Internet Distribution, E-Commerce and Other Computer Related Issues:
Current Developments in Liability On-Line,
Business Methods Patents and
Software Distribution, Licensing and
Copyright Protection Questions

Table of Contents

Contents

Internet Distribution, E-Commerce and Other Computer Related Issues:

Current Developments in Liability On-Line, Business Methods Patents and Software Distribution, Licensing and Copyright Protection Questions

By Andre R. Jaglom*

I. *Liability On-Line: Copyright and Tort Risks of Providing Content, or Who's In Charge Here?*

A. *The Applicability of Multiple Laws*

Use of the Internet generally, and the World Wide Web in particular, has exploded in recent years. Many thousands of companies have established "home pages" on the web, through which they communicate advertising and marketing materials, as well as other content, to those who choose to access their sites. Often purchases and other contracts may be made directly online. Frequently links are provided by which browsers may be taken automatically to other sites, with materials and content provided by third parties. Many companies provide access to storehouses of information through their site, becoming significant content providers.

These business websites are often (indeed, perhaps typically) established by marketing personnel with little consideration given to the legal risks that may be incurred. The Internet is a unique medium in that it is effectively borderless, providing instant global exposure for the information made available on the web. This raises thorny questions of the applicable law governing the provider of such information. Laws in well over a hundred countries with Internet access potentially govern advertising content, consumer protection, permissible speech, defamation, intellectual property infringement and myriad other matters. Consider the following examples:

- An Italian publisher is enjoined from publishing its "PLAYMEN" magazine in the United States because it infringes the "PLAYBOY" trademark. Publication in Italy is lawful. The publisher then makes the magazine available over the Internet from a computer in Italy. A federal district court has held that conduct to violate the injunction.[1]
- Virgin Atlantic Airways, a British airline, advertises a discount airfare between Newark and London on the Internet. The U.S. Department of Transportation fined Virgin Atlantic $14,000 for failure to comply with U.S. advertising rules requiring clear disclosure of applicable taxes.[2]
- The Australian affiliate of Project Gutenberg, which posts public domain works of literature online, makes "Gone With the Wind" available on its website. The

---

* *Mr. Jaglom is a member of the New York City firm of Tannenbaum Helpern Syracuse & Hirschtritt LLP.* *The assistance of Matthew R. Maron and Jason B. Klimpl, associates at the firm, is gratefully acknowledged.*

1 *Playboy Enterprises Inc. v. Chuckleberry Publishing Inc.*, 939 F. Supp. 1032 (S.D.N.Y. 1996).

2 L. Rose & J.P. Feldman, *Practical Suggestions for International Advertising and Promotions on the 'Net'*, CYBERSPACE L. at 8 (May 1996).

copyright for the novel has expired in Australia, putting it in the public domain, but remains in force in the United States. How should the Australian site respond to a demand from the copyright holder to take down the novel?

- A major French catalog company decides to put its catalog on the web. Some fifty pages of the catalog sell lingerie, with photographs designed to appeal to the French buyer. What repercussions might there be from the availability of this catalog in fundamentalist Islamic countries? What should counsel advise the company President before his next business trip to Singapore or Iran?[3]

- The French Evin Act of January 10, 1991 forbids all "advertising and direct or indirect promotion" regarding tobacco and, in certain circumstances, alcohol. The French TOUBON law of August 4, 1994 requires that businesses offer their products and services to consumers in the French language.[4] What are the consequences of these laws for websites located outside France but accessible there?

- Finally, the distributor of KaZaA file sharing software is incorporated in Vanuatu in the South Pacific. It is managed from Australia and uses servers based in Denmark. Its source code was last seen in Estonia. The developers live in the Netherlands, where the Netherlands Supreme Court has held its software to be lawful. The U.S. music industry has sued the distributor for copyright infringement under U.S. law in a U.S. court.[5] Does U.S. law apply? Is there jurisdiction? Can any judgment be enforced?

B. *Jurisdictional Questions*

These not so hypothetical situations raise obvious jurisdictional questions. Put aside for the moment the questions of whether foreign countries would apply concepts of jurisdiction similar to those familiar to U.S. counsel, or in the case of some countries would even concern themselves with niceties of jurisdiction. (The capital sentence levied *in absentia* by ayatollahs in Iran on author Salman Rushdie for publication abroad of the allegedly blasphemous "Satanic Verses" suggests that at least some nations would have no difficulty with penalizing conduct on the web.)

Under U.S. law one might argue that the availability of a passive website within a state is insufficient to confer jurisdiction over the operator of the site in that state, at least in the absence of evidence that the site operator purposefully availed itself of the benefits of that state (for

---

[3] A. Bertrand, *Collective Administration of Copyrights, Artists Rights and the Law of Publicity on the Internet: Current Issues and Future Perspectives*, 3 New York State Bar Association International Law and Practice Section Fall Meeting 1227 (1996).

[4] *Id*. at 9. In part due to objections from the European Commission, these laws not have been construed not to apply to broadcasts from abroad of World Cup soccer games and similar sporting events that include otherwise forbidden advertising, which are rebroadcast in France without control over content, nor to advertising legally broadcast from abroad by companies not resident in France. *Id.* In the absence of such international constraints and resulting narrow construction, however, similar laws could obviously have a major impact on website operators. A suit was filed against the Georgia Institute of Technology by private plaintiffs complaining that the English language website set up by Georgia Tech's French campus in Metz violated French law. The case was dismissed in June 1997 on procedural grounds because the plaintiff groups failed to file a police complaint before suing, leaving unresolved the larger substantive issue. *French Purists Lose Their Cases*, N.Y. TIMES (June 10, 1997).

[5] A. *Harmon, Music Industry in Global Fight on Web Copies*, N.Y. TIMES (Oct. 7, 2002).

specific jurisdiction with respect to matters arising out of the website itself) or continuously and systematically conducted part of its general business there (for general jurisdiction over the website operator for all matters). That, indeed, was the holding in *Digital Control Inc. v. Boretronics,*[6] *Mink v AAAA Development LLC,*[7] *Cybersell Inc. v. Cybersell Inc.*[8] and *Bensusan Restaurant Corp. v. King and the Blue Note,*[9] among others.[10] That argument, however, might fail for a national or multinational corporation that does intend its site to be viewed globally.

Many courts have disagreed with the *Bensusan Restaurant* line of holdings. *Inset Systems, Inc. v. Instruction Set Inc.*[11] held that a Massachusetts corporation was subject to jurisdiction in Connecticut by reason of its advertising on a website available for viewing in Connecticut, thus "purposefully avail[ing] itself of the privilege of doing business within Connecticut." *CoolSavings.com Inc. v. IQ Commerce Corp.*[12] held that establishing a website accessible to all states constitutes purposeful establishment of minimum contacts with all states.[13] *National Football League v. Miller,*[14] while purporting to follow *Bensusan,* held that the operator of a passive website was subject to jurisdiction in New York because he profited from sales in interstate commerce of advertising on the website, which caused harm to the plaintiffs in New York and was viewed by many New Yorkers.

---

[6] 161 F. Supp.2d 1183 (W.D. Wash. 2001) (rejecting the passive/active test set forth in *Zippo Mfg. Co. v. Zippo Dot Com Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997) (discussed below), the court ruled that "until the advertiser is actually faced with and makes the choice to dive into a particular forum, the mere existence of a worldwide website, regardless of whether the site is active or passive, is an insufficient basis on which to find that the advertiser has purposely directed its activities at residents of the forum state").

[7] 190 F.3d 333 (5th Cir. 1999).

[8] 130 F.3d 414 (9th Cir. 1997).

[9] 937 F. Supp. 295 (S.D.N.Y. 1996). The Second Circuit affirmed *Bensusan* on other grounds, that New York law is narrower in its assertion of personal jurisdiction than the U.S. Constitution permits. *Bensusan Restaurant Corp. v. King*, 126 F.3d 25 (2d Cir. 1997). New York law "reaches only tortious acts performed by a defendant who was physically present in New York when he performed the wrongful act"' and would not even reach "a New Jersey domiciliary [who was] to launch a bazooka across the Hudson at Grant's tomb. . . in an action by an injured New York plaintiff," or tortious acts committed outside New York by persons who derive substantial revenues from interstate commerce. In *Bensusan*, neither was the case, but this narrower holding offers less comfort to Internet marketers.

[10] *See also, e.g., Wildfire Communications, Inc. v. Grapevine, Inc.*, No. 00-CV-12004-GAO (D. Mass. Sept. 28, 2001) (the existence of a website accessible by Massachusetts citizens countered by a lack of actual purchases by Massachusetts customers is not sufficient to subject an out of state website to jurisdiction in Massachusetts); *Perry v. RightOn.com*, 90 F. Supp. 2d 1138 (D. Or. 2000); *Northern Lights Technology, Inc. v. Northern Lights Club*, 97 F.Supp.2d 96 (D. Mass. 2000); *K.C.F.C. v. Nash*, 49 U.S.P.Q.2d (BNA) 1584, 1998 U.S. Dist. LEXIS 18464 (S.D.N.Y. Nov. 24, 1998), *reported in* 57 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 136 (Dec. 17, 1998); *Hearst Corp. v. Goldberger*, 1997 U.S. Dist LEXIS 2065, 1997 WL 97097 (S.D.N.Y. 1997); *Pavlovich v. Superior Ct. of Santa Clara County*, 58 P.3d 2 (Cal. Sup. Ct., 2002) (Internet publication of DVD decryption code, even with knowledge of possible harm to California resident, is not enough to show conduct expressly aimed at California and does not satisfy purposeful availment test).

[11] 937 F. Supp. 161 (D. Conn. 1996).

[12] 53 F. Supp. 2d 1000 (N.D. Ill. 1999).

[13] *See also Remsburg v. Docusearch Inc.*, 2002 WL 130952, 2002 DNH 35 (D. N. H. 2002) (five transactions with New Hampshire resident by which he obtained information used to murder victim, plus a pretextual call to victim by defendant to obtain requested information, were sufficient for jurisdiction over defendant in wrongful death action). *See also Haelan Products, Inc. v. Beso Biological Research, Inc.*, 43 U.S.P.Q.2d (BNA) 1672, 1997 U.S. Dist. LEXIS 10565 (E.D. La. 1997) (website, plus 800 telephone number and advertisements in nationally circulated publications sufficient to consider jurisdiction).

[14] 54 U.S.P.Q. 2d 1574 (S.D.N.Y. 2000).

Similarly, consider *United States v. Thomas*,[15] affirming the *criminal* conviction on obscenity charges in federal court in Tennessee of a California couple who sold sexually explicit photographs by making them available for downloading from a computer bulletin board in California. The offending materials were downloaded in Tennessee by a United States Postal Inspector acting on the complaint of a Tennessee resident. The defendants argued that venue in Tennessee was improper because they did not cause the files to be transmitted to Tennessee. That was done by the zealous postal inspector. The Sixth Circuit held otherwise, finding substantial evidence that the defendants set up their bulletin board so that persons in other jurisdictions could access it.[16] The Sixth Circuit therefore held not only that venue in Tennessee was proper, but that the appropriate community standards to be applied in determining whether the materials were obscene were those of Tennessee.[17]

Other cases have upheld jurisdiction based on forum state activities beyond mere website accessibility, such as advertising in forum state media, sales of passwords or services to or communications with forum state residents, contracting for forum state access with Internet service providers, explicit on-line solicitations and some level of interactivity or information gathering.[18]

---

15 74 F.3d 701 (6th Cir. 1996).

16 In addition, the court found the defendants to have specifically approved the distribution of offending materials to a Tennessee resident by calling the postal inspector in Tennessee in response to a message he left at their bulletin board and providing him with an account number to use in accessing their service. The tenor of the Sixth Circuit's opinion suggests that this fact may not have been dispositive, but it certainly provides a greater degree of intentional contact with the forum than the pure establishment of a website accessed by others with no direct interaction with the site operator, as was the situation in the *Maritz* case.

17 *Id.* at 709-11.

18 *See, e.g., Abiomed, Inc. v. Turnbull,* 379 F.Supp.2d 90 (D. Mass. 2005) (postings on Yahoo! electronic message board directed to forum state residents constituted sufficient contacts with forum to support jurisdiction); *First Act, Inc. v. Brook Mays Music Co,* .311 F. Supp. 2d 258 (D. Mass. 2004) (emails sent to forum state residents constituted sufficient contacts with forum to support jurisdiction); *National College Athletic Ass'n v. BBF Int'l*, No. 01-422-1, U.S. Dist. Ct. (E.D. Va. May 4, 2001), *reported in* WORLD INTERNET L. Rep. (BNA) June 2001, at 23 (in ruling on a domain name dispute, Virginia court exercised jurisdiction over defendant Haitian entity which marketed its gambling websites in Virginia and entered contracts with Virginia residents); *Starmedia Network Inc. v. Star Media Inc.*, 2001 WL 417118 (S.D.N.Y. Apr. 23, 2001), *reported in* 62 PATENT, TRADEMARK & COPYRIGHT J. 153 (BNA) (May 11, 2001), at 41 (New York long arm statute reached Washington state defendant that operated a website serving a national market even though the website had no New York customers, but did have potential business in New York); *Internet Doorway Inc. v. Parks,* 138 F.Supp.2d 733 (S.D. Miss. 2001), *reported in* WORLD INTERNET L. Rep. (BNA) June 2001, at 20 (the action of sending an e-mail message to a Mississippi resident established the necessary minimum contacts to exercise specific personal jurisdiction over such sender in Mississippi); *Ty Inc. v. Baby Me Inc.*, N.D. Ill., No. 00 C 6016 (Apr. 6, 2001), *reported in* 62 PATENT, TRADEMARK & COPYRIGHT J. 153 (BNA) (May 11, 2001), at 40 (sale of three plush toys to Illinois resident through defendant's website subjected Hawaiian defendant to jurisdiction in Illinois); *Kollmorgen Corp. v. Yaskawa Electric Corp.*, 169 F.Supp.2d 530 (W.D. Va. Dec. 13, 1999) (subsidiary's website conveying impression parent and subsidiary acted in consort to place goods in stream of commerce was enough to establish jurisdiction over parent); *American Network, Inc. v. Access America/Connect Atlanta, Inc.*, 975 F. Supp. 494 (S.D.N.Y. 1997); *Digital Equipment Corp. v. Altavista Technology Inc.*, 960 F. Supp. 456 (D. Mass. 1997); *Rubbercraft Corp. of California v. Rubbercraft, Inc.*, 1997 WL 835442 (C.D. Cal. Dec. 17, 1997), *reported in* 55 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 358 (Feb. 26, 1998) (website, toll-free telephone number, advertising in national media and significant income from sales in forum state supports personal jurisdiction); *Maritz Inc. v. CyberGold Inc.*, 947 F. Supp. 1328 (E.D. Mo. 1996), (operation of a California website that asked customers to add their addresses to targeted email addressing system constituted "active solicitation" sufficient to satisfy the "minimum contacts" requirement for jurisdiction in Missouri; and defendant was found to be "purposely avail[ing] itself" of privilege of conducting activities in Missouri); *Heroes Inc.*

The jurisdictional standard of purposefully availing oneself of the privilege of doing business in a state is met, for purposes of claims arising from the defendant's activities in a state, where there are numerous transactions with residents of the state. Thus where a domain name registrar was alleged to have engaged in some 5,000 transactions with Ohio residents and its site was accessible in Ohio, the Sixth Circuit held in *Bird v. Parsons*[19] that it was subject to its jurisdiction in a trademark infringement suit, since the infringement arose from the registration business.[20] The D.C. Circuit similarly found jurisdiction over a defendant whose website allowed Washington, D.C. residents to form contracts with it to buy securities and brokerage services in *Gorman v. Ameritrade Holding Corp.*[21] The Court distinguished *GTE New Media Services Inc. v. BellSouth Corp.*,[22] where a yellow pages website was "essentially passive," allowing customers to obtain information, but not to contract with the defendants. And in the KaZaA situation described in the last bullet of section I.A. above, the millions of downloads of KaZaA software in California were held to confer jurisdiction over the software's distributor in a contributory copyright infringement claim.[23] Similarly, in *Chloe v. Queen Bee of Beverly Hills, LLC,*[24] the Second Circuit, reversing the district court, held that a California online retailer was subject to personal jurisdiction in New York for trademark infringement in an action involving the shipping of counterfeit designer purses to New York where such goods were ordered through the defendants' website. The court reasoned that minimum contacts were established under New York's long-arm statute, among other things, since at least 50 incidents of sales of the allegedly infringing goods to New Yorkers had been accomplished through the defendants' website. Most recently, in *Signazon Corp. v. Nickelson*, the court declined to dismiss plaintiff's copyright and trademark infringement claims because website sales established minimum contacts in the forum jurisdiction to support a finding of personal jurisdiction.[25]

Likewise, in *UBID Inc. v. The GoDaddy Group Inc.*[26] the Seventh Circuit held that GoDaddy, a domain name registrar based in Arizona, was subject to general and specific personal jurisdiction in Illinois under the Anti-Cybersquatting Consumer Protection Act for registering domain names that infringed on the trademarks of defendant, despite the lack of evidence that GoDaddy specifically targeted its activities in Illinois. The Seventh Circuit reversed the lower court's finding of lack of jurisdiction by stating that GoDaddy had sufficient

---

v. Heroes Foundation, 958 F. Supp. 1 (D. D.C. 1996); *EDIAS Software Int'l LLC v. BASIS Int'l Ltd.*, 947 F. Supp. 413 (D. Ariz. 1996).

