obtain a number of emails. Upon receipt of the subpoena, ICA's ISP posted a sampling of ICA emails on its website, many of which were privileged and personal. ICA employees then filed a civil suit against Farey-Jones and his counsel claiming, inter alia, violation of the Wiretap Act and the Computer Fraud and Abuse Act.

Regarding the Wiretap Act, the Ninth Circuit reiterated that Konop applies to only "acquisition contemporaneous with transmission" and held that Congress did not intend the term "intercept" to apply to electronic communications in electronic storage. The Court upheld the district court's dismissal of the Wiretap claim.

Under the Computer Fraud and Abuse Act, the Ninth Circuit held that the Act's civil remedies extend to "[a]ny person who suffers damage or loss by reason of a violation of this section." The district court had dismissed the Computer Fraud and Abuse Act claims on the theory that the Act does not apply to "unauthorized use of a third party's computer." The Ninth Circuit instead interpreted the Act broadly to include harm suffered by individuals other than the computer's owner, particularly if they have rights to data stored on the computer.

5. Digital Millennium Copyright Act

This law, known as the "DMCA", is found at 17 U.S.C. §1201(b), and prohibits the sale of products that may be used to "circumvent a technological measure that effectively controls access to a work" protected by the copyright statute. See also the earlier description of this law under the discussion of the civil causes of action, in the copyright section of this paper.

Ninth Circuit

2002

N.D. Calif.

United States v. Elcom, 203 F.Supp.2d 1111 (N.D. Cal. 2002). Defendant Elcomsoft Company Ltd. ("Elcomsoft") developed and sold a product known as the Advanced eBook Processor ("AEBPR"). AEBPR is a Windows-based software program that allows a user to remove use restrictions from Adobe Acrobat PDF files and files formatted for the Adobe eBook Reader. The program allows a purchaser of an eBook Reader formatted electronic book to convert the format to one that is readable in any PDF viewer without the use restrictions imposed by the publisher. Defendant Dmitry Sklyarov was the author of the Advanced eBook Processor.

Sklyarov was arrested July 16, 2001, after a hacker conference in Las Vegas, Nev., and charged with five counts of copyright violations in the first criminal complaint under the Digital Millennium Copyright Act ("DMCA"). He was indicted for alleged violations of Section 1201(b)(1)(A) and (C) of the DMCA, 17 U.S.C. §§1201(b)(1)(A) and (C). Sklyarov contended that Section 1201(b) is unconstitutionally vague as applied to itself because it did not clearly delineate the conduct that it prohibits. Specifically, Sklyarov argued that the DMCA bans only those tools that are primarily designed to circumvent usage control technologies in order to enable copyright infringement. In response, the court held, "Nothing within the express language would permit trafficking in devices designed to bypass use restrictions in order to enable a fair use, as opposed to an infringing use. The statute does not distinguish between devices based on the uses to which the device will be put. Instead, all tools that enable circumvention of use restrictions are banned, not merely those use restrictions that prohibit infringement."

Sklyarov also argued that the DMCA violates the First Amendment as applied to the sale of the AEBPR, that the DMCA violates the First Amendment because it infringes the First Amendment rights of third parties, and that the DMCA violates the First Amendment because it is impermissibly vague. The Court rejected all three of those arguments. The case against him and his software company was dismissed December 17, after a jury found them not guilty of those five counts of copyright violations. *U.S. v. Elcom Ltd.*, No. CR-01-20138 (N.D. Calif. December 17, 2002).

6. No Electronic Theft Act

The No Electronic Theft Act ("NET", 17 U.S.C. § 506(a)(2), 18 U.S.C. § 2319(c)) became law on December 16, 1997. The NET changed the law to create a cause of action against those who pirate copyrighted materials, regardless of whether they seek a profit from their actions. This change addressed the increasing number of computer users copying software and other material without thought of monetary gain, but merely out of a desire to distribute the material to other users. The NET Act provides for punishment when a person has willfully produced or distributed one or more illegal copies, with a total retail value of more than $1,000, during any 180-day period. If more than 10 copies have been distributed within 180 days, and the combined retail value is greater than $2500, the crime rises to the level of a felony.

> (c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code -
>
> > (1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;
> >
> > (2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
> >
> > (3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000. 17 U.S.C. § 506(a)(2), 18 U.S.C. § 2319(c); s*ee also* http://www.usdoj.gov/criminal/cybercrime/ip.html.

Seventh Circuit

2003

U.S. v. Slater, 348 F.3d 666 (7th Cir. 2003) (affirming convictions). The defendants, Jason Slater and Christian Morley, belonged to "Pirates With Attitudes" (PWA). During the sentencing hearing, the district court utilized the upward adjustment provision of the 1998 Sentencing guidelines, as the retail loss exceeded $2000. Morley was sentenced to 24 months imprisonment and Slater to eight months imprisonment and six months community custody.

On appeal, Morley and Slater raised two issues – (1) that the PWA's use of the copyrighted software fell within the fair use exception and (2) that the district court's valuation of the infringing items was clearly erroneous.

Under the fair use claim, Morley urged the court to find the PWA's site "noncommercial". The court rejected this argument because users of the site, though not required to contribute money in order to obtain the software, had to, in essence, barter valuable services to receive the software. Morley's second assertion, that the site was "educational" because the site was supported by a university professor – was also struck down by the court.

Slater contested the district court's valuation of the infringing items. In non-software cases, courts have calculated the value of infringing items based on their retail value on the black market. Slater claimed that since the members paid nothing to download the programs, the retail value of the programs on the black market was zero. The Seventh Circuit found that the district court appropriately rejected this theory, and properly utilized the normal retail price of bona fide copyrighted software in the valuation. The Seventh Circuit stated that where there is little or no evidence of the value of the infringing item, a court may utilize the value of the infringed item in its valuation.

7. Economic Espionage Act of 1996

The statute criminalizes the knowing theft of trade secrets, as well as attempts or conspiracies to steal trade secrets. In order to find a defendant guilty of conspiracy, the prosecution must prove (1) that an agreement existed, (2) that it had an unlawful purpose, and (3) that the defendant was a voluntary participant. *United States v. Echeverri*, 982 F.2d 677, 679 (1st Cir. 1993). The government must prove that the defendant possessed both the "intent to agree and [the] intent to commit the substantive offense." *United States v. Andu'jar*, 49 F.3d 16, 20 (1st Cir. 1995) (citing *United States v. Garcia*, 983 F.2d 1160, 1165 (1st Cir. 1993)). In addition, the government must prove that at least one conspirator committed an "overt act," that is, took an affirmative step toward achieving the conspiracy's purpose. *See* 18 U.S.C. §§ 1831 & 1832(a)(5); *United States v. Cassiere*, 4 F.3d 1006, 1014 (1st Cir. 1993).

First Circuit

2000

United States v. Martin, 228 F.3d 1 (1st Cir. 2000). This case arose out of an electronic mail "pen-pal" relationship between a dissatisfied Maine chemist, Caryn Camp, and a California scientist, Dr. Stephen Martin. Camp first began work at IDEXX, Inc. ("IDEXX"), a manufacturer of veterinary products headquartered in Portland, Maine, in May of 1995. Camp's responsibilities as an IDEXX chemist included mixing chemicals for diagnostic test kits for both pets and livestock. At the time of her employment, she signed non-disclosure and non-competition agreements, promising in part not to "disclose to others, or use for [her] own benefit or the benefit of others, any of

the Developments or any confidential, proprietary or secret information owned, possessed or used by [IDEXX] or its customers or contractors." The proprietary information included, but was not limited to, "trade secrets, processes, data, know-how, marketing plans, forecasts, unpublished financial statements, budgets, licenses, prices, costs, and employee, customer and supplier lists." Camp also signed the IDEXX policy on ethics and business conduct, which prohibited employees from revealing "proprietary knowledge or data" without prior authorization.

…

Martin was CEO of Wyoming DNA Vaccine ("WDV"). In Camp's last several days at IDEXX, she continued to collect products and information, which she forwarded to Martin on July 24. The package included operating manuals, IDEXX marketing materials, research and development data, a sales binder prepared by an independent contractor, as well as a binder labeled "Competition."

Unfortunately for Camp and Martin, Camp inadvertently sent her July 25 e-mail (acknowledging that July 24 was her last day and detailing the contents of her second package) to John Lawrence, the global marketing manager for Poultry/Livestock at IDEXX.

Camp agreed to testify against Martin as part of a plea agreement. A jury convicted them of wire fraud, mail fraud, conspiracy to steal trade secrets, and conspiracy to transport stolen property in interstate commerce. Martin appealed his conviction. Although Martin argued insufficient evidence to establish an agreement between Martin and Camp, insufficient evidence to prove that Martin had the necessary intent to injure the owner of the trade secret, and no trade secrets received from Camp, the First Circuit affirmed.

Third Circuit

1998

United States v. Hsu, 155 F.3d 189 (3d Cir. 1998). The Third Circuit was the first to address § 1832(a), which specifically covers private corporate espionage. In ruling on the defense's motion for access to the owner's trade secrets, allegedly "material" to the defense, the Third Circuit, held that legal impossibility was not a defense to a charge of attempted misappropriation of trade secrets in violation of 18 U.S.C. § 1832(a)(4), and was not a defense to a charge of conspiracy.

Seventh Circuit

2002

U. S. v. Lange, 312 F.3d 263 (7th Cir. 2002) (affirming the conviction). Lange stole computer data from his former employer, and then attempted to sell the data to one of the employer's competitors. He put the information up for sale via the Internet to anyone willing to pay $100,000. A potential buyer alerted his former employer, who in turn called the FBI. After analyzing the necessary ingredients of a trade secret, the Seventh Circuit affirmed Lange's conviction. The Court determined that there was

sufficient evidence that the information that he stole derived independent economic value, actual or potential, from not being generally known to the public, and not being readily ascertainable through proper means by the public. Thus, the information constituted "trade secrets" under the Economic Espionage Act.

8. Electronic Communications Privacy Act, Wiretap Act, Stored Communications Act, & Communications Act.

The 1986 Electronic Communications Privacy Act ("ECPA") modified the Wiretap Act 18 U.S.C. §§ 2510-2521. It prohibits the intentional interception of "any wire, oral, or electronic communication". Section 2512(1)(b) criminalizes the manufacture, assembly, possession, or sale of so-called "Pirate Access Devices" in interstate or foreign commerce. Section 2520(a) provides for civil actions by "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of" the ECPA.

The ECPA also modified the Stored Communications Act, 18 U.S.C. §§ 2701-2710. This is also known as the "Stored Wire and Electronic Communications and Transactional Records Access Act" ("SECTRA"). It prohibits the intentional unauthorized access of "a wire or electronic communication while it is in electronic storage in such system". SECTRA explicitly creates a private cause of action as follows: "[A]ny . . . person aggrieved by any violation of this chapter . . . may, in a civil action, recover from the person or entity . . . which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2707(a).

The Communications Act, 47 U.S.C. § 605, provides a civil remedy for the unauthorized use or publication of various wire or radio communications, including encrypted satellite broadcasts..

First Circuit

1993

Williams v. Poulos, 11 F.3d 271, 285 (1st Cir. 1993) (rejecting a good faith defense where defendant mistakenly believed his use and disclosure was authorized by the statute).

2003

In re Pharmatrak Inc. Privacy Litigation, 220 F.Supp.2d 4 (1st Cir. 2003). The First Circuit reversed the lower court, citing precedent that consent under the ECPA "should not casually be inferred," *Griggs-Ryan v. Smith*, 904 F.2d 112, 117-118 (1st Cir. 1990), and that the circumstances must convincingly show "actual consent rather than a constructive consent". *Williams v. Poulos*, 11 F.3d 271, 281-282 (1st Cir. 1993). The First Circuit also ruled that Pharmatrak clearly "intercepted" communications under the ECPA: "The acquisition by Pharmatrak was contemporaneous with the transmission by the Internet users to the pharmaceutical companies." Pharmatrak's NETcompare code was "effectively an automatic routing program. ... It was code that automatically

duplicated part of the communication between a user and the pharmaceutical clients and sent this information to a third party (Pharmatrak)."

2005

U.S. v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc, reversing the First Circuit's panel decision in 2004). Councilman was vice-president of Interloc, which acted as an ISP, and which intercepted and copied certain incoming e-mails. The court stated that "electronic communication" as used in the Wiretap Act includes communications that are in "transient electronic storage that is intrinsic to the communication process". Therefore, the court held, interception of an e-mail message that is in such storage is an offense under the Wiretap Act.