19 289 F.3d 865 (6th Cir. 2002).

20 *See also Neogen Corp. v. Neo Gen Screening, Inc.*, 282 F. 3d 883 (6th Cir. 2002) (passive website available in Michigan, that also let Michigan residents use passwords to view blood test results, with at least 14 transactions with Michigan residents, constituted purposeful availment sufficient for jurisdiction; citing *Zippo Mfg. Co*, *infra*).

21 293 F.3d 506 (D.C. Cir. 2002).

22 199 F.3d 1342 (D.C. Cir. 2000).

23 *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 243 F. Supp. 2d 1073 (C.D.Cal. 2003) (Order Denying Defendant Sharman Networks Ltd.'s and Defendant Lef Interactive's Motions to Dismiss). *See also Arista Records, Inv. v. Sakfield Holding Co. S.L.*, 314 F.Supp.2d 27 (D.D.C. 2004) (multiple downloads of files from defendant's website by D.C. residents was "purposeful, active, systematic, and continuous activity" in D.C.); *see also Shropshire v. Canning*, 809 F. Supp. 2d 1139 (N.D.Cal. 2011) (where Canadian citizen uploaded infringing video to YouTube's servers in California, and the video was accessible to and viewed by potentially thousands of people in the U.S., the act of infringement was not "wholly extraterritorial" to the U.S. and was subject to the U.S. Copyright Act).

24 *Chloe v. Queen Bee of Beverly Hills, LLC*, 09-3361-cv (2d Cir. 2010), *reported in* Law.com (Aug. 9, 2010), *available at* http://www.law.com/jsp/article.jsp?id=1202464392587&rss=newswire.

25 2013 WL 3168372 (D. Mass, June 20, 2013).

26 *UBID Inc. v. The GoDaddy Group Inc.*, 623 F.3d 421(7th Cir 2010).

minimum contacts due to its national advertising campaign and the "hundreds of thousands" of transactions between GoDaddy and Illinois residents. This case suggests that advertising, coupled with online services accessible – and in fact accessed – from other jurisdictions, is sufficient to establish personal jurisdiction.

The Seventh Circuit also recently held that a Native-American cigarette sales business operating out of Colorado was subject to personal jurisdiction in Illinois because the business (i) maintained a commercial venture online, (ii) shipped to every state except New York, and (iii) purposefully availed itself of opportunities in Illinois by shipping cigarettes to Illinois residents.[27]

A growing number of cases have followed *Zippo Manufacturing Co. v. Zippo Dot Com Inc*.,[28] which developed a relatively simple active/passive test for determining jurisdiction over a website operator. Websites are categorized on a spectrum from purely passive sites that merely make information available to visitors, which do not alone provide a basis for jurisdiction, through levels of increasing interactivity to full e-commerce sites that permit online contracts and transactions with forum residents, which do suffice as a jurisdictional basis in the forum. The more interactive the site, the more likely jurisdiction is to be found. In one case, a district court held that a website with hyperlinks that generated revenue for the site when clicked under a pay-per click arrangement was sufficiently interactive to create jurisdiction in Illinois, where the site was devoted to Illinois attractions and made money from Illinois-related links.[29]

The *Zippo* approach has been criticized by some courts. A number have rejected the *Zippo* approach in favor of the reasoning of *American Information Corp. v. American Infometrics, Inc.*,[30] which applied a "targeting-based" test that asks whether the defendant's actions were aimed at the forum state to determine if jurisdiction was proper.[31]

---

[27] *State of Illinois v. Hemi Group LLC,* No. 09-1407, 2010 U.S. App. LEXIS 19126 (7th Cir., Sept. 14, 2010) *reported in* http://www.foley.com/publications/pub_detail.aspx?pubid=7521&elq_mid=11204&elq_cid=996107#page=1

[28] 952 F. Supp. 1119 (W.D. Pa. 1997) (developing the active/passive test, which gave the court the power to exercise jurisdiction over an extra-jurisdictional website operator if the website was an interactive site, but not if it was a passive site that merely provided information). *See, e.g., 3M Co. v. Icuiti Corp.*, 2006 WL 1579816 (D. Minn. 2006) (unpublished opinion) (nationwide advertising including Minnesota and sales to Minnesota, including five website sales, were sufficient for jurisdiction), *available at* http://pub.bna.com/ptcj/052945June1.pdf; *ALS Scan Inc. v. Digital Service Consultants Inc.* 293 F.3d 707 (4th Cir. 2002); *Neogen Corp., supra*; *Litmer v. PDQUSA.com*, 326 F.Supp.2d 952 (N.D. Ind. 2004); *Med-Tec Iowa Inc. v. Computerized Imaging Reference Systems Inc.*, 223 F.Supp.2d 1034 (S.D. Iowa 2002); *Euromarket Designs, Inc. v. Crate & Barrel Ltd.*, 96 F. Supp. 2d 824 (N.D. Ill. 2000); *Search Force, Inc. v. Dataforce Int'l, Inc.*, 112 F. Supp. 2d 771 (S.D. Ind. 2000); *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998) (website providing political gossip and rumor and providing for e-mail communications and e-mail subscriptions, was interactive and subject to jurisdiction in the District of Columbia).

[29] *Chicago Architectural Foundation v. Domain Magic, LLC,* 2007 WL 3046124 (N.D. Ill. 2007).

[30] 139 F. Supp. 2d 696 (D. Md. 2001).

[31] *See, e.g., Wilkerson v. RSL Funding, LLC*, 2011 WL 3516147 (Tex. App. Ct. Aug. 11, 2011) reported by Eric Goldman's *Technology and Marketing Blog* on Aug. 23, 2011 (in bypassing the Zippo test – and resorting to a purposeful availment standard – the court stated that the interactive features of Yahoo! and Yelp are creations of the owners of the sites and their "interactive" nature cannot be imputed to an individual user for purposes of determining whether minimum contacts were established for jurisdictional purposes); *ISI Brands Inc. v. KCC Int'l Inc.*, 458 F. Supp. 2nd 81 (E.D.N.Y. 2006) (lack of sales by interactive website to forum other than two sales arranged by plaintiff insufficient to show targeting of New York residents); *Hy Cite Corp. v. Badbusinessbureau.com*, 297 F.Supp.2d 1154 (W.D.Wis. 2004) (interactive website, sale of one book and exchange of emails insufficient to show purposeful availment, targeting of Wisconsin citizens; rejecting *Zippo*); *Ottenheimer Publishers, Inc. v. Playmore, Inc.*, 158 F. Supp. 2d 649 (D. Md. Aug. 13, 2001); *Starmedia Network, Inc. v. Star Media, Inc.* 2001 WL 417118

Alternatively, the jurisdictional question in *Systems Designs Inc. v. New CustomWare Co.*[32] was decided based on the Californian defendant's satisfaction of minimum contacts in Utah under a looser "effects test" – the effects of defendant's actions in Utah were sufficient to assert jurisdiction. The defendant's relevant actions were its use of a trademark registered to a Utah company and its maintenance of a website from which services could be purchased by Utah residents (although none had been) and which listed sample clients with substantial connections to Utah. The First Circuit found no jurisdiction over a Japanese company and its website for adopting the name of an American jazz musician who brought a Lanham Act claim, finding no substantial effect in the U.S., where the defendant's website was written in Japanese and hosted from Japan, especially as the only U.S. sales were induced by the plaintiff for purposes of the litigation.[33]

An "effects" test is quite broad in application, making online operators subject to suit whenever their activities cause consequences, while a "targeting" test seems more inline with traditional notions of "purposeful availment." The majority of courts seem to follow the *Zippo* active/passive analysis, with a growing number requiring "purposeful availment" in the form of targeting the forum state as an additional element[34].

Other courts have cited *Calder v. Jones*[35] for the proposition that the "effects" test also requires intentional "targeting" of the forum state. In *Dudnikov v. Chalk & Vermilion Fine Arts, Inc.*,[36] the plaintiffs operated from their home in Colorado a business selling fabrics and printed products on eBay. When the out-of-state owners of a copyrighted image saw that the plaintiffs had used a similar image in their products, the copyright owners utilized eBay's Verified Rights Owner Program, under which eBay may automatically terminate an ongoing auction when it receives a notice of claimed infringement. eBay cancelled the auction of the plaintiffs' products. When the plaintiffs sought a declaratory judgment against the copyright owners in a federal court in Colorado, the copyright owners moved to dismiss based on the court's lack of personal jurisdiction. Reversing the district court's holding that there was no jurisdiction, the Tenth Circuit noted that personal jurisdiction may be asserted where the defendants have "expressly

---

(S.D.N.Y. Apr. 23, 2001). *See also Aero Products Int'l Inc. v. Intex Corp.*, 2002 WL 31109386 (N.D. Ill. 2002), *reported in* 65 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 15, *available at* http://pub.bna.com/ptcj/022590.pdf.; *First Act, Inc. v. Brook Mays Music Co.*, 311 F.Supp.2d 258 (D. Mass. 2004) (finding personal jurisdiction based on sixty emails sent by defendant knowingly to Massachusetts residents, where emails were the subject of the suit).

32 248 F. Supp. 2d 1093 (D. Utah 2003).

33 *McBee v. Delica Co.*, 417 F.3d 107 (1st Cir. 2005), *reported in* 70 PAT.,TM & Copyr.J. (BNA) 439 (Aug. 12, 2005) *available at* http://pub.bna.com/ptcj/042733Aug2.pdf; *The Bear Mill, Inc. v. Teddy Mountain, Inc.*, 2008 WL 2323483, No. 2:07-CV-492-ETC-LMB (D. Idaho 2008) (personal jurisdiction proper under the "effects test" where website was accessible in Idaho and resulting harm in Idaho).

34 *E.g., Pebble Beach Co. v. Caddy*, 453 F. 3d 1151(9th Cir. 2006) (availability of website in California insufficient for jurisdiction without showing targeting of California residents or other directing of activities at California); *Carefirst of Maryland Inc. v. Carefirst Pregnancy Centers Inc.*, 334 F.3d 390 (4th Cir. 2003) (in order to find jurisdiction over Illinois company the company must have acted with manifest intent to reach Maryland residents which requires more than maintenance of a semi-interactive website); *Toys "R" Us, Inc. v. Step Two, S.A.*, 318 F. 3d 446 (3rd Cir. 2003) (approving *Zippo* but holding that Spanish language-only commercially interactive website of Spanish company that shipped goods only within Spain was not sufficient to support personal jurisdiction in New Jersey; however, jurisdictional discovery was warranted based on the possible existence of the requisite contacts to show purposeful availment of conducting activity in New Jersey, which may include non-Internet activities).

35 465 U.S. 783.

36 514 F.3d 1063 (10th Cir. 2008).

aimed" their activities at the forum state knowing that the "brunt of the injury" would be felt in the forum state:

> Defendants sent a [Notice of Claimed Infringement] to eBay expressly intending (and effectually acting) to suspend plaintiffs' auction in Colorado. Plaintiffs' suit arises from, and is indeed an effort to reverse, the intended consequences of defendants' NOCI which they incurred in Colorado. [Moreover] defendants knew plaintiffs' business was located in Colorado. And defendants point us to no basis in traditional notion of fair play or substantial justice that would preclude suit in that forum.[37]

Similarly, in *Righthaven LLC v. MajorWager.com Inc.,*[38] the United States District Court for the District of Nevada held that MajorWager.com, a Canadian website operator that published an article without authorization from the copyright owner, was subject to personal jurisdiction in Nevada. The court stated that the *Calder* "effects test" was met since MajorWager.com committed an act of infringement that it knew would result in injury in the forum state (i.e., the injured plaintiff was located in Las Vegas). Likewise, the U.S. Court of Appeals for the Ninth Circuit applied the *Calder* test to rule that an Ohio-based Hollywood gossip website directed its activities towards California after finding many of the advertisements on the site were targeted at California residents.[39] The Ninth Circuit also recently found that the fact that a website had purchased "California" as a Google AdWord to be among the facts that indicated a purposeful direction toward California.[40] These rulings suggest that commercial media websites that seek a national range of users can expect to be subject to suit in a multitude of states.

And in 2011, the highest court in New York ruled that where a defendant uploads infringing material owned by a New York copyright owner to the Internet, the location of the alleged injury is the location of the copyright owner, because the infringer's aim is "to make the works accessible to anyone with an Internet connection, including computer users in New York."[41] It further noted that "the place of uploading is inconsequential and it is difficult, if not impossible, to correlate lost sales to a particular geographic area." The Court of Appeals did note that for jurisdiction to attach, the defendant must reasonably expect there to be consequences in New York and must derive substantial revenue from interstate commerce, and there must be the constitutionally required "minimum contacts" with the State.

Across the Atlantic, German prosecutors indicted the general manager of Compuserve's German operation on charges of trafficking in pornography because it provided Internet access to its customers without blocking independent child pornography sites, as well as failing to block

---

[37] 514 F.3d at 1082; *See also Licciardello v. Lovelady*, 544 F.3d 1280 (11th Cir. 2008) (Florida district court's jurisdiction over a non-resident defendant proper where defendant posted infringing materials on a website accessible in Florida because the conduct was "expressly aimed at a specific individual in the forum whose effects were suffered in the forum").

[38] *Righthaven LLC v. MajorWager.com Inc.*, No. 10-484 (D. Nev. 2010), *reported in* 81 PATENT, TRADEMARK & COPYRIGHT JOURNAL 1990 (BNA) 57 (Oct. 12, 2010).

[39] *Mavrix Photo Inc. v. Brand Technologies Inc.*, 9th Cir. No. 09-56134 (Aug. 8, 2011) reported in Bason, *9th Cir: Calif.- Focused Ads, Adwords Sufficed for Jurisdiction in Two Disputes,* 82 PAT., TRADEMARK & COPYRIGHT J. 2027 (Aug. 12, 2011).

[40] *CollegeSource Inc. v. AcademyOne Inc.*, 9th Cir. No. 09-56528 (Aug. 8, 2011) reported in Bason, *9th Cir: Calif.- Focused Ads, Adwords Sufficed for Jurisdiction in Two Disputes,* 82 PAT., TRADEMARK & COPYRIGHT J. 2027 (Aug. 12, 2011).

[41] *Penguin Group (USA) Inc. v. American Buddha*, 2011 WL 1044581 (N.Y.Ct.App. March 24, 2011), *reported in* PAT., TRADEMARK & COPYRIGHT J. 714 (BNA) (April 1, 2011).

sites with Nazi and neo-Nazi material, which are illegal in Germany.[42] After conviction, he was given a two year suspended prison sentence and fined.[43] The guilty verdict was finally overturned in November 1999, based on a new multimedia law enacted after the conviction.[44] The incident nonetheless suggests the risks of non-compliance with foreign law.

In France, a court held it had jurisdiction to hear a trademark case brought by a French trademark owner alleging infringement by a U.S.-based Internet site.[45] In contrast, a Dutch court declined jurisdiction over a U.S. company website alleged to have infringed a trademark, finding the site wasn't directed at the Benelux public because it was a .com domain, in English only, prices were in dollars, and products could not be delivered in the Netherlands, among other factors.[46] And, more recently, the French Supreme Court held that a website that did not target the French public did not infringe French trademarks.[47]

The French courts have also asserted jurisdiction over Yahoo! Inc., a California-based Internet company, as a result of various Nazi items offered on Yahoo!'s auction site, which was accessible by users in France, in contravention of French law[48] prohibiting the display or sale of racist material.[49] The presiding judge ordered Yahoo! to block French users from viewing Nazi memorabilia;[50] however, in a later decision he declined to go so far as to impose an obligation upon Internet service providers to block access to racist material.[51] The Yahoo! ruling was upheld on appeal[52] and generated significant concern over the repercussions that such a decision, which would allow one country to regulate access to sites originating elsewhere, would have on the entire Internet. (An April 2002 European Parliament vote opposing such blocking of website content in favor of self-regulation by Internet service providers may limit such orders in the future.[53] But despite the Parliament vote, Deutsche Bahn AG has moved against Internet search engines Google, Yahoo! and Alta Vista seeking the removal of links to sites of extremist groups with information on rail sabotage.[54])

---

42 *Germany Charges Compuserve Manager*, N.Y. TIMES, Apr. 10, 1997, at D19.