Second Circuit

2002

Specht v. Netcscape Communications, 306 F.3d 17 (2d Cir. 2002). Internet users and website operator sued, alleging that Netscape's "SmartDownload plug-in" software program, made available on Netscape's website for free downloading, invaded plaintiffs' privacy by clandestinely transmitting personal information to Netscape when plaintiffs employed the plug-in program to browse the Internet. Netscape moved to compel arbitration, and to stay the court proceedings. The court denied the motion. On appeal, the Second Circuit affirmed, holding, in part, that

> whether defendants violated plaintiffs' rights under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act--involves matters that are clearly collateral to the Communicator license agreement. … the Communicator license agreement governed disputes concerning Netscape's browser programs only, not disputes concerning a plug-in program like SmartDownload.

Third Circuit

2005

DirecTV Inc. v. Pepe, 431 F.3d 162, 78 U.S.P.Q.2d 1612 (3rd Cir. 2005) (reversing the judgment of the District Court that no private right of action exists under 18 U.S.C. § 2520(a) for violations of 18 U.S.C. § 2511(1)(a), and remanding). The defendants allegedly pirated encrypted satellite television broadcasts. DIRECTV did not appeal the District Court's denials of its claims under § 2512, rooted in defendants' mere purchase or possession of unauthorized interception devices. The Third Circuit expressed no opinion as to the merits of District Court's denial of the § 2512 claims.

Fourth Circuit

2000

United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000). A network banner alerting the user that communications on the network are monitored and intercepted may be used to demonstrate that a user furnished consent to intercept communications on that network.

Fifth Circuit

1976

United States v. Turk, 526 F. 2d 654 (5th Cir. 1976) ("interception" must be contemporaneous with transmission of the communication).

1994

Steve Jackson Games v. U.S. Secret Service, 36 F. 3d 457 (5th Cir. 1994) ("interception" did not refer to stored electronic communications, because the definition of electronic communications does not mention "storage"). In dicta, the Court stated that the ECPA doesn't prohibit retrieving stored electronic communications.

2000

Peavy v. WFAA-TV, Inc., 221 F.3d 158, 178-79 (5th Cir. 2000). Although a defendant must have intended to intercept a covered communication, he or she need not have specifically intended to violate the Wiretap Act. In other words, a mistake of law is not a defense to a Wiretap Act charge. The First Amendment does not create a general defense to Wiretap Act violations for media.

Peavy v. Harman, 37 F. Supp. 2d 495, 513 (N.D. Tex. 1999), aff'd in part and reversed in part, 221 F.3d 258 (5th Cir. 2000). "Use" requires some "active employment of the contents of the illegally intercepted communication for some purpose." Thus, "use" does not include mere listening to intercepted conversations.

2007

McEwen v. SourceResources.com, No. H-06-2530, U.S. Dist. LEXIS 10156 (S.D. Tex. February 13, 2007) (denying defendants' motion to dismiss based on SECTRA allegedly not covering the illegal acquisition of mere telephone numbers and dates of calls). Plaintiffs are all former employees of Xtria, LLC. Plaintiffs alleged that Xtria hired Childs, a private investigator, to learn whether they had inappropriate commercial contacts with Xtria's employees or customers. As part of this investigation, Plaintiffs believe that Childs employed Source to obtain their cell phone records, including, at a minimum, the numbers each Plaintiff dialed from his or her cell phone, without consent. Judge Atlas held that "the records at issue, that is, phone numbers Plaintiffs dialed and the dates of calls, are encompassed by the definition of "electronic communication" under § 2510(12)."

Sixth Circuit

1999

Dorris v. Absher, 179 F.3d 420, 426 (6th Cir. 1999). "Use" does not include mere listening to intercepted conversations.

Seventh Circuit

2000

United States v. Andreas, 216 F.3d 645, 660 (7th Cir. 2000). For purposes of claiming the "consent" exception, government employees are not considered to be "acting under color of law" merely because they are government employees. Whether a government employee is acting under color of law under the wiretap statute depends on whether the individual was acting under the government's direction when conducting the interception.

2002

Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002). A network banner alerting the user that communications on the network are monitored and intercepted may be used to demonstrate that a user furnished consent to intercept communications on that network.

2003

Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003) (affirming dismissal). College athletes sued an ISP (and also the perpetrators (not located), and college officials (safely protected by a qualified immunity)) for providing internet access and web hosting to sellers of a video of the unclothed athletes that had been illicitly taken in college locker rooms. The athletes claimed that the ISP aided and abetted the illicit photographers in their illegal enterprise by providing the website, and by providing access to sell the videos. The Seventh Circuit said that 18 U.S.C. 2511 should not be read to implicitly create secondary liability. Additionally, the Court noted that the ISP did not satisfy the normal understanding of an abettor, in that the ISP did not have a desire to promote the wrongful venture's success. The Court likened the athletes' argument to holding a newspaper liable for advertising by a massage parlor that is a front for prostitution. Since the ISP did not have a reason to believe the activity was illegal, nor were the services sold (web hosting and bandwidth access) such that the ISP should know the buyer had no legal use for them, there could be no liability as an aider or abettor.

2006

McCready v. eBay, Inc., 453 F.3d 882 (7th Cir. 2006) (affirming a dismissal of two lawsuits, and ordering McCready to show cause why he should not be sanctioned for his abuse of process). McCready operated an online business in which he bought and sold various items through several accounts he had registered with eBay. Several eBay users used eBay's Feedback Forum to complain that McCready failed to deliver the goods he sold, or delivered goods of lower quality than he had advertised. After investigating the claims, eBay suspended McCready's accounts, and advised him that

he would be reinstated if he reimbursed the claimants. In response, McCready embarked on retaliatory litigation. In this lawsuit, one of many, McCready claimed that eBay's production of documents in compliance with a subpoena in a Michigan case violated the ECPA and the Stored Communications Act. The district court dismissed McCready's claims under Rule 12(b)(6). Good faith reliance on a subpoena is a complete defense to actions brought under the ECPA and SCA. 18 U.S.C. §§ 2520(d)(1) & 2707(e). The Seventh Circuit found that there was "no indication that eBay acted in any fashion other than good faith". The Seventh Circuit, after reviewing all the frivolous lawsuits and frivolous motions filed by McCready, stated:

> McCready is hereby ordered to show cause within 30 days why he should not be required to pay $2,500 to this court's clerk. Should McCready fail to respond or merely attempt to reargue his case, then the $2,500 sanction will be imposed and McCready will be barred from filing, with appropriate exceptions, any paper in all federal courts in this circuit for no less than two years.