43 *Morning Briefcase*, DALLAS MORNING NEWS, May 29, 1998, at 2D, *cited in* P. Swire, *Of Elephants, Mice and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991, 992 n.5 (1998).

44 *German Court Overturns Pornography Ruling Against Compuserve*, N.Y. TIMES, Nov. 18, 1999, at C4.

45 *Saint-Tropez Commune v. SA Eurovirtuel*, *reported in* 53 INTA Bulletin No. 3, Feb. 1, 1998, at 2.

46 *Allergan v. Basic Research & Kleinbecker USA*, case no. 243729, (The Hague Dist. Ct. Aug. 25, 2005), *reported in* WORLD INTERNET L REP. (BNA) (Nov. 2005) at p. 15.

47 *Hugo Boss v. Reemtsma Cigarettenfabrik* (French Sup. Ct. Jan. 11, 2005), *reported in* WORLD INTERNET L. REP. (BNA) (Sept. 2005) at p. 9.

48 Section R645-1 of the French Criminal Code.

49 *Association Union des Etudiants Juifs de France et al. v. Yahoo! Inc.*, *reported in* WORLD INTERNET L. REP. (BNA) (7/00).

50 *Judge leaves screening of racist material to French ISPs*, Oct. 31, 2001, *available at* www.stormfront.org/forum/t4819.

51 *ISPs Not Obligated to Block Access to Hate Portal: Action Internationale pour la Justice, La Licra et al. v. Association Franchaise d'Acces et de Services Internet et al.*, *reported in* WORLD INTERNET L. REP. (BNA) (Dec. 2001). Similarly, on July 27, 2001, a German court ruled that a German Internet domain registry was not responsible for web content, but rather the party seeking action against a website must address the owner of the site. *See Registry Not Responsible For Web Content*, *reported in* CASE REPORTS (BNA) Oct. 2001, at 20.

52 John Tagliabue, "French Uphold Ruling Against Yahoo on Nazi Sites," N.Y. TIMES, Nov. 21, 2000, at C8.

53 T. Richardson, "Europe Elbows Internet Content Blocking"; THE REGISTER (11/4/2002); http://www.theregister.co.uk/content/6/24808.html.

54 J. Evers, "German Railway Operator to Sue Google over Sabotage Links," COMPUTERWORLD (4/16/2002).

Yahoo! sought to have the U.S. Courts rule the French judgment unenforceable in the U.S. under the First Amendment. Initially, a U.S. District Court ruled in favor of Yahoo!, but the Ninth Circuit reversed, holding there was no jurisdiction in the U.S. over the French groups that had won the judgment against Yahoo! in France, although the Court of Appeals has granted rehearing *en banc*.[55] (Another federal district court has also refused to enforce a French judgment against a U.S. website operator on First Amendment grounds, holding the website operator to be protected in its posting of photos of a fashion show to which the designer had objected.[56]) Some commentators believe the French court's attempt to restrict Nazi memorabilia on Yahoo! may be a harbinger of an Internet where geolocation techniques determine which sites a viewer may enter based on the laws of and restrictions imposed by the country, state or even city from which such viewer is surfing the Internet.[57] And if Yahoo! had substantial assets in France, the daily fine levied on Yahoo! by the French court for failure to comply with its order might well be meaningful.

Moreover, even in the U.S., there are efforts to require blocking of unacceptable websites, as evidenced by a Pennsylvania statute requiring Internet service providers to block access by Pennsylvania residents to websites containing child pornography or face criminal penalties.[58] (The statute was held unconstitutional in September 2004).[59] In contrast, legislation has been proposed in Congress to create an office of Global Internet Freedom to fight Internet blocking and provide technological means to circumvent censorship tools.[60] Aimed at censorship by such authoritarian regimes as China and North Korea, the legislation seems to demonstrate that the merits of Internet blocking lie in the eye of the beholder, justified in the eyes of the French for Nazi memorabilia and of Pennsylvanians for child pornography, but an evil to be combated by Congress where used to restrict freedom of information. Given worldwide differences in viewpoint, a crazy-quilt of rules is the foreseeable result.

The result of that situation is equally predictable: content will be hosted where it is unrestricted, with ISPs left to try to block access in countries where material is unlawful. Already, in the wake of the U.S. *Yahoo!* decision, an Australian hate site that would violate Australian anti-racism laws has been moved to a U.S. host.[61] One approach to dealing with the morass is Google's practice of excluding from its French and German listings − but not from the main google.com search engine − sites objectionable in those countries. Given that French and German users can access google.com, it is questionable whether this approach will be found to comply with the law in these nations.[62]

---

55 *Yahoo! Inc. v. La Ligue Contre Le Racisme Et l'Antisemitisme*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev'd*, 379 F.3d 1120 (9th Cir. 2004) (rehearing en banc granted).

56 *Louis Féraud Int'l S.a.r.l. v. Viewfinder, Inc. d/b/a Firstview.com*, 2005 WL 2420525L (S.D.N.Y. 2005).

57 Lisa Guernsey, "Welcome to the Web. Passport, Please?," N.Y. TIMES, Mar. 15, 2001, at G1.

58 PA crimes code, 18 Pa.Cons.Stat. § 7330, Internet Child Pornography. *See Application of Fisher*, No. Misc. 689 Jul 02 (Ct. Common Plans, Montgomery Co. Sept. 17, 2002) (order requiring Internet service provider to remove or disable access to child pornography) *available at*: http://www.steptoe.com/publications/219e.pdf.

59 *Center for Democracy and Technology v. Pappert*, 337 F.Supp.2d 606 (E.D.Pa. 2004).

60 *See* c|net news.com (Oct. 3, 2002), http://news.com.com/2102-1023-960679.html; J. Straziuso, "Lawsuit Claims Net Filters Overcensor, Wants Reversal," USA TODAY (Jan. 6, 2004), http://www.usatoday.com/tech/news/techpolicy/2004-01-07-censor-law-appeal_x.htm.

61 See Internet Law News (BNA) (Sept. 30, 2002).

62 See D. McCullagh, "Google Excluding Controversial Sites," c|net news.com (Oct. 23, 2002) at http://news.com.com/2100-1023-963132.html.

The French Yahoo! decision is by no means unique. A Milan appeals court's recent ruling on a defamation claim follows the same logic. The court ruled that a defamation claim against a site created in Israel was prosecutable despite Italian case law disallowing the prosecution of defamation that originates outside of Italy. The Milan court distinguished the case by citing the fact that Italian Internet users needed Italy-based service to view offending pages.[63]

Likewise, the High Court of Australia has ruled that a Barron's online article containing allegedly defaming material which originated on Dow Jones & Co.'s servers in New Jersey was also "published" in Australia via the web; therefore a defamation suit based on the article could properly be brought under Australia's strict defamation laws, at least where the plaintiff lived in Australia and Dow Jones explicitly sold subscriptions to Barron's online to Australians.[64] This Australian ruling would create liability for on-line publishers anywhere their material is read, or at least wherever a potential victim might be found.

The England and Wales High Court reached a similar result, finding jurisdiction over a Nevada-based company and a New York attorney that published articles online allegedly defaming Don King, the U.S. based boxing promoter.[65] The Court held words are published where they can be read, and that King had a reputation to protect in England. To similar effect is a Scottish decision holding that "Scottish courts have jurisdiction over . . . a threatened wrong that is likely to produce a harmful event within Scotland" and concluding that any country in which a website has a significant impact should have jurisdiction.[66]

However when a Canadian lower court followed this approach, finding jurisdiction over a series of Washington Post articles accusing a U.N. official of improprieties while stationed in Kenya, because the articles were accessible online in Ontario and the plaintiff had been living in Ontario for two years at the time, so that the damage to his reputation would be greatest in Ontario, the decision was reversed.[67] The Ontario Court of Appeal held that there was no "real and substantial connection" between Ontario and the plaintiff's claims, and that it "was not reasonably foreseeable" when the articles were written that the plaintiff "would end up as a resident or Ontario three years later." The Court of Appeal stated, "To hold otherwise would mean that a defendant could be sued almost anywhere in the world based upon where a plaintiff may decide to establish his or her residence long after the publication of the defamation."

Conversely, English Court of Appeal held that an English penal law prohibiting the publishing of racially inflammatory material yielded jurisdiction over defendants who uploaded such material to a website hosted by a server in California. The court reasoned that the defendants wrote, edited and uploaded the material while physically in England. Thus, in the

---

63 *Controlling Access to Foreign websites: In re Dulberg*, WORLD INTERNET L. REP. (BNA), Feb. 2001, at 14.

64 *Dow Jones & Co., Inc. v. Gutnick* (2002) 194 A.L.R. 433, [2002] H.C.A. 56 (Australia). A complaint challenging the Australian High Court ruling under the Optional Protocol to the International Covenant on Civil and Political Rights has been filed with the United Nations High Commissioner for Human Rights, arguing that the High Court ruling subjects publishers to suit in multiple jurisdictions in violation of the Protocol. M. Rose, "Dow Jones Employee Appeals to U.N. in Libel Case," WALL ST. J. p. 34 (April 16, 2003).

65 *King v. Lewis* [2004] EWHC 168 (QB) (06 February 2004) *available at* http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWHC/QB/2004/168.html&query=title+%28+King.+%29+and+title+%28+v.+%29+and+title+%28+Lewis+%29&method=boolean.

66 *Bonnier Media Ltd. v. Smith*, available at www.scotcourts.gov.uk/opinions/DRU2606.html. *See also* "Frenchman Sentenced in Senegal for Internet Libel," *available at* http://www.qlinks.net/items/qlitem17391.htm.

67 *Bangoura v. Washington Post* (Ontario Sup. Ct. Justice January 27, 2004), *available at* www.canlii.org/on/cas/onsc/2004/2004onsc10181.html, *reported in* WORLD INTERNET L. REP. (BNA) 14 (Feb.2004), *rev'd* (Ontario Court of Appeal Sept. 16, 2005) *reported in* Toronto Star (Sept. 16, 2005).

court's view, the defendants had engaged in substantial publishing activities in England. Notably, the defendants' conduct would not have been a crime in California.[68]

While the Supreme Court has not yet ruled on the issue of Internet jurisdiction, several federal court decisions are in line with the Ontario appellate decision and contrary to the other international decisions discussed above. The Fourth Circuit dismissed a libel action brought in Virginia by a Virginia prison warden against two Connecticut newspapers, holding their articles, posted on their websites, about treatment of Connecticut prisoners housed in Virginia prisons was aimed at a Connecticut audience and not at Virginia, and so there was no jurisdiction over the newspapers in Virginia.[69] The Fifth Circuit affirmed a dismissal for lack of personal jurisdiction in a defamation suit in Texas by the former Associate Deputy Director of the FBI over an article posted on a Columbia University-hosted Internet site, where the article made no reference to Texas and was not directed particularly at Texas readers.[70] And the Eastern District of Pennsylvania held that a passive website for offshore gambling fans that allegedly defamed a Pennsylvania resident was not subject to jurisdiction in Pennsylvania, because it had not intentionally aimed its tortious conduct at the forum state. The Court held, "There is a difference between tortious conduct targeted at a forum resident and tortious conduct expressly aimed at the forum. Were the former sufficient, a Pennsylvania resident could hale into court in Pennsylvania anyone who injured him by an intentional tortious act committed anywhere."[71]

A New Jersey appellate court, however, upheld long-arm jurisdiction in New Jersey where a California resident posted disparaging comments about a New Jersey resident, town, police department and the New Jersey resident's neighbors. The court found that this "targeting" provided reason to foresee being haled into court in New Jersey.[72] Similarly, a federal court in Texas found jurisdiction (although it dismissed the complaint for failure to state a claim) over a non-resident defendant who posted allegedly defamatory statements on a website focused on Texas history about a plaintiff who had indicated in an earlier posting that she lived in Texas. The court held the defendant knew the brunt of any injury would be felt in Texas.[73]

In *Internet Solutions Corporation v. Marshall*,[74] the court held that comments posted by an out-of-state blogger which allegedly defamed a Florida company could not, without more, satisfy the due process clause and yield jurisdiction over the author in Florida. In its holding, the court noted that the blogger-author did not specifically target Florida residents.

As the law in this area was developing, some commentators argued that the reasonable solution to such problems was to apply to those making information available on the Internet the

---

[68] *Reported in Court of Appeal finds racist material hosted in California is subject to English law*, Lexology (March 24, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=d6e9a46d-fd20-4cf0-8452-f213fcee9bf2.

[69] *Young v. New Haven Advocate*, 315 F.3d 256 (4th Cir. 2002), *cert. denied* 123 S. Ct. 2092 (May 19, 2003).

[70] *Revell v. Lidov*, 371 F.3d 467 (5th Cir. 2002).

[71] *English Sports Betting, Inc. v. Tostigan*, 2002 WL 461592 (E.D. Pa. 2002). *See also Oxford Round Table, Inc. v. Mahone*, 2007 WL 3342288 (W.D. Ky. 2007) (no jurisdiction over resident of England who allegedly defamed Kentucky corporation), *available at* http://www.steptoe.com/assets/attachments/3276.pdf.com

[72] *Goldhaber v. Kohlenberg*, 395 N.J. Super. 380, 928 A. 2d 948 (Super. Ct. N.J. App. Div. 2007), *available at* http://pdfserver.amlaw.com/nj/Goldhaber.pdf.

[73] *McVea v. Crisp*, 2007 WL 4205648 (W.D. Tex. 2007), *available at* http://www.steptoe.com/assets/attachments/3275.pdf.

[74] No. 6:07-cv-1740-Orl-22KRS, 2008 WL 958136 (M.D. Fla. 2008).

law of the jurisdiction where the server is located.[75] The theory behind this thinking was that, like a library in the same location, an Internet service is a passive instrument which must be intentionally accessed by the user. Such a user may therefore violate the law of his country by visiting the library and returning with information that is unobjectionable in the library's jurisdiction but illegal in his home land, but the library should not be subject to penalty.

Equally, the user in Iran who downloads photographs of Miss March from the Playboy Internet site may be subject to harsh penalties by the conservative judiciary in Tehran, but Playboy should not be. It is the user in Iran, goes the argument, not Playboy, which never entered or acted in Iran, who has violated Islamic law. The only difference is that the library visit is physical and the web access electronic. Indeed, in the United Kingdom, a court found that the location of a server determined the appropriate jurisdiction to regulate internet content.[76] Of course, given the ease of locating a server in almost any chosen location, such a rule would lead to servers being located in favorable jurisdictions in a form of forum shopping by server location.

Unfortunately, this approach, while perhaps logical, depends for implementation on nations willingly forgoing jurisdiction over conduct that reaches their citizens at home and at a minimum, facilitates the violation of their laws and, often, their core religious or moral standards. However, in a hopeful harbinger of legislation to come, the UK passed a law in February 2003 making on-line tobacco advertisements illegal, but expressly provided that entities that do not carry on business in the UK will not be in violation of this law as a result of their websites with tobacco ads being accessed in the UK.[77]

While the law, both internationally and domestically, continues to develop on jurisdiction over websites, such a voluntary limitation of jurisdiction on a widespread basis is unlikely for now, as evidenced by the *Maritz* decision and the *Thomas* conviction, where even the United States judicial system found jurisdiction to hold liable, or even convict, foreign service operators who simply made offending materials available via Internet or telephone access. The German Compuserve indictment is in the same sense.[78]

In a case presenting the other side of this coin, a federal court in New Jersey recently rejected the notion that the server's location should be determinative, holding that the mere

---

[75] A. Bertrand, *Collective Administration of Copyrights, Artists Rights and the Law of Publicity on the Internet: Current Issues and Future Perspectives*, 3 New York State Bar Association International Law and Practice Section Fall Meeting 1227 (1996); A. Gigante, *Ice Patch on the Information Superhighway: Foreign Liability for Domestically Created Content*, 14 CARDOZO ARTS & ENT. L.J. 523 (1996). A proposed Convention on Transfrontier Computer-Network Communications contained in the Gigante article is available at http://dvorak.org/gigante/. The treaty would prohibit signatories from regulating or restricting communications and e-mail originating outside their territory and passing or routed through any part of a computer network located on their territory, and would apply the civil law of the originating party to determine private rights and obligations with respect to a communication.

[76] *Football Dataco Ltd et al. v. Sportradar GmbH, reported in* Strikeman Elliott LLP, "UK Ruling – Internet Jurisdiction Based on Server Location?" (Lexology, November 30, 2010), *available at* *http://www.lexology.com/library/detail.aspx?g=7e73e360-e0f8-459c-9632-baa25fa9b182* (subscription required).