Eighth Circuit

1996

Reynolds v. Spears, 93 F.3d 428, 435-36 (8th Cir. 1996) (reliance on incorrect advice from a law enforcement officer is not a defense). "Use" does not include mere listening to intercepted conversations. *Id*. at 432-33.

Ninth Circuit

1993

United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (the need to monitor misuse of computer system justified interception of electronic communications pursuant to subsection 2511(2)(a)(i))).

1999

Sussman v. ABC, Inc., 186 F.3d 1200 (9th Cir. 1999). The First Amendment does not create a general defense to Wiretap Act violations for media.

2001

Konop v. Hawaiian Airlines, 236 F.3d 1035 (9th Cir. 2001) (withdrawn, 262 F3d. 972 (9th Cir. August 28, 2001) Konop, an airline pilot, maintained a website that criticized the airline. He protected it with passwords, that he gave to only friends, mostly pilots. An airlineV.P. accessed the website using another pilot's password. On January 8, 2001, the Ninth Circuit found liability under the ECPA, holding that "intercept" had the same meaning for wire or electronic communications. However, on August 28, 2001, the Ninth Circuit withdrew its opinion. Then, in August, 2002, the Ninth Circuit held that the employer did not "intercept" the website's contents in violation of the Wiretap Act, reversing the district court's judgment with respect to Konop's claims under the Stored Communications Act. *Konop v. Hawaiian Airlines, Inc.*,302 F.3d 868, (9th Cir. 2002).

2004

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004) (affirming dismissal of a Wiretap Act claim, and reversing a dismissal with prejudice of a Computer Fraud and Abuse Act claim, with instructions to dismiss with leave to amend to allege damages or loss).

During the course of commercial litigation between Integrated Capital Associates (ICA) and Farey-Jones, Farey-Jones ordered his lawyer to subpoena ICA's ISP and obtain a number of emails. Upon receipt of the subpoena, ICA's ISP posted a sampling of ICA emails on its website, many of which were privileged and personal. ICA employees then filed a civil suit against Farey-Jones and his counsel claiming, inter alia, violation of the Wiretap Act and the Computer Fraud and Abuse Act.

Regarding the Wiretap Act, the Ninth Circuit reiterated that Konop applies to only "acquisition contemporaneous with transmission" and held that Congress did not intend the term "intercept" to apply to electronic communications in electronic storage. The Court upheld the district court's dismissal of the Wiretap claim.

Under the Computer Fraud and Abuse Act, the Ninth Circuit held that the Act's civil remedies extend to "[a]ny person who suffers damage or loss by reason of a violation of this section." The district court had dismissed the Computer Fraud and Abuse Act claims on the theory that the Act does not apply to "unauthorized use of a third party's computer." The Ninth Circuit instead interpreted the Act broadly to include harm suffered by individuals other than the computer's owner, particularly if they have rights to data stored on the computer.

2006

Freeman v. DirecTV, Inc., No. 457 F.3d 1001 (9th Cir. 2006) (affirming dismissal of the claims of a group of satellite signal pirates against DirecTV, because 18 U.S.C. § 2702 does not provide a basis for asserting conspiracy and aiding and abetting claims.). Gray operated a number of web sites from his home in British Columbia, Canada, offering information relating to the pirating of the DirecTV signal. The Supreme Court of British Columbia granted DirecTV an injunction and an order entitling DirecTV to seize Gray's computers and the data contained therein, and the order allowed for "any and all evidence seized or delivered up pursuant to the order [to] be used in subsequent civil proceedings commenced by DirecTV against any third party, including, but not limited to proceedings against [Gray's] customers, suppliers, members, and subscribers."

Earlier in 2003, DirecTV had sued Lawrence Freeman for distributing illegal signal theft devices. During the litigation against Freeman, in response to initial discovery requests, DirecTV produced portions of the information gathered at Gray's residence. This information included the content of communications posted on electronic message boards accessed through Gray's web sites. On March 16, 2004, DirecTV and Freeman settled the lawsuit, and signed a settlement agreement and release.

On April 5, 2004, Freeman and Michael Scherer filed a class action against DirecTV. In an amended complaint, Scherer claimed that he, like Freeman, was a participant on the message boards and web sites run by Gray. Freeman and Scherer asserted that the sharing of data from Gray to DirecTV was not authorized by the Canadian court because DirecTV had agreed that the evidence would be in custody of the independent solicitor instead of DirecTV's solicitors, and that it was only released pursuant to the agreement between Gray and DirecTV. Freeman and Scherer claimed further that because there was a subsequent agreement between Gray and DirecTV that allowed DirecTV to receive the data from the independent solicitor, DirecTV conspired with and aided and abetted Gray in the disclosure of the stored communications in violation of 18 U.S.C. § 2702.

The Ninth Circuit held, “We reject Freeman and Scherer's to read implicitly into these statutory provisions claims for conspiracy or aiding and abetting. In addition to being contrary to the plain language of §§ 2702 and 2707, such an implied interpretation is not supported by legislative history or case law.”

Tenth Circuit

1991

Heggy v. Heggy, 944 F.2d 1537, 1541-42 (10th Cir. 1991) (rejecting a "good faith" defense based upon a mistake of law).

1992

Thompson v. Dulaney, 970 F.2d 744, 749 (10th Cir. 1992) (a “defendant may be presumed to know the law”).

2002

United States v. Angevine, 281 F.3d 1130, 1133 (10th Cir. 2002). A network banner alerting the user that communications on the network are monitored and intercepted may be used to demonstrate that a user furnished consent to intercept communications on that network.

Eleventh Circuit

2003

U.S. v. Steiger, 318 F.3d 1039 (11th Cir. 2003) (confirming a conviction). Steiger was convicted on a number of counts involving the sexual exploitation of minors. An anonymous source provided the FBI and the Montgomery, Alabama, Police Department with photos of Steiger’s activities, his name, IP address, and checking account records, along with information on the specific folders on Steiger’s computer where the photos were kept. The anonymous source also informed the authorities that Steiger was either a physician or paramedic. The anonymous source obtained this information using a Trojan Horse posted on a pornography website. On appeal, Steiger

claimed that the information obtained by the source was inadmissible under the Wiretap Act. The Eleventh Circuit held that the anonymous source did not "intercept" any electronic communications in violation of the Wiretap Act. The Court relied on the 9th and 5th Circuits' narrow definition of "intercept" as requiring contemporaneous acquisition of the electronic communications. The Court found no contemporaneous acquisitions here as a result of the anonymous source's use of the Trojan Horse. The Court also held that hacking into a home computer does not by itself implicate "Unlawful Access to Stored Communications" (18 U.S.C. § 2701), because a home computer does not provide an electronic communication service ("ECS") to others.