[77] B. Thompson, *Cigarette ads thrive online*, BBC News March 11, 2003, *located at* http://news.bbc.co.uk/1/hi/technology/2763643.stm.

[78] *See also U.S. v. Mohrbacher*, 182 F.3d 1041 (9th Cir. 1999) (person who downloads contraband from computer bulletin board is guilty of receiving contraband, but not of shipping or transporting it; provider of bulletin board would be guilty of the latter).

physical presence of a web server in a particular state does not in itself provide sufficient contacts to create jurisdiction of that state over the website.[79]

The European Union has been active in attempting to resolve cross-border electronic commerce issues. In 2003, the E.U. Commission issued a draft regulation to govern jurisdictional issues surrounding cross-border consumer e-transactions under the EU Community Regulation on the Law Applicable to Non-Contractual Obligations, otherwise known as Rome II. While Rome II was substantially implemented, this particular regulation is still in the process of negotiation. As originally drafted, the regulation would create jurisdiction over on-line sellers in the home state of the purchaser, a concept which is at odds with the principles of the E-Commerce Directive. The International Chamber of Commerce, among others, has called on the European Union to reconsider this approach in favor of a regulation that would make the laws of the country of origin of goods or services the basis for settling disputes arising out of e-business transactions. The ultimate resolution remains to be seen. However, the Court of Justice of the European Union has recently found, by way of its interpretation of Article 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000, that with regard to litigating disputes involving online content, the courts of the infringing party's state and the claimant's state both have jurisdiction to hear the case.[80] This would hold true for trademark infringement.[81] However, in the area of copyright infringement, the European Court of Justice recently found that jurisdiction over copyright protection exists in the courts of any Member State where the relevant website is accessible.[82]

Regulation of Gambling

A 1996 article in the New York Times noted that "[t]here are few patches of legal turf the states guard more fiercely than gambling."[83] The article noted the problem of regulating websites that offer wagering over the Internet without regard to the location of the gambler. The State of Minnesota sued a Las Vegas-based company that offered sports betting on-line, contending that the company committed consumer fraud in asserting that its service was legal, as it may have been in Nevada. The issue, once more, was whose law governs a website in one jurisdiction that may be accessed from every other jurisdiction in the world. A Minnesota court resolved the jurisdictional issue in the State's favor, holding that advertising on a website available in Minnesota was sufficient to confer jurisdiction over the defendants, particularly in light of the

---

[79] *Amberson Holdings LLC v. Westside Story Newspaper* (D. N.J. 2000) *reported in* 60 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 686 (10/27/00).

[80] Case C−523/10, *Wintersteiger AG v. Products 4U* , *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=121744&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3097597 (Apr. 19, 2012).

[81] http://www.whitecase.com/articles/032014/intellectual-property-infringement-on-the-internet-what-court-to-call/#.U3F_j1dLp8F

[82] *Id. citing* ECJ judgment of 3 October 2013 – Case C-170/12 – *Pinckney. available at* http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5129d6e3786ee4b5db16f84c3f7056dbf.e34KaxiLc3eQc40LaxqMbN4OaNmNe0?text=&docid=142613&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=211061.

[83] J. Sterngold, *A One-Armed Bandit Makes a House Call*, N.Y. TIMES, Oct. 28, 1996, at D1, col. 2.

maintenance of a toll-free telephone number and a mailing list that included Minnesota residents.[84]

A similar case was brought by federal prosecutors in New York against the owners and managers of six offshore Internet gambling sites. The sites were licensed by the governors of the Caribbean and Central American countries where they were based, raising similar issues of jurisdiction and choice of law.[85] In 1999, a New York court granted injunctive relief against one such operator, finding a violation of law despite the fact that a user of the gambling site who gave a New York address was not permitted to gamble.[86] The court granted relief, reasoning that the restriction could easily be circumvented by a New Yorker who provided an address in Nevada or other state where gambling was legal.[87]

Likewise an appellate court in the Netherlands ordered a UK originating sports betting website to restrict access by Dutch residents for various reasons under Dutch law.[88] The decisive elements of the case for the court were the ability of individuals to participate from computers located in the Netherlands and to have proceeds deposited in Dutch bank accounts. Such cases engender uncertainty by suggesting that websites can be subject to the laws of any and all countries from which they may be accessed.

Other nations take different views. In the United Kingdom, courts look to the location of the last act of the offense. In the gambling context, this is deemed to be the receipt of the player's instructions, or the random operation determining the result. As these generally occur offshore, there is no criminal offense in the U.K. On the other hand, advertising the opportunity to gamble may also be unlawful, and the viewing of such an advertisement − even online − will be a "last act" within the jurisdiction.[89]

In Germany, however, the availability of a German language version of the www.goldenjackpot.com website was deemed sufficient to establish "that the Internet casino in issue has directly targeted the German market."[90]

International law raises additional considerations in this area. In November 2004, a World Trade Organization panel ruled that U.S. prohibitions on online gambling constituted an unfair trade barrier, upholding a complaint by Antigua and Barbuda, home to dozens of online casinos.[91] An appeals panel largely reversed, applying an exception where nations show that

---

84 *Minnesota v. Granite Gate Resorts, Inc.*, No. C6-95-7227, 1996 WL 767431 (Minn. Dist. Ct., County of Ramsey 2d Jud. Dist., Dec. 10, 1996).

85 *14 Charged by U.S. In First Such Case On Internet Betting*, N.Y. TIMES, Mar. 5, 1998, at A1, col. 8.

86 *See United States v. Cohen*, 260 F.3d 68 (2d Cir. 2001) (court upheld conviction of founder of World Sports Exchange under the Wire Wager Act, 18 USC § 1084).

87 *New York v. World Interactive Gaming Corp.*, 714 N.Y.S.2d 844, 1999 N.Y. Misc. LEXIS 425 (1999). Jurisdiction was clear in *World Interactive Gaming*, as the defendants had many other jurisdictional contacts in New York. The decision in *World Interactive Gaming*, along with *Twentieth Century Fox Film Corp. v. iCraveTV* (Civil Action No. 00-121 (W.D. Pa. Jan. 28, 2000)), was a copyright infringement suit where jurisdiction was asserted over a Canadian defendant which had tried to limit its targeting to Canadian residents, have been contrasted with Judge Fogel's decision in *Yahoo! Inc. v. La Ligue Contre Le Racisme Et l'Antisemitisme*, 169 F.Supp.2d 1181 (N.D. Cal. 2001)).

88 *Ladbrokes v. De Lotto*, WORLD INTERNET L. Rep. (BNA) Oct. 2003, at 21.

89 C. Rohsler, *Internet Gambling – Worldwide Themes and Dissonances*, WORLD INTERNET L. REP. (BNA) at 6 (Aug. 2003).

90 *Id*. (reporting Ct. App. Hamburg, Judgment of Nov. 4, 1999).

91 Associated Press, "WTO says United States Should Drop Ban on Offshore Internet Gambling," Mercury News.com (Nov. 10, 2004), http://www.siliconvalley.com/mld/siliconvalley/news/editorial/10146233.html.

special laws are needed to protect "public morals." The appeals panel did, however find that a U.S. law that allowed online betting on horse races, but only with U.S.-based offtrack companies, discriminated against foreign operations in violation of international law.[92] A WTO Compliance panel ruled in February 2007 that the U.S. had failed to comply with the prior ruling, opening the door to trade sanctions,[93] and in December Antigua was permitted to violate copyrights on U.S. content up to a value of $21 million.[94] Similarly, the European Commission has recently begun investigating the impact of U.S. gambling law on European internet gambling providers.[95] The EC's investigation was initiated by the Remote Gambling Association, which alleged that U.S. law, and its enforcement by the U.S. Department of Justice, discriminates against European internet gambling providers in violation of the General Agreement on Trade in Services ("GATS"). The investigation may lead to the filing of a complaint at the WTO. The United States has announced, however, its intention to withdraw from certain commitments under GATS by "clarifying" that the agreement does not extend to internet gambling.[96]

Within the EU, in September 2009 the European Court of Justice delivered a far-reaching opinion, which upheld Portuguese legislation prohibiting foreign online gaming companies from offering gambling services in Portugal.[97] In rejecting the gaming companies' arguments that the Portuguese legislation was incompatible the EU's "freedom to provide services," the European Court held that Portugal's law was justified by the objective of combating fraud and crime. Thus, subject to satisfying certain conditions (*e.g.*, avoiding overreaching and discrimination), European Member States are generally now free to "define in detail the level of protection sought" from foreign gambling sites. The ruling is a clear victory for EU Member States and further undermines the remote gambling industry.

C. *Determining Applicable Law*

The Electronic Commerce Directive, a regulatory framework for e-commerce, was put forth by the European Union in 2000.[98] The E-Commerce Directive employs a "country of

---

92 F.Butterfield, "U.S. Limits on Internet Gambling Are Backed," N.Y. TIMES (April 8, 2005), p. C14 col.1.

93 "WTO Panel Upholds Ruling on U.S. Internet Gambling Laws," WORLD COMMUNICATIONS REG. REP. (BNA) at 15 (April 2007).

94 "In Trade Ruling, Antigua Wins a Right to Piracy," N.Y TIMES (Dec. 22, 2007), *available at* http://www.nytimes.com/2007/12/22/business/worldbusiness/22gambling.html.

95 *Reported in* Steptoe & Johnson, E-Commerce Law Week (March 15, 2008).

96 *Reported in* Steptope & Johnson, E-Commerce Law Week (Dec. 29, 2007) (The U.S. has agreed to compensate the EU, Canada and Japan for this "clarification" because "under the terms of the GATS, the United States must compensate any WTO member that demonstrates that it would be harmed by a change in U.S. GATS commitments." *Id*.).

97 *Liga Prtuguesa de Futbol Profissional (CA/LPFP) and Bwin Int'l Limited v. Departmento de Jogos da Santa Casa da Misericórdia de Lisboa*, European Court of Justice (Case No. C-42/07) (Sept. 8, 2009).

98 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), 2000 Official Journal L178, 17/07/2000, *available at* http://www.tourismlaw.eu/documents/tourism_legislation/EU_8june2000_uk.pdf. The E-Commerce Directive was scheduled to be implemented by the legislatures of all E.U. Member States by January 17, 2002. However, all but three E.U. Member States missed the deadline and while as of November 21, 2003, twelve E.U. Member States and three European Economic Area countries (Iceland, Liechtenstein and Norway) have enacted implementing legislation, three (France, Netherlands and Portugal) have yet to do so. *Report From the Commission to the European Parliament, the Council and the European Economic and Social Committee: First Report on the Application of Directive 2000/31/EC*, Nov. 21, 2003, at 6, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0702:EN:NOT.

origin" approach when determining which country has jurisdiction over ISPs, thereby making the country in which an "information society service provider" maintains a fixed establishment, regardless of where the website or server is located, responsible for exercising control over the service provider and the country whose law will govern in the absence of agreement to the contrary.[99]

The country of origin principle, however, does not apply to consumer transaction contracts.[100] Consumers remain protected by the laws of their own nation,[101] such as Germany's requirement that consumers be notified of their right to revoke online transactions.[102] The Brussels I Regulation, which went into effect on March 1, 2002 and is binding in Member States without the need of implementing legislation, provides jurisdiction in a consumer's home country over a foreign defendant that "pursues commercial or professional activities in the . . . the consumer's domicile or, by any means, directs such activities to that Member State . . . and the contract falls within the scope of such activities."[103] The question of whether a website available in a Member State is an activity "directed" at that Member State is similar to the question of "targeting" in the U.S. jurisprudence. Factors may include languages used on the website, currencies used for showing prices, the use of country flags to select languages and similar indicia showing an intent to deal with a country's residents. Despite the significant protections provided to consumers by the Brussels I Regulation, those consumers will still have to seek enforcement of any judgment they obtain in the Member State of the website operator. Critics claim the Brussels I Regulation will inhibit businesses from offering goods and services over the Internet, while consumer advocates claim that the increased protection of Internet consumers will increase consumer confidence and elevate the levels of consumer spending.[104]

Similarly, a French court found that Google Inc.'s bulk book scanning project is subject to and in violation of French copyright law, which contains no exception for fair use. In *Editions du Seuil v. Google Inc.*, Google argued that the U.S. fair use doctrine applied to its Book Search website because the books were scanned in the United States. The *Tribunal de grande instance de Paris* disagreed, holding that French law applied because the works had French authors and the materials were aimed at French Internet users.[105] The material specifically targeted French users through a French-language website and domain name "books.google.fr." Consequently, the court held that "[t]he result of this combination of factors is that France is the country that maintains the closest links with this lawsuit, which justifies application of French law."[106]

Moreover, a company that sells over the Internet increasingly must also consider various international legislative requirements with regard to how the contract is executed and performed. For instance, the European Union Electronic Commerce Directive requires that any promotional

---

99 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 (the "E-Commerce Directive"), *available at* http://www.tourismlaw.eu/documents/tourism_legislation/EU_8june2000_uk.pdf,Annex.

100 *Id.*, Recitals (29), (53), (55), (56), (65), Art. 1, §3, Annex.

101 *Id*., Recital (55).

102 *See* M.Hilber, "Round-Up of Recent E-Commerce Decisions in Germany," WORLD COMM. REG. REP. (BNA) (Sept. 2006).

103 Council Regulation No. 44/2001 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, art. 15(c).

104 P. Van de Velde and C. Heeren, *Jurisdiction Over Consumer Contracts: the Impact of the "Brussels I" Regulation on B2C E-Commerce*, WORLD INTERNET L. REP. (BNA) (October 2003).

105 *Reported in* 79 PATENT, TRADEMARK & COPYRIGHT J. 1947 (BNA) (Jan. 1, 2010) at 226.

106 *Id*.

offers or commercial communications be "clearly identified as such", that the identity of the sender is clearly identifiable, and that the offers or communications clearly and unambiguously disclose any conditions of participation.[107]

This Directive also grants the same legal validity to documents electronically signed as for their handwritten signed counterparts, provided that the electronic signature employs a reliable process of identification, guaranteeing a link between a document and the signature attached to it.[108]

The United States has similar legislation embodied in the E-SIGN Act, which gives equal force to e-signatures and signed papers, but requires that any electronic sale inform consumers of their right (a) to receive the information in paper form; (b) to withdraw their consent to the transaction and any conditions, consequences, and fees of such withdrawal; and (c) a description of the hardware and software required to access the electronic records.[109] In addition, 47 states and the District of Columbia have adopted the Uniform Electronic Transactions Act ("UETA")[110], whose main purpose is to establish the legal equivalence of electronic records and signatures with paper writings and manually-signed signatures, removing barriers to electronic commerce.[111] UETA has been so widely accepted among the states in part because the E-SIGN Act pre-empts state laws affecting electronic signatures, making an exception only when a state has adopted UETA in the form it was proposed.[112]

The United Nations Commission on International Trade Law has developed a Model Law on Electronic Signatures. If adopted, the Model Law is not expected to have a significant impact on most developed countries, including Japan, the United States and the European Union's Member States, which have largely enacted electronic signature legislation. However, some commentators have pointed out that the U.N.'s Model Law is nothing like the electronic signature laws passed in either Europe or the United States and the effects, if adopted, will be unpredictable and sweeping.[113] In addition, the UN General Assembly adopted a new convention on using electronic communications in international contracting, which builds on the Model Law. The convention will be open for signature by nations from January 2006 to January 2008.[114]

Thus, for now, the applicable maxim is plainly *communicator emptor*. At a minimum, companies establishing websites need to consider the legal implications of their site, if not in every state and country in the world, at least in those in which it conducts significant business. In order to protect themselves fully, companies which are not in fact engaged in national or global business should consider placing on their site a disclaimer of any intent to solicit business, or even site visitors, from outside specified jurisdictions. This is particularly important in light of

---

[107] D. Marino and D. Fontana, *The EU Draft Directive on Electronic Commerce*, WORLD INTERNET L. REP. (BNA) (3/00), at 26.

[108] Laurent Szuskin and Myria Saarinen, *Enactment of the Decree Relating to E-Signatures*, WORLD INTERNET L. REP. (BNA) (June 2001), at 7.

[109] Stephanie Tsacoumis and Victoria P. Rostow, *E-SIGN Your Life Away: Digital Signatures in the New Economy*, 4 WALLSTREETLAWYER.COM, at 20.

[110] UETA was approved by the National Conference of Commissioners on Uniform State Laws at its annual meeting in July 1999.

[111] Illinois, New York and Washington, as well as Puerto Rico, have not yet enacted UETA. For current statistics on the adoption of the UETA, *see* http://www.nccusl.org/Act.aspx?title=ElectronicTransactionsAct.

[112] *Most UETA Bills Introduced in 2001 Pass*, WORLD INTERNET L. REP. (BNA) (Sept. 2001), at 17.

[113] Stewart Baker, quoted in *U.N. Commission to Consider Draft Model Law on E-Signatures at June Meeting*, WORLD INTERNET L. REP. (BNA) (May 2001), at 31.

[114] http://www.un.org./apps/news/story.asp?NewsID=16685&Cr=general&Cr1=assembly.

the developing trend in the United States that a state's jurisdiction over a particular website is conferred through actual transactions in the state.[115]

State securities regulators have endorsed this approach from the securities law standpoint, exempting offerings that disclaim offering to residents of specific states, provided the offering is not directed at state residents by other means and sales are not made in the state.[116] Similar issues arise as the SEC considers how to regulate offerings of securities by foreign websites.[117] Currently, the SEC will not consider an offshore (non-U.S.) Internet offer as targeted at the U.S. and will not treat it as occurring in the U.S. for registration purposes if the offerors take adequate measures to prevent U.S. persons from participating.[118] Australia and Japan have similar rules and have published guidelines offerors can follow, including a jurisdictional disclaimer, to avoid violating their securities laws.[119]

Similarly, in a series of three no-action letters, the SEC permitted websites to screen investors by way of an accreditation questionnaire and issuing passwords to those found to be qualified. Only after reviewing the password would the investor actually access the website and view corporate offerings. This process was found not be a "general solicitation" in violation of Rule 507.[120]

---

[115] *See, e.g.*, *Ford Motor Co. v. Texas Dep't of Transp.*, No. 00-50750 (5th Cir. 2001) (Internet sale by Ford of used motor vehicles violated state statute prohibiting automobile manufacturers from retailing motor vehicles to consumers); *National Football League v. Miller*, No. 99 Civ. 11846(JSM), 2000 WL 335566 (S.D.N.Y. 2000) (income derived by defendant from New Yorkers placing bets through advertisers on defendant's website created jurisdiction in New York); *Euromarket Designs Inc. v. Crate & Barrel Ltd.*, 96 F.Supp.2d 824 (N.D. Ill. 2000) (completed Internet transaction between Irish vendor and Illinois resident constituted sufficient contacts for jurisdiction); *American Eyewear Inc. v. Peeper's Sunglasses and Accessories Inc*., 106 F.Supp.2d 895 (N.D. Tex. 2000) (personal jurisdiction created in Texas by regular Internet transactions of Minnesota corporation with Texas residents); *People Solutions, Inc. v. People Solutions, Inc*, No. 3:99-CV-2339-L, 2000 U.S. Dist. LEXIS 10444 (N.D. Tex. 2000) (website allowing Texas residents to order goods online insufficient to establish personal jurisdiction because no goods actually sold to Texas residents), *but cf. America Online Inc. v. Huang*, 1060 F.Supp.2d 848 (E.D. Va. 2000) (registration of Internet domain name with Virginia–based company was insufficient contact to create jurisdiction); c*ontra, Bancroft & Masters Inc. v. Augusta Nat'l Inc*., 223 F.3d 1082 (9th Cir. 2000), *reported in* 60 PAT. TRADEMARK & COPYRIGHT J. (BNA) 366 (Aug. 25, 2000) (protest letter sent to domain name registrar in state sufficient to provide jurisdiction).

[116] Alaska Administrator of Securities, In Re: Offers Effected Through Internet That Do Not Result in Sales of Securities in Alaska, Admin. Order 96-065 (Dec. 20, 1995); Indiana Sec. Div., In the Matter of: Securities Offered on the Internet but Not Sold in Indiana, Order No. 95-0115 AO (Nov. 15, 1995); Texas Sec. Bd., § 139.17, Offer Disseminated Through the Internet; all *cited in* E. Schneiderman & R. Kornreich, *Personal Jurisdiction and Internet Commerce*, N.Y.L.J. June 4, 1997, at 1.

[117] *See* discussion in J. Coffee, *Brave New World?: The Impact(s) of the Internet on Modern Securities Regulation*, 52 Bus. Law, 1195, 1227-32, suggesting international treaties as a potential approach. In November 2001, the SEC sponsored a Major Issues Conference on Securities Regulation in the Global Internet Economy, which was the first SEC-supported conference since 1984 that is devoted to examining broad policy issues in securities regulation. *See* http://www.sec.gov/news/headlines/majorissues.htm.

[118] Stéphan Le Goueff, *Offering Financial Services on the Web: Experiencing the World Wide (Legal) Web*, WORLD INTERNET L. REP. (BNA) (Feb. 2001), at 26. The SEC has issued guidance rules for the offer of securities on the Internet in the U.S. which are contained in the SEC International Series Release No. 1125, effective as of March 23, 1998.

[119] Id. *See also, FSA Introduces Guidelines on Foreign Firms' Internet Ads*, WORLD INTERNET L. REP. (BNA) (Feb. 2001), at 6.

[120] *See* J. Coffee, "Brave New World?: The Impact(s) of the Internet on Modern Securities Regulation," 52 Bus. Law. 1195, 1219-21 (1997), *citing* IPOnet, SEC No-Action Letter, 1997 SEC No. Act. LEXIS 642 (July 26, 1996);

Franchise regulators have taken a similar approach. The North American Securities Administrators Association ("NASAA") has adopted a "Statement of Policy Regarding Offers of Franchises on the Internet," which deems franchise and advertising offers on the Internet as exempt from franchise registration and disclosure statutes in states where the offer indicates that it is not being made to residents of the state, it is not otherwise directed at residents of the state, and no franchise sales are made in the state before compliance with the state's franchise registration and disclosure law.[121] This approach has since been adopted in seven states, including Indiana,[122] Maryland[123] and New York.[124] Such a disclaimer approach is doubtless anathema to website designers and marketing staff, but (if the disclaimer is not contradicted by the facts) at least provides an argument that the company is not "purposely availing itself" of the privilege of conducting activities in unexpected places and so should not be held subject to jurisdiction there.

The NASAA has also issued a "Statement of Policy Regarding Franchise Advertising on the Internet," which provides that any communication about a franchise offering made through the Internet should be exempted from franchise filing requirements[125] if the franchisor provides the URL of the advertising to the state franchise administrator and the Internet advertising is not directed to any person in the jurisdiction.[126] New York has implemented the NASAA policy statement.[127]

The United Kingdom has enacted the Consumer Protection (Distance Selling) Regulations 2000, which offers similar protection. Specifically, prospective purchasers must be provided with the name and address of the supplier; a description of the goods and services; the price for the goods, including tax; arrangements for payment, delivery and performance; and the ability of the purchaser to cancel the contract.[128]

International policy makers from fifty-two member nations have been trying to set common rules governing online trade and commerce for ten years through the Hague Convention on Jurisdiction and Foreign Judgments. As it is currently drafted, the Hague treaty would require

---

Angel Capital Electronic Network, SEC No-Action Letter, 1997 SEC No. Act. LEXIS 812 (Oct. 25, 1996); Lamp Technologies, Inc. SEC No-Action Letter, 1997 SEC No-Act. LEXIS 638 (May 29, 1997).

[121] NASAA Statement of Policy Regarding Offers of Franchises on the Internet, *available at* http://www.nasaa.org/content/Files/Internet_Offers_Franchises.pdf.

[122] Order No. 97-0378AO, BUS. FRANCHISE GUIDE (CCH) ¶ 5140.011 (Dec. 24, 1997).

[123] Code of Md. Regs., Div. of Securities § 02.02.08.18.

[124] Dep't of Law, Bureau of Investor Protection and Securities – Codes, Rules and Regulations of the State of N.Y., Tit. 13, Ch. VII § 200.13 (1999), BUS. FRANCHISE GUIDE (CCH) ¶ 5320.13.

[125] Nine of the franchise registration states require franchisors that offer franchises in those states to file copies of their franchise sales advertisements prior to publication. Steven Goldman & Mark P. Forseth, *Internet Franchise Advertising: Will Franchise Regulation Join the Information Age?*, 7 LJN'S FRANCHISING BUS. NEWS & L. ALERT 11 (Aug. 2001), at 6.

[126] See NASAA Statement of Policy Regarding Franchise Advertising on the Internet, *available at* http://www.nasaa.org/content/Files/Franchise_Advertising_Internet.pdf. Likewise, the Federal Trade Commission has issued a notice of proposed rulemaking with respect to the dissemination of financial performance representations outside of the offering circular, including Internet advertising. Goldman & Forseth, *supra* at 5.

[127] Dep't of Law, Bureau of Investor Protection and Securities – Codes, Rules and Regulations of the State of N.Y., Tit. 13, Ch. VII § 200.13 (1999), BUS. FRANCHISE GUIDE (CCH) ¶ 5320.13.

[128] Statutory Instrument 2000 No. 2334, *available at* www.legislation.hmso.gov.uk/si/si2000/20002334.htm.

participants to enforce each others' commercial laws even if such laws prohibit actions that are legal under local laws.[129]

There are many critics in the United States who fear that U.S. citizens will lose many of their rights under such a lowest common denominator approach where all websites are required to comply with the laws of every member nation. On the other hand, the software, movie and recording industries, along with other copyright holders, view the treaty as an effective means of enforcing copyright violations abroad.[130] Although the U.S. has been involved in the Hague Treaty drafting process, it remains to be seen whether it will sign onto the finished product.

D. *Copyright Infringement*

Another problem with subjecting those making information available on the Internet only to the law of the jurisdiction where the server is located is the fact that those wishing to infringe intellectual property will then establish their servers in countries with weak or nonexistent copyright law and so insulate themselves from liability. This concern might also be addressed by treaty, with the willingness of signatory nations to limit jurisdiction over servers in other countries being conditioned on such other countries' enforcement of laws protecting intellectual property as well as their adherence to the treaty.

Regardless of how this is addressed, the issue of potential copyright infringement must be considered by website operators as well. Obviously, appropriate licenses are essential for all text, sounds and images placed on the site, and a work for hire agreement should be in place with all outside website designers and developers. But might the risk of infringement liability go farther?

Consider *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,[131] in which the Church of Scientology sued for copyright infringement of its religious texts by a former minister turned critic who posted portions of the texts on an Internet Usenet newsgroup. The suit also named the operator of a computer bulletin board on which the former minister directly posted the works and which transmitted them to Netcom, an Internet service provider, which then transmitted the postings to Usenet servers throughout the Internet. The Church of Scientology had notified both these parties that the former minister's postings infringed and demanded that they act to prevent him from accessing the Usenet through their systems. Netcom exercised no editorial control, but simply received and transmitted all such Usenet postings, as is essential for the Usenet forum to work.

The district court, on a motion for summary judgment, found no direct infringement by Netcom, either for copying or distribution, analogizing it to the owner of a copying machine who allows the public to make copies on it. Users of the machine may directly infringe, but the owner's liability is analyzed under the principles of contributory infringement.[132] Otherwise, every Usenet server in the world transmitting the infringing postings would be liable for infringement, regardless of knowledge of the content of the postings. The court also rejected a theory of vicarious liability of Netcom as well, finding that while Netcom might have had the

---

[129] Lisa M. Bowman, *Global treaty could transform Web*, CNET NEWS.COM (June 22, 2001) located at http://news.cnet.com/Global-treaty-could-transform-Web/2100-1023_3-268850.html?tag=mncol;1n.

[130] Jeffrey Benner, *New World Order, Copyright Style*, WIRED NEWS (Sept. 11, 2001) located at http://www.wired.com/news/politics/0,1283,46676,00.html.

[131] 907 F. Supp. 1361 (N.D. Cal. 1995).

[132] *Id.* at 1369-72.

right and ability to control the activities of its subscribers, there was no evidence that it had any direct financial benefit from the infringement.

Netcom was not home free, however. In considering whether it might be liable as a contributory infringer, the court found that, as an access provider, Netcom stored and transmitted the infringing messages, thus participating in the infringement to a greater extent than, for example, the lessor of premises that are later used for infringement. It also found that the plaintiff's notice to Netcom of the infringement raised a question of fact as to Netcom's knowledge of the infringement.[133] If Netcom was established to have such knowledge, taking into consideration the perhaps colorable claim of fair use in this case, it would be liable as a contributory infringer, particularly in light of its admission that it did not even look at the postings in question after receiving notice.[134] (As described below, a similar "contributory infringer" theory may also apply to trademark claims.)

A German court reached just this conclusion, finding an online news site to have violated German copyright law for linking to a software vendor's site whose products the news site knew could be used to circumvent copyright protection mechanisms on DVDs.[135] In 2012, a Dutch court found that hyperlinks on a website may, under some circumstances, qualify as infringement and that such infringement may attach to an individual or organization that links to infringing content.[136] The court declared that linking (as was found in this case) would qualify as infringement if the following three factors were found: (1) intervention; (2) a new audience; and (3) profit.[137]

Under this approach, might not the operator of a web page also be found to be a contributory infringer if it supplies links to other websites or servers containing infringing materials, at least after a demand by the copyright holder to remove the links?[138] Admittedly, the provision of a link is less active than the storage and transmission of infringing material and somewhat closer to the situation of the landlord who provides premises later used for infringement, and that argument might indeed carry the day.

One court has so held, dismissing a claim of infringement based on links from the defendants' website to another site containing infringing copies of the plaintiff's photographs, at

---

[133] Perhaps as an effect of the Scientology/Netcom case, Slashdot.org, an open-source software developers' website, censored its own website by removing a user's posting containing quotes from a Church of Scientology copyrighted church tract in the face of legal threats from the Church of Scientology and advice from their counsel that such posting violated the Digital Millennium Copyright Act. Roger Parloff, *Threat of Scientologists' Legal Wrath Prompts Slashdot to Censor a Posting*, THE STANDARD (Mar. 16, 2001), located at www.thestandard.com/article/display/0,1151,22941,00.html.

[134] *Id.* at 1373-75. *See also Marobie-FL Inc. v. National Ass'n of Fire Equipment Distributors*, 983 F. Supp. 1167 (N.D. Ill. 1997) (website operator directly liable for infringing use of clip art; Internet service provider not directly liable, but might be contributorily liable depending on knowledge of material's copyright and extent of monitoring or control of website); *Sega Enterps., Ltd. v. Maphia*, 948 F. Supp. 923 (N.D. Cal. 1996) (operator of bulletin board with knowledge of uploading and downloading of unauthorized copies of software was contributory infringer).

[135] *BMG Records GmbH v. Heise Zeitschriften Verlag* (Intermediate Court of Appeals of Munich, July 28, 2005), *reported in* E-COMMERCE LAW WEEK (August 20, 2005), http://www.steptoe.com/publications-1671.html.

[136] *Sanoma Media Netherlands,v. GeenStijl.nl*, *available* at http://www.scribd.com/doc/105702632/Sanoma-Playboy-en-Britt-Dekker-tegen-GeenStijl.

[137] *Id.*

[138] The Austrian Supreme court ruled on December 19, 2000, that in creating a hyperlink to another website, an operator of a website thereby incorporates the linked website into its own and is fully responsible and liable for the content of the linked site. *Liability for Links: OGH 19.12.2000, 4 Ob 274/00y*, *reported in* WORLD INTERNET L. REP. (BNA) (May 2001), at 13.

least in the absence of knowledge by the defendant of the infringing photographs.[139] Prudence, however, dictates that upon receipt of any notice of infringement with respect to material accessible through a company's website, counsel should at least investigate the claim, and remove the link to the allegedly infringing material if the claim appears to have merit. The infringement concern is heightened if a website provides for visitors to upload comments or files to discussion areas or other areas in which they may be viewed by others.

When Google received such a notice under the Digital Millennium Copyright Act, discussed below, from the Church of Scientology, asserting that Google search results for "Scientology" provided links to copyrighted material, it removed the links to avoid infringement litigation. It also, however provided a copy of the Scientology notice to the Chilling Effects Clearinghouse, at chillingeffects.org, and informs users when a search would yield a removed link, pointing them instead to chillingeffects.org. Ironically, the posted notice from the Church of Scientology, to which Google linked, contained the URLs for the very sites to which the notice objects.[140]

Questions of liability for internet service providers also arise where their customers engage in infringement or other unlawful conduct. An Australian court held that an internet service provider was not liable for its customers' copyright violations where the customers engaged in unauthorized downloading of film and television programs. In *Roadshow Films v. iiNet Limited*[141], plaintiffs from the film industry argued that the ISP had violated Australia's Copyright Act of 1968, which provides that a person is liable for infringement if the person "sanctions, approves or countenances" the infringement. In rejecting the plaintiffs' arguments, the Federal Court of Australia held that an ISP does not sanction, approve or countenance the unlawful acts of its customers by merely providing internet access to such customers, notwithstanding the fact that the ISP had knowledge that such infringement was occurring and did not take any steps to prevent it.