9. Child Online Protection Act of 1998

The Child Online Protection Act of 1998 ("COPA") makes it a crime punishable by fine or imprisonment for a Web site operator to "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web make[] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." 47 U.S.C. § 231(a)(1).

Supreme Court

2002

Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2002). Section 231(a)(1) defines "material that is harmful to minors" by a three-part test that tracks the *Miller* (*Miller v. California*, 413 U.S. 15 (1973)) obscenity test. One part of the test is whether "the average person, applying contemporary community standards, would find [that the material, taken] as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest."

On appeal from the same Philadelphia district court that the Supreme Court reversed on the constitutionality of the Children's Internet Protection Act ("CIPA"), *U.S. v. American Library Ass'n, Inc.,* No. 02-361, __ U.S. __ (June 23, 2003), the Supreme Court held that COPA is not unconstitutionally overbroad just because it uses the "community standards" test like that from *Miller* to regulate speech on the Internet. The Court also stated that the serious value prong of the *Miller* test is judged by a national, rather than, community standard, which "allows appellate courts to impose some limitations and regularity on the definition by setting, as a matter of law, a national floor for socially redeeming value."

Third Circuit

2003

American Civil Liberties Union v. Ashcroft, 322 F.3d 240 (3d Cir. 2003). On remand from the Supreme Court, the Third Circuit, in its second review of COPA, held that the law fails to satisfy the First Amendment's "strict scrutiny" standard for content-based restrictions on speech, and it prohibits a substantial amount of speech protected under the First Amendment.

10. Wire Fraud 18 U.S.C. § 1343

The wire fraud statute, 18 U.S.C. § 1343, was enacted in 1952. The entire statute reads as follows:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

Second Circuit

2003

United States v. Jackson, 346 F.3d 22 (2d Cir. 2003) (affirming a conviction). Jackson was charged, among other crimes, with wire fraud in violation of 18 U.S.C. § 1343, from an extensive scheme to defraud wealthy individuals. He would first identify a wealthy target by searching the Internet. He would then purchase personal information about the individual from an "information broker" on the Internet, and would call places such as banks and hotels using the information he previously acquired in order to obtain even more private information such as account numbers and credit card expiration dates. Then Jackson used the credit card numbers to order merchandise which he would have shipped to a place where he then could pick it up by pretending to be the victim. Jackson pled guilty to wire fraud, in addition to the other charges, pursuant to a plea agreement.

Third Circuit

2002

U.S. v. Nickens, 38 Fed. Appx. 721 (3rd. Cir. 2002). Using a "harvesting" program, Nickens obtained E- mail addresses for individuals who had unsuccessfully bid on products on E-Bay and other on-line auction businesses. In his E-mails, Nickens

claimed to have the same or a similar product for sale but wanted to deal directly with the customer and avoid the utilization of auction businesses. He required that the money for the product purchased be wired or sent by certified check to accounts set up at Northern Central Bank before the merchandise would be delivered.

Nickens shipped no merchandise and, as customers complained, he employed a variety of delaying tactics. Nickens pled guilty pursuant to a plea agreement to a sixty-seven count indictment with wire fraud involving the use of the Internet, in violation of 18 U.S.C. § 1343. On appeal of his sentence, the Third Circuit held that imposition of a two-level sentencing enhancement for committing the offense through mass-marketing was proper.

Seventh Circuit

2002

U.S. v. Gajdik, 292 F.3d 555 (7th Cir. 2002). Gajdik operated a fraud scheme on eBay. After a stint of legitimate transactions, Gajdik began selling designer sunglasses that he misrepresented as new and under manufacturer's warranty. The sunglasses were in fact broken and discarded glasses that Gajdik retrieved from a dumpster outside of a Peoria distribution warehouse and reassembled. Gajdik quickly graduated to auctioning expensive merchandise such as Rolex, Auderman Piquet, and Patek Phillipe watches, diamonds, collectable coins, and computers. Gajdik neither possessed nor intended to obtain or deliver any of these items. Still, Gajdik's fraudulent auctions attracted many bidders, and eBay users from around the world, believing they were purchasing high-end goods, sent him nearly $700,000. Gajdik entered a plea agreement with the government, and pleaded guilty to seventeen of the government's twenty-one charges, including eight counts of wire fraud, 18 U.S.C. § 1343.

Ninth Circuit

2001

U.S. v. Pirello, 255 F.3d 728 (9th Cir. 2001), *cert. denied*, *Pirello v. U.S.*, 534 U.S. 1034 (2001) Pirello placed four separate advertisements on an Internet classified-ads website, known as Excite Classifieds, each soliciting buyers for a different type of computer. The advertisements posted by Pirello were part of a fraudulent scheme whereby Pirello would induce prospective buyers to send him money for computers he never intended to deliver. Pirello pled guilty to using the Internet to commit wire fraud in violation of 18 U.S.C. § 1343. The district court applied a two-level enhancement to Pirello's base offense level under the United States Sentencing Guidelines, for using mass-marketing to effectuate his crime. Pirello appealed. The Ninth Circuit affirmed.

Tenth Circuit

2002

U.S. v. Blanchett*,* 41 Fed. Appx. 181 (10th Cir. 2002). The defendants placed advertisements offering computer equipment to the highest bidder on eBay. After a victim became the highest bidder and "won" the auction, the defendants contacted him or her by e-mail with payment instructions and a promise that the equipment would be shipped after receipt of payment. In fact, the defendants never intended to send the advertised equipment to the highest bidder. One defendant pled guilty, and the district court enhanced his sentence, following the Ninth Circuit in *Pirello*, which held that the mass-marketing enhancement was appropriate when a defendant defrauded people by placing a classified advertisement for computers on the Internet. The Tenth Circuit affirmed.