By contrast, the French Cour de Cassation held that an ISP may be liable for its customers' copyright infringement where the ISP displays paid advertising on infringing websites of such customers. In *Tiscali Media v. Dargaud et al.*,[142] the defendant ISP argued that it was immune from copyright infringement liability under the EU E-Commerce Directive,[143] which provides that "hosting services providers" are generally not liable for stored content unless they have actual knowledge of the infringement. Here, however, the court held that the ISP functioned not merely as a service provider, but also as a co-publisher by encouraging users to create personal webpages and by generating additional revenue from soliciting third-parties to place advertisements on the infringing webpages.[144]

Despite the fact that a web hosting company did not have actual notice that its customer's website offered counterfeited products for sale, a 2011 South Carolina decision held the hosting company liable for contributory infringement where the customer's website clearly advertised the sale of copied golf clubs.[145] Similarly, the U.S. Court of Appeals for the Ninth Circuit upheld a

---

139 *Bernstein v. JC Penney Inc.*, 50 U.S.P.Q.2d (BNA) 1063 (C.D. Cal. 1998).

140 *See* D. Gallagher, "New Economy," N.Y. TIMES, Apr. 22, 2002.

141 (No. 3) [2010] Federal Court of Australia 24.

142 Cour de Cassation (1st section, civil), 14 January 2010, *Telecom Italia (formerly Tiscali Media) v the companies Dargaud Lombard and Lucky Comics*.

143 2000/31/EC.

144 *See French Cour de Cassation threatens Web 2.0*, Eversheds (Mar. 12, 2010).

145 *Roger Cleveland Golf Co. Inc. v. Prince*, No.: 2:09-2119MBS (Mar. 14, 2011) reported in Polley, MISC. IT

jury's determination that a web hosting company was contributorily liable for allowing its customers to build websites that infringed Louis Vuitton trademarks and copyrights.[146] The Court of Appeals approved a $10.8 million award, noting that the defendants had direct control over the "switch" that kept the websites online and available and that the defendants had received at least 18 Notices of Infringement from Louis Vuitton – it was immaterial whether the defendants *intended* to cause infringement where the defendants had actual or constructive knowledge that the users of their services were engaged in infringing activities.[147] These decisions illustrate that creative plaintiffs are increasingly looking to the ISPs and web hosting companies of infringing users for liability and action to deter infringement.[148]

The issue of internet service providers' obligations to combat intellectual property piracy has been addressed by the European Court of Justice, which ruled in November 2011 that internet service providers cannot be required by a Belgian court to install filtering systems to prevent the illegal downloading of files.[149] The ECJ noted that the EU electronic commerce legislation approved in 2004 makes it clear that national authorities could not adopt measures to force ISPs to carry out general monitoring of the information transmitted on a network.[150] This leaves France's "three strikes law" (also known as the Hadopi law), which allowed for internet service to be cut off to anyone caught illegally downloading three times, on questionable footing.[151]

Framing, Deep Linking, and Thumbnails

Similarly, the practice of linking to third party sites while maintaining a "frame" of one's own poses copyright concerns. Such framing of another's copyrighted site might constitute an infringing derivative work subjecting the "framer" to liability.[152]

Thus, in one case, an image search engine, ditto.com, was held by the Ninth Circuit to have made fair use of photographs it indexed and displayed as small thumbnail images, but might have infringed when it framed full-size images within its own web page context, where a direct link to the copyright owner's site might have been permissible.[153] More recently, the Central District of California held that Google did not infringe an adult subscriber-based website's copyright when it provided frames and in-line links to full-size images on the adult website, Perfect 10, because it held that it was the website that actually "served" the images that was displaying them to users, so that the images were displayed by the adult website rather than by

---

RELATED LEGAL NEWS (distributed by e-mail on Mar. 26, 2011).

[146] *Louis Vuitton Mallettier, S.A. v. Akanoc Solutions Inc. et al.*, 658 F.3d 936 (9th Cir 2011).

[147] *Id.*

[148] *See also*, Hogan Lovells, Irish Court: IP Addresses not personal data (April 23, 2010), *available at* http://www.hldataprotection.com//2010/04/articles/international-compliance-inclu/irish-court-ip-addresses-not-personal-data/ (reporting the settlement of a dispute between several major record labels and Ireland's largest ISP as a result of the ISP's alleged failure to adequately discourage peer-to-peer copyright infringements on its network; terms of the settlement agreement require the ISP to send warning notices to subscribers who are detected to be engaged in unauthorized file sharing and, if ignored, to terminate the subscriber's Internet access).

[149] Kirwin, *EU Court Rules Internet Service Providers Cannot Be Forced to Filter Illegal Downloads* 83 PAT., TRADEMARK & COPYRIGHT J. 2042 (BNA) (Dec. 2, 2011).

[150] *Id.*

[151] *Id.*

[152] *Futuredontics Inc. v. Applied Anagramic Inc.*, 1998 WL132922, 45 U.S.P.Q. 2d 2005 (C.D. Calif. 1998), *aff'd* 152 F.3d 925 (9th Cir. 1998) (unpublished opinion).

[153] *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003), withdrawing prior opinion reported at 280 F. 3d 934 (9th Cir. 2002).

Google.[154] The Ninth Circuit affirmed that portion of the decision, but reversed the District Court finding that the display of thumbnail images by Google likely infringed, because, the Ninth Circuit held, Perfect 10 was unlikely to overcome Google's fair use defense, because of the transformative nature of Google's use.[155]

In 2012, the Seventh Circuit held that myVidster, a website that allowed its users to provide links to infringing copyrighted material, should not be held liable as a contributory infringer. The Court noted that the individuals who originally copied and uploaded the copyrighted material were the infringers, but that myVidster did not encourage that copying.[156]

Over the past several years German Courts had reached conflicting decisions, one holding the display of thumbnails by the Google search engine to be infringing under German law, and another holding it lawful.[157] More recently, the German Federal Supreme Court held that Google's use of thumbnails of copyrighted photographs without the photographer's express consent did not infringe on the photographer's copyrights, reasoning that the photographer gave implied consent by allowing the photos to be placed on the internet, without protections.[158]

Moreover, a recent holding by the Second Circuit should alert U.S. companies to the pitfalls of ignoring foreign copyright law. In *Sarl Louis Feraud International v. Viewfinder, Inc.,*[159] the plaintiff clothing designer brought an action to enforce a judgment issued by the Tribunal de Grande Instance de Paris. The defendant was the operator of a website on which it posted photographs of the plaintiffs' fashion shows. After being served with the plaintiffs' intellectual property infringement action, the defendants failed to respond and the French court issued a default judgment. The plaintiffs then filed in the United States District Court for the Southern District of New York, seeking to enforce the judgment under New York's Uniform Foreign Money Judgment Recognition Act,[160] which provides that foreign judgments that are enforceable in the country where rendered are "deemed conclusive between the parties and

---

154 *Perfect 10 Inc. v. Google Inc.*, 416 F. Supp.2d 828 (C.D. Cal. 2006).

155 *Perfect 10 Inc. v Amazon.com Inc.*, 2007 WL 4225819 (9th Cir. Dec. 3, 2007). The Ninth Circuit remanded for a determination on contributory infringement based on Google's knowledge of infringement by sites to which it linked. In 2012, the Ninth Circuit again refused Perfect 10's request for an injunction to stop Google's use of thumbnail images of Perfect 10's copyrighted nude photos, holding there was no evidence of irreparable harm to Perfect 10 despite Perfect 10's impending bankruptcy. *Perfect 10 v. Google Inc.*, 653 F.3d 976 (9th Cir. 2011) reported in Dutra, *Google Again Escapes Perfect 10 Injunction Request as Ninth Circuit Adopts eBay Ruling*, 82 PAT., TRADEMARK & COPYRIGHT J. 2027 (Aug. 12, 2011).

156 *Flava Works v. Marques Rondale Gunter*, 689 F.3d 754 (7th Cir. 2012).

157 *Compare* Decision of Regional Court of Hamburg, *reported in* WORLD INTERNET L. REP. (July 2004), *with* Decision of District Court of Erfurt (Case No. A2:3 O 1180/05), *reported in* WORLD COMM. REG. REP. (April 2007) at 20. *See also* Decision of Munich Dist. Ct. No Az: 21 O 20028/05 (Jan. 10, 2007), *reported in* WORLD COMM. REG. REP. (BNA) (March 2007) at 17 (framing of copyrighted pictures on website was copyright infringement); Decision of the of Regional Court of Hamburg (Cases No. 308 O 42/06, 308 O 248/07). It is worth noting that in 2010, the German Federal Supreme Court ruled that Google could use and display a thumbnail preview of a picture taken from an artist's website because the artist had not included available code in the website that disallows permission to use it. *See* Weston, "Google Gets Thumbs Up from German Court to Use Small Picture Previews," *reported in* Mondaq (May 19, 2010), *available at http://www.mondaq.in/article.asp?article_id=100686*. Thus, the technological development of such code puts the ability to control the use of thumbnails in the hands of the copyright owner, and the failure to avail oneself of this control may be deemed permission to use.

158 Bhatti, *German Court: Google's Publication of Thumbnail Images Doesn't Infringe Copyright*, 83 PAT., TRADEMARK & COPYRIGHT J. 2038 (Nov. 4, 2011).

159 489 F.3d 474 (2d Cir. 2007).

160 N.Y. C.P.L.R. §§ 5302, 5303.

enforceable by U.S. courts."[161] The district court found that enforcing the French judgment would be repugnant to public policy because it would violate the defendant's First Amendment rights. Reversing the district court's judgment, the Second Circuit noted that under French law, "creations of the seasonal industry of dress and article" are entitled to copyright protection. The court then admonished the defendants for failing to appear before the French court:

> Viewfinder had the opportunity to dispute the factual basis of plaintiffs' claims in the French court, but it chose not to respond to the complaint. As this court has held: "By defaulting [in the foreign adjudication], a defendant ensures that a judgment will be entered against him, and assumes the risk that an irrevocable mistake of law or fact may underlie that judgment."[162]

Thus, the Second Circuit focused solely on whether the French law was repugnant to the public policy of New York. The court noted that a public policy analysis rarely results in a court declining to enforce a judgment unless "it is inherently vicious, wicked or immoral, and shocking to the prevailing moral sense."[163] While recognizing that laws antithetical to the First Amendment will not be enforced, the court held that the district court failed to fully analyze the nature of the French law. The court therefore remanded the matter back to the district court to determine whether French copyright laws provide protections comparable to those under the First Amendment, and whether French law provides something akin to "fair use," which the defendant failed to assert by defaulting. The case demonstrates the importance of foreign intellectual property laws and judgments which parties ignore at their peril.[164]

Pop-up advertisements that appear in a different window over a competitor's website generally have been held noninfringing.[165]

"Deep-linking" to pages on another site (bypassing the other site's home page and advertising), without such frames or confusion of source, has been held to be neither copyright infringement nor unfair competition, although a claim for tortious interference with prospective economic advantage because of lost income from bypassed advertisers was allowed to proceed.[166]

---

[161] 489 F.3d at 477.

[162] *Id.* at 479 (citing *Ackermann v. Levine*, 788 F.2d 830, 842 (2d Cir. 1986).

[163] *Id.* (quoting *Sung Hwan Co. v. Rite Aid Corp.*, 7 N.Y.3d 78, 82 (2006)).

[164] See also, *H & K v. Google*, Paris TGI 10/9/09, *reported in* 79 PAT., TRADEMARK & COPYRIGHT J. 1946 (BNA) (Dec. 18, 2009) at 197 (fair use doctrine unavailable under French law, which controls because the operative facts occurred in France; Google infringed a photographer's copyright by displaying his work as a thumbnail on Google Images and failed to promptly remove the works in response to the photographer's objections).

[165] *U-Haul Int'l v. WhenU.com Inc.*, 279 F.Supp.2d 727 (E.D. Va. Sept. 5, 2003) (Sept. 19, 2003). *See also Wells Fargo & Co. v. WhenU.com*, 293 F.Supp.2d 734 (E.D. Mich. 2003), *reported in* 67 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 63 (Nov. 28, 2003).

[166] *Ticketmaster Corp. et al. v. Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 4553, 54 U.S.P.Q.2d (BNA) 1344 (C.D. Ca. 2000); *but see SNC Havas Numerique & SA Cadres on Line v. SA Keljob*, Commercial Court of Paris (Dec. 26, 2000) (asserting principle that simple links are implicitly authorized, but deep links need an explicit consent from the linked website and holding that the practice of deep linking to help wanted ads on rival services without giving credit to host site constituted "disloyal competition" that could be interpreted as "an appropriation of the work and efforts of others" and ordering the firm to stop deep linking), *reported in* WORLD INTERNET L. REP. (BNA) (Aug. 2001); *SA Keljob v. SNC Havas Numerique & SA Cadres on Line*, Tribunal de Grande Instance de Paris (Sept. 5, 2001) (finding that defendant infringed plaintiff's trademark and company name and ordering the payment of one million francs in damages) *reported in* WORLD INTERNET L. REP. (BNA) (JAN. 2002); *Competition Law and Internet Links: Case (AZ.: 312 0 606/00)*, WORLD INTERNET L. REP. (BNA) (May 2001) (Hamburg Regional Court recently enjoined company selling computer games on-line from maintaining a link to a competitor's website that gave misleading impression of a commercial arrangement between the two entities).

European courts are struggling with the issue as well. In Denmark, such deep-linking to newspaper articles by a search engine was held to violate the newspaper's rights under the European Union's Database Protection Directive, the Danish Court holding that the newspaper's website constituted a database and so was protected from the search engine's re-use, which adversely affected advertising revenue by bypassing the newspaper's home page.[167] One Dutch court held to the contrary, finding that deep links to newspaper articles infringed neither copyright nor database rights, while in another case, the Dutch Supreme Court found that deep links to listings of the Netherlands Association of Real Estate Brokers infringed both copyright and database rights.[168] In Germany, the Federal Supreme Court found deep links to press articles violated no rights and did not constitute unfair competition.[169] And in France, the Court of First Instance of Nanterre ruled that deep-linking to the website of a software developer did not constitute copyright infringement because: (i) the failure to link to the home page of the developer's website did not by itself constitute infringement; and (ii) the web page containing the deep link provided information about the software developer.[170]

News aggregators or websites that compile headlines and other content from other news websites have become one of the latest copyright challenges that the Internet poses to traditional media. While the law is not completely settled, some courts have held that aggregators of content in real-time misappropriate information since they unfairly capitalize on the research and work of competitors.[171]

The Digital Millennium Copyright Act,[172] enacted in October 1998, addresses some of these issues. The Act exempts service providers who meet its safe harbors from monetary damages and from injunctive relief beyond (i) an order requiring denial of access to infringing material at a specified site on the provider's system; (ii) an order requiring denial of access to an identified infringer and (iii) other relief necessary to prevent infringement of specified copyrighted material, if such relief is least burdensome to the provider as comparably effective relief.[173] The safe harbors apply to unaltered transmission of infringing material initiated by third parties; unknowing storage of or linking to infringing material, where the provider receives no direct financial benefit from the infringement and acts promptly to remove or block access to the material claimed to be infringing.[174]

---

[167] *Danish Newspaper Publishers Ass'n v. Newsbooster.com ApS*, Lower Bailiff's Court, Copenhagen (July 5, 2002) *reported in* WORLD INTERNET L. REP. (Aug. 2002) at 17. *See also* www.wired.com/news/politics/0,1283,54083,00.html; www.wired.com/news/print/0,1294,54083,00.html (reporting on a similar decision by Munich's Upper Court in Germany).

[168] J. Vreeman & P. Van der Putt, "An Update on Issues Impacting E-Commerce in the Netherlands" WORLD INTERNET L. REP. (BNA) at 11 (Oct. 2003).

[169] *Paperboy.de* (German Fed. Sup. Ct July 2003), *reported in* "Germany: Deep Linking Is Compatible with Copyright and Competition Law," WORLD INTERNET L. REP. (BNA) at 16 (Oct. 2003) and D. Cullen, "Deep Links Are Legal in Germany," THE REGISTER (July 20, 2003), www.theregister.co.uk/content/6/31838.html.

[170] Baker & McKenzie, *Deep linking may not constitute copyright infringement*, *reported in* Lexology (July 2, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=3fbd00d3-3eb3-48c0-a8e7-6f3af82e070d (subscription).

[171] See *Barclays Capital Inc. v. Theflyonthewall.com*, 2010 WL 1005160 (SDNY March 18, 2010) (holding that a website that aggregated research analysts' stock recommendations without permission was liable to several financial services firms for "hot news" misappropriation).

[172] H.R. 2281; Pub. L. No. 105-304, 17 U.S.C. § 512.

[173] H.R. 2281, Pub. L. No. 105-304 § 202(j).