11. Spamming: Federal & State Laws

Here are a couple of terms that you will see in this area:

"forged spamming"	spamming using non-existent domain names
"domain-name hijacking"	spamming using an unsuspecting server

The federal CAN-SPAM Act of 2003 became effective January 1, 2004. Parts of it are shown below.

Chapter 47 of title 18, United States Code, was amended by adding at the end the following new section:

SEC. 3. DEFINITIONS.

In this Act:

(11) INTERNET ACCESS SERVICE.—The term ''Internet access service'' has the meaning given that term in section 231(e)(4) of the Communications Act of 1934 (47 U.S.C. 231(e)(4)).

§ 231. Restriction of access by minors to materials commercially distributed by means of World Wide Web that are harmful to minors

(e) Definitions
For purposes of this subsection,[1] the following definitions shall apply:

(4) Internet access service
The term "Internet access service" means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may

also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.

(12) PROCURE.—The term ‘‘procure’’, when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one’s behalf.

Sec. 1037. Fraud and related activity in connection with electronic mail

`(a) IN GENERAL- Whoever, in or affecting interstate or foreign commerce, knowingly—

`(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,
`(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,
`(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,
`(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or
`(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,

or conspires to do so, shall be punished as provided in subsection (b).

`(b) PENALTIES- The punishment for an offense under subsection (a) is--

`(1) a fine under this title, imprisonment for not more than 5 years, or both, if--

`(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or
`(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

`(2) a fine under this title, imprisonment for not more than 3 years, or both, if--

`(A) the offense is an offense under subsection (a)(1);

`(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

`(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

`(D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period;

`(E) as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or

`(F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and

`(3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.

`(c) FORFEITURE-

`(1) IN GENERAL- The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States--

`(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

`(B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

`(2) PROCEDURES- The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

…

SEC. 5. OTHER PROTECTIONS FOR USERS OF COMMERCIAL ELECTRONIC MAIL.

(a) REQUIREMENTS FOR TRANSMISSION OF MESSAGES-

(1) PROHIBITION OF FALSE OR MISLEADING TRANSMISSION INFORMATION- It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this paragraph--

(A) header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading;
(B) a `from' line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading; and
(C) header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

(2) PROHIBITION OF DECEPTIVE SUBJECT HEADINGS- It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message (consistent with the criteria used in enforcement of section 5 of the Federal Trade Commission Act (15 U.S.C. 45)).
(3) Inclusion of return address or comparable mechanism in commercial electronic mail-
(A) IN GENERAL- It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that--
(i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and
(ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.
(B) MORE DETAILED OPTIONS POSSIBLE- The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an

option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.

(C) TEMPORARY INABILITY TO RECEIVE MESSAGES OR PROCESS REQUESTS- A return electronic mail address or other mechanism does not fail to satisfy the requirements of subparagraph (A) if it is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period.

(4) PROHIBITION OF TRANSMISSION OF COMMERCIAL ELECTRONIC MAIL AFTER OBJECTION-

(A) IN GENERAL- If a recipient makes a request using a mechanism provided pursuant to paragraph (3) not to receive some or any commercial electronic mail messages from such sender, then it is unlawful--

(i) for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request;

(ii) for any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request;

(iii) for any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message would violate clause (i) or (ii); or

(iv) for the sender, or any other person who knows that the recipient has made such a request, to sell, lease, exchange, or otherwise transfer or release the electronic mail address of the recipient (including through any transaction or other transfer involving mailing lists bearing the electronic mail address of the recipient) for any purpose other than compliance with this Act or other provision of law.

(B) SUBSEQUENT AFFIRMATIVE CONSENT- A prohibition in subparagraph (A) does not apply if there is affirmative consent by the recipient subsequent to the request under subparagraph (A).

SEC. 7. ENFORCEMENT GENERALLY.

(g) Action by Provider of Internet Access Service-

(1) ACTION AUTHORIZED- A provider of Internet access service adversely affected by a violation of section 5(a)(1), 5(b), or 5(d), or a pattern or practice that violates paragraph (2), (3), (4), or (5) of section 5(a), may bring a civil action in any district court of the United States with jurisdiction over the defendant--

(A) to enjoin further violation by the defendant; or

(B) to recover damages in an amount equal to the greater of--

(i) actual monetary loss incurred by the provider of Internet access service as a result of such violation; or

(ii) the amount determined under paragraph (3).

(2) SPECIAL DEFINITION OF `PROCURE'- In any action brought under paragraph (1), this Act shall be applied as if the definition of the term `procure' in section 3(12) contained, after `behalf' the words **`with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this Act'.**

(3) STATUTORY DAMAGES-

(A) IN GENERAL- For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message that is transmitted or attempted to be transmitted over the facilities of the provider of Internet access service, or that is transmitted or attempted to be transmitted to an electronic mail address obtained from the provider of Internet access service in violation of section 5(b)(1)(A)(i), treated as a separate violation) by--

(i) up to $100, in the case of a violation of section 5(a)(1); or

(ii) up to $25, in the case of any other violation of section 5.

(B) LIMITATION- For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed $1,000,000.

(C) AGGRAVATED DAMAGES- The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if--

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravated violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES- In assessing damages under subparagraph (A), the court may consider whether--

(i) the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent such violations; or
(ii) the violation occurred despite commercially reasonable efforts to maintain compliance with the practices and procedures to which reference is made in clause (i).

(4) ATTORNEY FEES- In any action brought pursuant to paragraph (1), the court may, in its discretion, require an undertaking for the payment of the costs of such action, and assess reasonable costs, including reasonable attorneys' fees, against any party.

Fourth Circuit

2006

Omega World Travel Inc. v. Mummagraphics Inc., 469 F.3d 348 (4th Cir. 2006) (affirming the district court's award of summary judgment to Omega on all of Mummagraphics' claims, and stating that a state cause of action for "immaterial" errors in header information was preempted by the CAN-SPAM act). Mummagraphics, Inc., a provider of online services, sought significant statutory damages from Omega World Travel, Inc., a Virginia-based travel agency. Mummagraphics alleged that Cruise.com (a wholly owned subsidiary of Omega) sent the messages in violation of the CAN-SPAM Act. The Fourth Circuit stated, "The CAN-SPAM Act preempts Mummagraphics' claims under Oklahoma's statutes. In addition, Mummagraphics failed to allege the material inaccuracies or pattern of failures to conform to opt-out requirements that is necessary to establish liability under the CAN-SPAM Act. The CANSPAM Act addresses 'spam' as a serious and pervasive problem, but it does not impose liability at the mere drop of a hat. … Because Mummagraphics failed to submit any evidence that the receipt of eleven commercial e-mail messages placed a meaningful burden on the company's computer systems or even its other resources, summary judgment was appropriate on this counterclaim."

2007

Aitken v. Communications Workers Of America, 2007 U.S. Dist. LEXIS 51434; 182 L.R.R.M. 2334 (E.D. Va. 2007) (denying a motion to dismiss a CAN-SPAM Act claim). MCI and Verizon sued the Communications Workers of America for the misappropriation of the identities of certain plaintiffs -- twelve managers at Verizon -- for the purpose of sending pro-union, anti-Verizon emails to Verizon employees under the managers' names. Those emails falsely appeared to originate from the Verizon managers, and disparaged Verizon, while touting the benefits of unionization with the Communications Workers of America.

Fifth Circuit

2005

White Buffalo Ventures, LLC v. University of Texas, No. 04-50362 (5th Cir. 2005). White Buffalo operates several online dating services, including www.longhornsingles.com (still operating in September 2007), which targets students at the University of Texas at Austin. Pursuant to its internal anti-solicitation policy, UT blocked White Buffalo's attempts to send unsolicited bulk commercial email. White Buffalo sued to enjoin UT from excluding its incoming email. The district court denied the injunction. On cross-motions for summary judgment, the court granted UT's motion and denied White Buffalo's. The Fifth Circuit affirmed, agreeing that federal law (CAN-SPAM Act) did NOT preempt UT's internal anti-spam policy and that UT's policy did NOT violate the First Amendment.

Ninth Circuit

2004

C.D. Cal.

United States v. Tombros, No. CR 04-1085 (C. D. Cal. 9/27/04). A Los Angeles-area resident pleaded guilty September 27, 2004, to violating the CAN SPAM Act, by driving around a neighborhood and using a wireless antennae attached to a laptop to find open, unencrypted wireless access points, and then sending thousands of spam messages advertising pornographic Web sites. This was the first conviction under the Act. Tombros faced a maximum possible sentence of three years in federal prison.

2007

U.S. v. Goodin, (S.D. Cal. June 14, 2007). Goodin, a "phisher", was sentenced to nearly six years in prison after the nation's first CAN-SPAM jury trial conviction. Goodin was convicted of committing identity theft, credit card fraud, witness harassment and other offenses, and ordered to pay $1,002,885.58 to the victims of his phishing scheme, including nearly $1 million to Earthlink. The jury found that Goodin sent thousands of e-mails through an Earthlink Internet connection to America Online users that appeared to be from AOL's billing department. The e-mails prompted the AOL customers to "update" their personal and credit card information on phony AOL webpages that Goodin controlled. Goodin then used his victims' personal and credit card information to make unauthorized credit card purchases. It cost Earthlink nearly $1 million to detect and combat Goodin's phishing schemes.

MySpace, Inc. v. Sanford Wallace, CV 07-1929-ABC, 2007 U.S. Dist. LEXIS 56814 (C.D. Cal. 2007) (granting-in-part plaintiff's motion for a preliminary injunction). Defendant has three dbs's: freevegasclubs.com, realvegas-sins.com, and Feebleminded Productions. Defendant had created more than 11,000 similar MySpace profiles and 11,383 unique America Online email accounts to register those profiles. Defendant circumvented plaintiff's unique-email-address registration requirement, and, by creating 11,000 unique profiles, defendant circumvented plaintiff's daily limit on the

number of messages that can be sent from any one profile in a single day. In total, defendant sent nearly 400,000 messages and posted 890,000 comments from 320,000 "hijacked" MySpace.com user accounts. Defendant also created "groups" on MySpace.com redirecting users to the Wallace Websites, including altering the MySpace "unsubscribe" link to point to the Wallace Websites rather than to actually allow members to unsubscribe, and he used software code to lay graphics containing links to the Wallace Websites over users' MySpace.com profiles. A final note: although defendant requested a bond of $1 million, the Court ordered plaintiff to post a bond in the amount of only $50,000.

MySpace, Inc. v. Globe.com, Inc, CV 06-3391-RGK, 2007 U.S. Dist. LEXIS 44143 (C.D. Cal. 2007) (granting-in-part plaintiff's motion for summary judgment under the CAN-SPAM act). Defendant is a public company that provides internet-based communications services ("TGLO Products"). Defendant operates one or more websites under various domain names, including glochat.com, tglophone.com, glo-talk.com and digitalvoiceglo.com. Beginning in January 2006, Defendant set up at least 95 identical or virtually identical "dummy" MySpace profiles, with corresponding e-message accounts. Defendant used these accounts to send almost 400,000 unsolicited commercial e-messages marketing TGLO Products to MySpace users. The Court found liability under the following CAN-SPAM sections: 15 U.S.C. §§ 7704(a)(1), 7704(a)(5) and 7704(b)(1)(A)(ii).

Gordon v. Virtumundo, Inc., 2007 U.S. Dist. LEXIS 55941 (W.D. Wash. 2007) (awarding attorneys' fees to the prevailing defendants). The Court stated,

> First, it is obvious that Plaintiffs are testing their luck at making their "spam business" extraordinarily lucrative by seeking statutory damages through a strategy of spam collection and serial litigation. … The Court finds that Plaintiffs' instant law-suit is an excellent example of the ill-motivated, unreasonable, and frivolous type of lawsuit that justifies an award of attorneys' fees to Defendants under Fogerty. The context of this litigation and the context of Plaintiffs' overall litigation strategy, involving at least a dozen federal actions, indicate that Plaintiffs are motivated by the prospect of multi-million-dollar statutory damages awards in exchange for their relatively paltry spam-collection and spam-litigation costs.
>
> Remarkably, it appears that Defendants' total request for compensation for 1,975.8 hours overstates the hours worked by 531.8 hours, which amounts to about 27% of the total hours requested.