[174] *A&M Records, Inc. et al. v. Napster, Inc.* 114 F. Supp. 2d 896 (N.D. Ca. 2000) (website not performing "passive conduit function" does not meet safe harbor under 17 U.S.C. § 512(a) and so is not entitled to protection; Napster

The DMCA also exempts service providers from liability for blocking or removing material in good faith based on information indicating it was infringing, even if it actually is not, provided the service provider acts promptly to notify the allegedly infringing subscriber of its action and, upon receipt of a counternotice, informs the putative copyright owner of the counternotice and advises that it will restore the material within ten business days unless an action is filed to enjoin the subscriber from the alleged infringement.

To qualify for the safe harbors, providers must designate an agent to receive notices and counternotices of these types. Moreover, it must adopt a policy for dealing with the notification process in a responsible manner. The Ninth Circuit held that America Online might have failed to do so and lost its DMCA protection when it changed the email addresses for DMCA notices without informing the Copyright Office or arranging for emails to be forwarded from the addresses it had previously used.[175]

Thus, the principal responsibility for policing infringement rests with the copyright owner.[176] The Ninth Circuit has held that service providers have no duty to police users' activity for infringement unless they have strong notice that infringement is taking place.[177] Moreover, because the DMCA requires that a takedown notice include a statement that the complaining party has a good faith belief that use of the material is unauthorized by the copyright owner or the law, at least one court has explicitly held that copyright holders must consider whether the material makes "fair use" of the copyright before requesting a service provider to remove purportedly infringing materials.[178]

In 2001, eBay Inc. won a precedent-setting decision in federal court under the DMCA. eBay was found not to have any liability for copyright infringement with respect to bootleg copies of a Charles Manson documentary sold on its site. eBay was contacted by the copyright owner who refused to submit a statement to eBay's Verified Rights Owner Program. The opinion stated that the copyright infringement actually occurred offline and that although eBay

---

was not mere conduit for file transfer, but offered search and directory functions to locate copyrighted music, and Napster had actual knowledge of infringing use); *RealNetworks Inc. v. Streambox Inc.*, C99-2070P (W.D. Wash. Dec. 23, 1999) (software that converted technologically protected copyrighted works into digital formats that could be copied, stored and freely distributed likely violated the Digital Millennium Copyright Act).

175 *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004).

176 Some copyright owners have even asserted that it would be an infringement of the copyright in the DMCA takedown notice to transmit the notice to third parties, such as chillingeffects.org. *See Tom Rubin*, *Anti-Transparency*, The Center for Internet and Society (Feb. 8, 2011), *available at* http://cyberlaw.stanford.edu/blog/2011/02/anti-transparency.

177 *Perfect 10 Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied* 128 S. Ct. 709 (2007). This standard places the burden on the copyright owner to enforce its legal rights under the DMCA by notifying service providers of potential infringement. Recent studies suggest that some media industry trade groups are overly aggressive in seeking to enforce their intellectual property rights under the Digital Millennium Copyright Act. A study from the University of Washington suggests that the Motion Picture Association of America, the Recording Industry Association of America and the Entertainment Software Association have sent hundreds of violation notices to universities based solely upon the I.P. addresses of students using certain file-sharing software, and not based upon whether copyrighted material was actually downloaded or uploaded. *The Inexact Science Behind DMCA Takedown Notices*, N.Y. TIMES (June 5, 2008), *available at* http://bits.blogs.nytimes.com/2008/06/05/the-inexact-science-behind-dmca-takedown-notices/.

178 *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D. Cal. 2008).

may facilitate the sale of pirated material, it does not have the right and ability to control such infringing activity, which is required for liability under the DMCA.[179]

However, online auction companies operating across international borders do not receive the same protection. On July 12, 2011, the European Court of Justice ruled that online auction marketplace operators such as eBay may be liable for trademark infringement where the operator plays an "active role" such that it has knowledge of or control over the data it hosts.[180] The ECJ stated that "EU trademark rules apply to offers for sale and advertisements relating to trademarked goods located in third countries as soon as it is clear that those offers for sale and advertisements are targeted at consumers in the EU."[181] The ECJ clarified that the operator will be liable if it was aware or should have been aware that the offers for sale in question were unlawful and failed to act expeditiously to prevent such acts.[182]

Consistent with the ECJ's position, the Paris Court of Appeals fined eBay International €200,000 for criminal handling of counterfeit goods in March 2012.[183] The court stated that eBay's passiveness in monitoring and ineffective sanctions demonstrated its will to further its own interests by not promptly closing the accounts of two users who had used multiple eBay accounts under pseudonyms to buy and resell large volumes of Chinese-manufactured counterfeit luxury products with brand names including Burberry, Chanel, Dior, Dolce & Gabana and Louis Vuitton.[184]

In 2010, Viacom sued YouTube for $1 billion in direct and secondary copyright infringement damages, claiming that over 100,000 infringing videos had been posted on its website.[185] The United States District Court for the Southern District of New York held that YouTube was not required to review users' content for potential copyright-infringement concerns before allowing the material to be posted to its site, stating that to "let knowledge of a generalized practice of infringement in the industry…impose responsibility on service providers to discover which of their users' postings infringe a copyright would contravene the structure and operation of the DMCA."[186] Thus, in the district court's view, general knowledge that infringement is commonplace does not give rise to a duty to search for, and eliminate infringing material. Unfortunately for YouTube, however, in April 2012, the Second Circuit reversed the district court and reinstated Viacom's infringement action.[187] While the appeals court agreed with

---

179 *Hendrickson v. eBay Inc. et al.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001). In January 2001, eBay had forgone its original policy of non-monitoring and began to search its site for copyrighted material, despite concerns as to whether knowledge would subject it to added liability in the event of infringement. Shannon Lafferty, *eBay Fears Liability as it Begins Policing Content*, THE RECORDER (Mar. 13, 2001).

180 Macdonald-Brown and Colbourn, *Online Marketplace Operator's Liability for Trademark Infringement*, 66 INT'L TRADEMARK ASS'N 16 (Sept. 15, 2011)*; EU High Court Rules Online Auctions May Be Liable for Trademark Infringement*, PAT., 82 TRADEMARK & COPYRIGHT J. 2024 (BNA) (March 16, 2012).

181 *EU High Court Rules Online Auctions May Be Liable for Trademark Infringement,* PAT., 82 TRADEMARK & COPYRIGHT J. 2024 (BNA) (March 16, 2012).

182 Macdonald-Brown and Colbourn, *Online Marketplace Operator's Liability for Trademark Infringement*, 66 INT'L TRADEMARK ASS'N 16 (Sept. 15, 2011).

183 *eBay International A.G. v. Burberry Ltd.*, Paris App. (March 6, 2012) reported in Mitchell, *Paris Appeals Court Rules eBay Liable for Sale of Counterfeit Luxury Goods*, 83 PAT., TRADEMARK & COPYRIGHT J. 2056 (BNA) (March 16, 2012).

184 *Id.*

185 *Viacom Int'l v. YouTube, Inc.*, 718 F. Supp. 2d 5l4 (S.D.N.Y. 2010).

186 *Id at 7.*

187 *Viacom Int'l v. YouTube*, 676 F.3d. 19 (2d Cir. 2012).

the lower court's reasoning that specific and identifiable knowledge of infringement, or of "red flags" suggesting infringement, is required to pierce the DMCA's safe harbor protections, the Second Circuit determined that there remained triable questions of fact with respect to YouTube's actual or "red flag knowledge" of infringement. Among other things, the Court of Appeals pointed to internal YouTube communications that referred to particular infringing videos.[188] Moreover, the Second Circuit held that the common-law doctrine of willful blindness may, in certain circumstances, be applicable to instances of infringement under the DMCA, and the issue was remanded to the district court to determine whether YouTube had engaged in a "deliberate effort to avoid guilty knowledge."[189] Although the Second Circuit's decision raises new questions for the district court, the good news for practitioners is that the court's opinion further solidifies the principle that a service provider's generalized knowledge of users' commonplace infringing activity is generally insufficient to remove the safe harbor protections of the DMCA. Based on *Viacom*, the Court in *Capitol Records, Inc. v. MP3tunes, LLC*, vacated its prior summary judgment decision favor of defendants on the issues of contributory infringement liability for songs "not subject to DMCA-compliant takedown notices" as well as defendants "lack of red flag knowledge" which were "material issues of fact that warrant trial."[190]

Similarly, a California district court ruled that an online service provider could invoke the protections of the DMCA's safe harbors where the provider adopted and implemented a policy of account terminations of repeat infringers.[191] In *Perfect 10, Inc. v. Google, Inc.*,[192] another California court held that Google's policy of terminating account holders on its Blogger service after receiving three valid DMCA notices of infringement was reasonable and an effective policy under the DMCA. These cases demonstrate the limits on a service provider's affirmative duty to prevent third-party infringement.

Despite these hurdles that copyright claimants may face, the potential liability for infringement claims and the responsibility to comply with the DMCA has not been lost on major forces in the computer and entertainment industries. In order to help stem the wave of infringement notices, Microsoft, NBC Universal and other computer and media companies have entered into an agreement "committed to eliminat[ing] infringement while content owners agree[] not to sue companies."[193] Although YouTube is not a party to the agreement, it shares in its "goals of principles."[194] YouTube also provides a service – described as a DMCA notice "substitute" – to companies seeking to police their copyrighted materials, creating a tool which allows a copyright owner to search the YouTube files and electronically notify YouTube upon a finding of infringement.[195] This sort of inter-company cooperation and private regulation may become commonplace as businesses seek to efficiently comply with the DMCA while avoiding unnecessary risk. For instance, a group of copyright owners and service providers recently agreed

---

188 *Id*.

189 *Id*.

190 2013 WL 1987225 (S.D.N.Y. May 14, 2013)

191 *Io Group, Inc. v. Veoh Networks, Inc.*, No. C06-03926, 2008 WL 4065872 (N.D. Cal., Aug. 27, 2008) (holding sufficient for the purposes of the DMCA's safe harbor provisions a policy whereby after a second infringement, a user's account is terminated, all material provided by the user is made inaccessible, and the user's email address and corresponding site account are blocked from the site).

192 *Perfect 10, Inc. v. Google, Inc.*, No. CV 04-9484 (C.D. Cal., July 26, 2010).

193 *Reported in* Joyce E. Cutler, *Beware of Unintended Consequences, E-Commerce Lawyers Are Warned*, PATENT, TRADEMARK & COPYRIGHT JOURNAL 280 (BNA) (June 20, 2008).

194 *Id*.

195 *Id*.

upon guidelines to follow to protect intellectual property while allowing entities or individuals to make use of user generated content. Among other things, the guidelines call for "(1) provid[ing] conspicuous notice [on website] terms of use that users may not submit infringing content; (2) implement[ing] content-filtering technology to automatically block infringing content that users may attempt to upload to their website; (3) provid[ing] content owners with [a] reasonable search capability to locate infringing content on the website; (4) if necessary, conduct[ing] a manual review of user-submitted content to determine if such content is infringing; and (5) expeditiously tak[ing] down infringing content and block and/or terminate users who repeatedly submit infringing content."[196]

E. *Defamation & the Communications Decency Act*

At one time, a similar concern might have been raised as to liability for defamation accessible through one's website. In *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[197] the court held Prodigy, an internet service provider (ISP) similarly placed to Netcom in the discussion above, to be liable to a securities firm as a publisher for allegedly defamatory statements posted on a Prodigy bulletin board. The court's decision relied on Prodigy's stated policy that it was "a family oriented computer network . . . that exercised editorial control over the content of messages posted on its computer bulletin boards." The court found that policy made Prodigy a publisher, rather than merely a distributor, of the notices posted on its bulletin boards, notwithstanding its argument that a manual review of the 60,000 messages per day posted to its bulletin boards was not feasible.

Stratton Oakmont thus faced on-line providers with a choice: forego editorial control over the content on your service and avoid legal liability for that content, or exercise some control, even imperfectly, and find yourself for whatever defamation your subscribers may commit. In 1996, however, Congress rejected this rule, in the Communications Decency Act made part of the Telecommunications Act of 1996. With the specific intent of overruling *Stratton Oakmont*, it added a new section 230 to the Communications Act of 1934, of which subsection 230(c)(1) provides that "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."[198]

Several years later, Prodigy was in court again arguing that they were not liable for defamation posted in a Prodigy chatroom by an imposter whom Prodigy had allowed to open several accounts.[199] The New York Court of Appeals upheld the trial court determination that, because Prodigy was not the publisher of the offending statements, they could not be held liable for those statements.[200] Over a decade later the New York Court of Appeals revisited the issue, affirming that a website provider could not be held liable for defamation for simply allowing defamatory material on its website.[201] The Court went further to hold that the immunity granted

---

196 "The CDA, DMCA, UGC, COPPA: Alphabet Soup and Online Legal Basics," *available at* http://www.wileyrein.com (2011); http://www.ugcprinciples.com/.

197 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710, 23 Media L. Rep. 1794 (Sup. Ct. Nassau Co. 1995).

198 47 U.S.C. § 230(c)(1). The Communications Decency Act has been held not to immunize an Internet service provider from contributory trademark infringement liability stemming from the conduct of one of its customers. *Gucci America Inc. v. Hall Associates*, 135 F. Supp. 2d 409 (S.D.N.Y. 2001); *Ford Motor Co. v. GreatDomains.com Inc.*, No. 00-CV-71544-DT (E.D. Mich. 2001).

199 *Lunney v. Prodigy Services Co.*, 250 A.D.2d 120 (1998), *aff'd*, 94 N.Y.2d 242, 723 N.E.2d 539 (1999), *cert. denied*, 120 S. Ct. 1832 (2000).

200 *Id*.

201 *Shiamili v. Real Estate Group of New York, Inc.*, 17 N.Y.3d 281 (June 14, 2011) reported in *Liability of Internet*

to service providers by the CDA extends even where the service provider takes an aggressive role in making content available, such as by exercising a publisher's traditional editorial functions, including adding headings, subheading and illustrations that do not "materially contribute" to the defamatory nature of the third-party statements.[202]

In a case involving acts of individuals, rather than ISPs, a California court applied the federal Communications Decency Act to dismiss libel claims against a woman who re-posted allegedly defamatory statements about a doctor, which were originally written by another person.[203] The court ruled that only the original author would be subject to a libel suit, even though if such activity had taken place in print media the libel claims against the defendant would be valid. One reason for the court's decision was that it is possible to quickly and inexpensively refute defamatory postings on the Internet.

Another California case, *Carafano v. Metrosplash.com, Inc.*,[204] recently strengthened the protection for ISP's under Section 230 of the Communications Decency Act. Defendant Matchmaker.com, an on-line dating service provider, required members to fill out an extensive multiple choice questionnaire and complete essays in response to specific questions. An unidentified third party posted a false profile under the name of the plaintiff, a television actress, including information, such as plaintiff's home phone number and address, with statements such as "looking for a one night stand" and that she liked being "controlled by a man." In response to plaintiff's claims, which included invasion of privacy and defamation, Matchmaker sought and was granted summary judgment under Section 230 of the Communications Decency Act because it did not "play a significant role in creating, developing or transforming the relevant information."[205]

Yet a third California case absolved eBay of liability for defamatory postings on its site by one user about another because of a release provision in its user agreement, but said that the Communications Decency Act did not provide immunity "for a distributor of information who knew or had reason to know that the information was defamatory.[206] In doing so, the court rejected the holding to the contrary of the U.S. Court of Appeals for the Fourth Circuit, which held that the Act did provide such immunity.[207]

Similarly, a federal district court in Florida found that the CDA protected a service provider from a suit over allegedly defamatory consumer reports even though the defendants had taken affirmative steps to encourage users to create the posts. In its holding, the court concluded that the service provider did not "create" or "develop" the posts.[208]

Service Providers: Closely Divided Court Upholds Immunity for Internet Provider Despite Its Arguably Active Role in Enhancing Defamatory Material, NYS Law Digest No. 621 (Sept. 2011).

202 *Id.*

203 *Barrett v. Clark*, 2001 WL 881259 (Cal. Sup. July 25, 2001) (unpublished opinion).

204 339 F.3d 1119 (9th Cir. 2003).

205 *Id.*, at 1125. *See also, Jurin v. Google Inc.*, 695 F. Supp. 2d 1117, 1123 (E.D. Cal. 2010) (Google's Adwords program, which suggests keywords, is a "neutral tool" that "does nothing more than provide options that advertisers could adopt or reject at their discretion, thus entitling [Google] to immunity" under the CDA).

206 *Grace v. Ebay Inc.*, 120 Cal. App. 4th 984 (Cal. App. 2d 2004).

207 *Zeran v. America Online, Inc.*, 129 F. 3d 327 (4th Cir. 1999). *See also Gentry v. eBay*, 99 Cal. App. 4th 816, 833 n.10 (2002).