The Court awarded to the defendants hourly attorneys' fees award of $ 96,240.00, plus costs in the amount of $ 15,200.00, although the requested amounts were much higher (spending 7 pages of the opinion on the merits of the case, and 11 pages calculating reasonable fees and costs)

Facebook, Inc., v. Connectu LLC, 489 F. Supp. 2d 1087 (N.D. Cal. 2007) (dismissing claims under California state law as being pre-empted by the CAN-SPAM act, and allowing other claims to be amended so as to fall under the CAN-SPAM act). Facebook and ConnectU operate competing social networking websites on the Internet. Facebook contended that ConnectU accessed the Facebook website to collect "millions" of email addresses of Facebook, and then sent emails to those users soliciting their patronage.

Phillips v. Netblue, Inc., 2006 U.S. Dist. LEXIS 92573 (N.D. Cal. 2006) (denying defendant's motion to amend its answer to assert that plaintiffs failed to mitigate its damages). The Court stated, "Having determined that the CAN-SPAM Act's statutory damages provisions are meant to penalize the spammer as opposed to compensate the victims of spam, the Court concludes that the doctrine of mitigation of damages has no applicability to any determination regarding the award of such damages."

Eleventh Circuit

N.D. Ga.

EarthLink Inc. v. Carmack, No. 02-CV-3041 (N.D. Ga. 2003). Carmack sent over 825 million e-mail messages to EarthLink subscribers in 2002, using 343 EarthLink accounts. Judge Thrash estimated the company's actual damages at more than $2.7 million. The court trebled those damages after granting EarthLink's state and federal racketeering claims, and then doubled it again to $16.4 million in total damages to "serve as a clear warning to Carmack," ordered that the judgment will not be dischargeable in bankruptcy, and further ordered that in the event another ISP files a lawsuit against Carmack, the liquidated damages will be $25,000 or $2 per 1,000 e-mails sent, whichever is greater, as well as lost profit damages, attorney's fees, expenses, and costs. Individual or end-user claims will be $1,000 per e-mail sent, as well as legal fees, expenses, and costs.

State Laws

As of November 18, 2003, David Sorkin's website http://www.spamlaws.com/us.html listed thirty-six states with anti-spam statutes.

California's anti-spam statute, Cal. Bus. & Prof. Code §17538.4, requires that California-based senders of unsolicited commercial e-mail messages, **or out-of-state senders of messages to California residents**, include the following

information in any e-mail message sent to a person with whom they have no pre-existing business relationship:

a valid toll-free telephone number and/or e-mail address to which recipients may call or write and ask to be removed from future e-mail messages;

in the first text of the message, a notice to recipients informing them of the ability to be removed from future e-mail messages; and

in the subject header, "ADV:" as the first four characters.

Effective September 1, 2003, Texas has an anti-spam statute, that provides criminal and civil penalties, and a civil cause of action. 4 Business & Commerce Code § 46 “Electronic Mail Solicitation”. This statute prohibits sending an unsolicited e-mail that 1) falsifies electronic mail transmission information or other routing information, 2) contains false, deceptive, or misleading information in the subject line, or 3) uses another person's Internet domain name without the other person's consent.

The sender of spam (“a commercial electronic mail message sent without the consent of the recipient by a person with whom the recipient does not have an established business relationship”) must include at the beginning of the subject line “ADV:”. If the spam is sexual in nature, the sender must include at the beginning of the subject line “ADV: ADULT ADVERTISEMENT”. Failure to include “ADV: ADULT ADVERTISEMENT”, or sending obscene material, is a Class B misdemeanor. Violations of the statute subject the offender to a civil penalty in an amount not to exceed the lesser of: 1) $10 for each unlawful message or action; or 2) $25,000 for each day an unlawful message is received or an action is taken.

The statute further provides that any individual may sue a spammer for a false, misleading, or deceptive act or practice under Subchapter E, Chapter 17, and under § 46.008 for actual damages, including lost profits. A person who prevails in the action is entitled to reasonable attorney's fees and court costs. In lieu of actual damages, the plaintiff can choose to recover the lesser of: 1) $10 for each unlawful message; or 2) $25,000 for each day the unlawful message is received.

There is one trap for the unwary plaintiff. Under § 46.009, the plaintiff must notify the attorney general by sending a copy of the petition by registered or certified mail not later than the 30th day after the date the petition was filed, and at least 10 days before the date set for a hearing on the action. If the plaintiff fails to do so, he is liable to the state for a civil penalty in an amount not to exceed $200 for each violation.

Three federal district courts, the Eastern District of Virginia, the Northern District of California, and the Southern District of Ohio, have held that under certain circumstances, spam constitutes the tort of “trespass to chattel.” *Verizon Online Services, Inc. v. Ralsky*, 203 F.Supp.2d 601 (E.D. Va. 2002); *America Online v. LCGM*,

46 F. Supp.2d 444, 451-52 (E.D. Va. 1998); *Hotmail Corp. v. Van Money Pie, Inc.*, 47 U.S.P.Q.2d 1020, 1022 (N.D. Cal. 1998); *CompuServe inc. v. Cyber-Promotions, Inc.*, 962 F. Supp. 1015, 1018 (S.D. Ohio 1997).

The following websites will help your client in fighting spam, without going to court:

www.declude.com	spam-fighting software products and free resources, such as a list of anti-spam databases
www.samspade.org	technical tools useful in fighting spam
www.spamhaus.org	real-time database of addresses of verified spammers, spam gangs and spam services register of known spam operations that have been thrown off ISPs
www.spamcon.org	forum for Internet users, administrators, marketers, anti-spam businesses and activists to collaborate and develop strategies

2003

New York

New York is actively prosecuting spammers. In the second week of May, 2003, Howard Carmack, the 'Buffalo Spammer' accused of sending more than 825 million unsolicited e-mails from illegal EarthLink accounts, was arrested and arraigned in New York on four felony and two misdemeanor counts. New York Attorney General Eliot Spitzer stated, "Spammers who forge documents and steal the identity of others to create their e-mail traffic will be prosecuted."

12. Texas Computer Crimes Statute 7 Texas Penal Code 33

This statute states in § 33.02, "Breach of Computer Security":

> "(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner."

Under the Texas Civil Practice and Remedies Code, section 143.001, "Cause of Action", a person can file a civil suit for this crime:

> "(a) A person who is injured or whose property has been injured as a result of a violation under Chapter 33, Penal Code, has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally."

Conclusion

Merely being aware of these Internet crimes may not be enough. You might want to review these cases once in a while, and keep checking the cybercrime.gov website for the latest new laws. Our elected officials keep passing new laws to help protect us from the cyber criminals, and you never know when one of your clients may inadvertently run afoul of some new law.