208 *Whitney Information Network, Inc. v. Xcentric Ventures, LLC*, 2008 WL 450095, No. 204-CV-47-FTM-34SPC (M.D. Fla. Feb. 15, 2008); *See also Global Royalties, Ltd. v. Xcentric Ventures, LLC*, 2007 WL 2949002, No. 07-956-PHX-FJM (D. Ariz. Oct. 10, 2007) (broadly interpreting the CDA and holding that Section 230 protected the

In the context of burgeoning social networking sites, a mother and her minor child sued MySpace Inc. and News Corp. for negligence stemming from the daughter's sexual assault by a person she met on MySpace.com. The Fifth Circuit held that the Communications Decency Act barred the suit because – as provided in Section 230 – MySpace was not responsible as a "publisher" of user-generated content posted by a third party.[209]

The CDA has even shielded online businesses that manipulate the selection of third party content. In *Reit v. Yelp, Inc.*,[210] a dentist sued Yelp, an online aggregator of business listings and information, for defamation when Yelp deleted ten positive reviews of the dentist after he complained about one allegedly defamatory review. Reit claimed that Yelp should lose CDA immunity because its removal of positive posts was beyond the normal editorial function of selecting material for publication, and was an attempt to coerce businesses into paying for advertising on Yelp. The court disagreed with Reit and held that the defamation claim was barred by the CDA because the information was supplied by a third party, Yelp's use of "bad" posts in marketing did not change the nature of the posted data, and Yelp's selection of the posts it maintained on Yelp.com could be considered the selection of material for publication, an act which is related to a publisher's role.[211]

Recently, however, an Illinois state appellate court found that the CDA does not provide immunity from a negligence action based upon a company's alleged failure to supervise an employee who had used company computer and phone systems to threaten and harass a co-worker.[212]

Nor may creative plaintiffs avoid the CDA's immunity protections by obtaining a judgment directly against individual defamers and subsequently moving against a website operator for a third-party enforcement of injunction to remove the content. In a case of first impression, a federal district court in Illinois held that an internet website host could not be compelled to remove defamatory material from its website where the host was not a party to the underlying action, which resulted in an injunction requiring individual defendants to remove their defamatory postings.[213] Specifically, the court rejected the plaintiffs' argument that the website was in "active concert or participation" with the defamers because the site's terms of use included, among other things, a claim of ownership of posted materials by the website operator and a statement that comments would never be removed.[214]

By contrast, European courts have taken a more limited view of ISP immunity from liability stemming from third-party postings. Specifically, both French and British courts have

---

defendants against suit stemming from defamatory statements made by website visitors of the "Ripoff Report").

[209] *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008).

[210] *Reit v. Yelp, Inc.*, 2010 WL 3490167 (Sup Ct, NY County, Sept. 2, 2010).

[211] Note that the CDA does not come into play in an action against the poster of information on a site like Yelp. Thus, in an action by a home contractor over allegedly defamatory postings by a former customer on a popular business review website, where the customer had also alleged that the contractor posted defamatory comments about her, a jury found that each side had defamed the other, so neither was entitled to damages. *See Dietz Development LLC v. Perez*, CL 2012-16249 (Va. Cir. Ct., Fairfax County), jury verdict, 1/31/14.

[212] *Lansing v. Southwest Airlines Company*, 2012 IL App (1st) 101164 (2012).

[213] *Blockowicz v. Williams*, 675 F. Supp. 2d 912 (N.D.Ill. 2009).

[214] With respect to similar arguments seeking to avoid the immunity protections of the CDA on the basis of a website's "copyright" or "ownership" of its content, a New York Court in *Finkel v. Facebook, Inc. et al.*, Index No. 102578/09 (N.Y. Sup. Ct., New York Cty., Sept. 16, 2009), ruled that "'Ownership' of content plays no role in the [CDA's] statutory scheme." Thus, Facebook was not liable for defamatory content notwithstanding its terms of use purporting to grant it an ownership interest in the content.

ruled recently that ISPs are not liable for postings on their websites, provided that they take all reasonable steps to remove an offending statement once they are notified of it.[215] The Electronic Commerce Directive[216] limits the liability of ISPs for unlawful material on their websites,[217] provided that the ISP is not the original sender of the material, does not select the receiver, does not select or modify the information sent, has no knowledge of illegal activity or information stored, and upon obtaining such knowledge, acts expeditiously to remove or disable access to such activity or information.[218]

In contrast, where the website in question is operated by the actual content provider, as with newspaper and magazine websites, for example, foreign courts appear more prepared to find jurisdiction and apply the law of jurisdictions where the alleged defamation is accessible than are U.S. courts.[219] Thus a court in France recently ruled that service providers will not be immune from liability stemming from user-submitted material where the service provider was involved in the "organization and presentation" of the link and headline.[220]

Moreover, the pendulum may be swinging back in the other direction in the United States. Despite its broad application, defenses under the CDA have not always been successfully asserted. Due to defendants' many successes invoking the CDA, parties have been increasingly creative in attempting to apply the CDA. The results have been mixed.

Thus, for example, in one case, the defendants operated a website which was engaged in "obtaining and selling confidential customer phone records without the affected customers' authorization." The court held that the CDA could not shield the defendants from an action brought by the FTC which alleged violations of the Act's prohibition on unfair business practices. The court reasoned that such use of the CDA would be contrary to "the legislative intent and statutory purpose of the CDA's immunity provision."[221] Similarly, an employer could not shield itself from Title VII liability by invoking the CDA where an employee had viewed her

---

[215] *See Multimania Production v. Linda Lacoste* (Versailles Ct. of App. 2000) (removal of unauthorized photos upon notification of such infringement satisfied "best effort" requirement relieving ISP of liability); *Godfrey v. Demon* (*reported in* 2 E-COMMERCE L. WKLY. (NLP IP Co.) 381, 4/6/00) (British ISP liable for failure to remove statement falsely attributed to someone else, despite notification of such statement); *Liability of Internet Service Providers: Bertrand Delanoe v. Ste. Alta Vista Company et al., (July 31, 2000), reported in* WORLD INTERNET L. REP. (BNA) (Feb. 2001), at 13 (the Internet service provider who hosted a minor's activities allegedly violating French legislation by posting hate speech via an Internet site devoted to Nazism was spared from prosecution); Laurent Szukin and Maria Saarinen, *Legislation on ISP's Liability*, WORLD INTERNET L. REP. (BNA) 10/00 at 5 (an amendment voted on June 28, 2000, modified the 1986 French Broadcasting Act to provide that an ISP could be held liable for the content of the websites it was hosting if a court has ordered it to disable access to a website and it has not, or if after a warning from a third party asserting that the websites it was hosting contained illegal or damaging information it has not implemented the necessary degree of care.

[216] As discussed above in Section I. C. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 (the "E-Commerce Directive"), *available at* http://www.tourismlaw.eu/documents/tourism_legislation/EU_8june2000_uk.pdf.

[217] "European Parliament Swiftly Passes Electronic Commerce Directive" E-COMMERCE L. WKLY. (NLP IP Co.) (5/1/00) at 544.

[218] Marino, Donatella and David Fontana, "The EU Draft Directive on Electronic Commerce" WORLD INTERNET L. REP. (BNA) 3/00 at 27; Laurent Szukin and Maria Saarinen, *Legislation on ISP's Liability*, WORLD INTERNET L. REP. (BNA) 10/00 at 5.

[219] *See* discussion in Section I.B., *supra*.

[220] *See* Steptoe & Johnson, *E-Commerce Law Week* (April 19, 2008) (discussing a recent ruling by the Paris Court of First Instance), *available at* http://www.steptoe.com/publications-5275.html.

[221] *FTC v. Accusearch, Inc.*, 2007 WL 4356786, No. 06-CV-105-D (D. Wyo. Sept. 28, 2007), *reported in* Steptoe & Johnson, *E-Commerce Law Week* (Oct. 27, 2007).

co-workers' pornographic materials displayed on a workplace computer.[222] And in another case, the CDA could not shield a defendant from a New Hampshire state "right of publicity claim," as such a claim is a "law pertaining to intellectual property" and was therefore not preempted by the CDA.[223] Finally, in *Fair Council of San Fernando Valley v. Roommate.com, LLC*[224] the 9th Circuit rejected the defendants' assertion that the CDA barred a discrimination claim stemming from allegedly discriminatory profiles created by the users of the defendants' website. The court noted that the website operators contributed to the development of the allegedly discriminatory profiles by requiring members to choose from among a limited number of defendant-generated profile descriptions (*i.e.*, they required users to disclose their sex, family status, and sexual orientation, as well as those of their desired roommate). Moreover, the defendants' search and e-mail systems were "designed to steer users based on discriminatory criteria." (Several courts have narrowly interpreted the Ninth Circuit's *Roommate.com* ruling as applying only to those instances in which a website "required" its users to participate in unlawful conduct.)[225]

Consequently, while the CDA has been broadly and successfully asserted by defendants in the past, courts have begun to find the CDA inapplicable in cases in which applying the CDA would be contrary to other public policy, or where the defendant played a significant role in the alleged conduct.

---

[222] *Avery v. Idleaire Technologies Corp.*, 2007 WL 1574269, No. 3:04-CV-312 (E.D. Tenn. May 29, 2007) (the court was "not aware of any federal case in the country that has applied this Act in such a manner"); *c.f. Doe v. City of New York*, 2008 WL 781640, No. 06-CV-13738 (S.D.N.Y. Feb. 6, 2008) (Section 230 does not shield a defendant from a discrimination claim because he added his own allegedly tortious speech; the court also found that CDA immunity does not apply to individual users) *reported in* Steptoe & Johnson, *E-Commerce Law Week* (Mar. 29, 2008).

[223] *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D. N.H. 2008) (disagreeing with *Perfect 10, Inc. v. CCBill LLC* and noting that the plain language of the CDA statute provides that it shall not "be construed to limit or expand any law pertaining to intellectual property"), *reported in* Steptoe & Johnson, *E-Commerce Law Week*, Steptoe Johnson (April 5, 2008).

[224] 521 F.3d 1157 (9th Cir. 2008) ("[i]f you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune"), *reported in* Steptoe & Johnson, *E-Commerce Law Week* (April 12, 2008); *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666 (7th Cir. 2008) (CDA barred plaintiff's claim where Craigslist published allegedly discriminatory housing advertisements, but noting that the defendant might have been liable if it had encouraged people to post the discriminatory ads), *reported in* Steptoe & Johnson, *E-Commerce Law Week* (March 22, 2008).

[225] For instance, in *Nemet v. Consumeraffairs.com*, 591 F.3d 250, 256-57 (4th Cir. 2009), the plaintiffs relied on *Roommate.com* for the proposition that the defendant website operator could not avoid liability under the CDA where it "participated in the preparation of [defamatory automobile] complaints by soliciting the complaint, steering the complaint into a specific category designed to attract class action lawyers, contacting the consumer to ask questions about the complaint and to help her draft or revise her complaint …." As such, the plaintiffs argued, the defendant was responsible for the "creation or development" of the allegedly defamatory posts so as to be a non-immune information content provider. The Fourth Circuit rejected the plaintiffs' argument and distinguished *Roommate.com*, holding that "[w]hereas the website in *Roommate.com* required users to input illegal content as a necessary condition of use, … Consumeraffairs.com [is allegedly to have merely] structured its website and its business operations to develop information related to class-action lawsuits," which itself is "a legal undertaking." Similarly, in *Dart v. Craigslist, Inc.*, 665 F. Supp. 2d 961, 968-69 (N.D. Ill. 2009), the court found that Craigslist was immune under Section 230, notwithstanding allegations that it hosted and organized user-generated prostitution classifieds. Specifically, the court found that Craiglist's creation of an "adult" classified section was not active inducement of illegal prostitution because the section did not necessarily call for illegal conduct. The court noted that in *Roommate.com*, the users were "required" to answer discriminatory questions. *See also, Goddard v. Google, Inc.*, 640 F. Supp. 2d. 1193 (N.D. Cal. 2009) (Google immune under the CDA – and not responsible for "creating or developing" fraudulent advertisements – where the Google AdWords program suggested keywords to advertisers, but did not "require" them).

F. *Trademark Infringement*

It is worth a brief look as well at some of the trademark issues raised by the Internet. In general, normal trademark rules apply. One cannot use the trademark of another if likelihood of confusion will result. Thus, whether the confusing use of the trademark of another is in the domain name itself,[226] or in a "metatag"[227] that is invisible to human viewers but detected by search engines,[228] it generally will be enjoined.[229]

Similarly, when Netscape Communications and Excite Inc. sold to advertisers the right to display banner advertisements to users who used the words "playboy" and "playmate" in their search requests, the Ninth Circuit held that such conduct was actionable, if consumer confusion was shown. The Court of Appeals remanded for a determination as to the extent of such confusion, in light of a survey offered to show that most users believe such ads come from the company that owns the trademarked search term.[230] The Court made a point of noting it was not addressing the situation in which the banner ad clearly identified the sponsor or overtly compared the sponsor's products to those of the trademark owner. It thus squarely made the issue of confusion determinative, calling it the "core element of trademark infringement."

Such "initial interest confusion," where a user is diverted to the site of someone other than the trademark owner and, once there, decides to stay even if it is not the site originally sought, was precisely the basis for the holding in *Flow Control Industries Inc. v. AMHL, Inc.*,[231] which found metatags in a website containing a competitor's trademarks to be infringing because they diverted traffic from the competitor's site to that of the infringer. Numerous courts have

---

[226] *E.g., Panavision Int'l v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998); *Playboy Enterps., Inc. v. Calvin Designer Label*, 985 F. Supp. 1220 (N.D. Cal. 1997).

[227] While several courts have ruled that metatags could be the basis for a trademark infringement claim, one court has held that "modern search engines make little if any use of metatags" and instead rely on "algorithms that rank a website by the number of other sites that link or point to it." *Standard Process, Inc. v. Banks*, 554 F. Supp. 2d 866 (E.D. Wis. 2008), *reported in* Steptoe & Johnson, *E-Commerce Law Week* (May 10, 2008). Indeed, in September 2009, Google announced that its search algorithm does not use keyword metatags in ranking search results. (The announcement is available at http://googlewebmastercentral.blogspot.com/2009/09/google-does-not-use-keywords-meta-tag.html.) It remains to be seen whether the *Standard Process* ruling is an isolated occurrence.

[228] *E.g., Promatek Industries Ltd. v. Equitrac Corp.*, 300 F.3d 808 (7th Cir. 2002) (requiring disclaimer on website redirecting users to plaintiff's site even though defendant had removed infringing metatags after suit was filed); *Brookfield Communications Inc. v. West Coast Entertainment Corp.*, 174 F.3d 1036 (9th Cir. 1999) (finding "initial interest confusion" where a user is diverted to the site of someone other than the trademark owner and, once there, decides to stay even if it is not the site originally sought); *Playboy Enters., Inc. v. Calvin Designer Label*, 985 F. Supp. 1220 (N.D. Cal. 1997); *Genertel v. Crowe Italia*, Court of Rome (Jan. 18, 2001) (penalizing an insurance company which used the name of a competitor in a meta-tag on its own site), *reported in First Italian Decision on Meta-Tags*, WORLD INTERNET L. REP. (BNA) (June 2001); *but see Chatam Int'l Inc. v. Bodum Inc.*, 157 F. Supp. 2d 549 (E.D. Pa. Aug. 10, 2001) (holding that initial interest confusion does not apply to websites as Internet users are accustomed to finding that a website is not exactly what they were seeking and applying such reasoning to dispute between a coffee company and a liquor company denying claim under the Anticybersquatting Consumer Protection Act).

[229] *But see North American Medical Corporation v. Axiom Worldwide, Inc.*, 522 F.3d 1211 (11th Cir. 2008) (citing the Supreme Court's holding in *eBay v. MercExchange LLC*, 547 U.S. 388 (2006) for the proposition that a finding of infringement, "use in commerce," and a likelihood of confusion does not automatically warrant an injunction without also showing irreparable harm).

[230] *Playboy Enterprises, Inc. v. Netscape Comm'ns Corp.* 345 F.3d. 1020 (9th Cir. 2004).

[231] 278 F. Supp. 2d 1193 (W.D. Wash. 2003). *See also SNA, Inc. v. Array*, 51 F. Supp. 2d 554 (E.D. Pa. 1999).

now followed this approach.[232] (Courts have differed, however, with respect to when the use of competitive trademarks might constitute nominative fair use.[233])

These issues have been raised repeatedly by Google's AdWords program under which it sells sponsored links to advertisers, whose advertisements appear when users make Google searches using the particular keywords.[234] When the keyword is a competitor's trademark, infringement claims have ensued. Most appeals courts have determined that such use of the competitor's trademark is a "use in commerce" and so actionable under the Lanham Act, even where the consumer never sees the trademark in an ad or on any goods or displays.[235] These courts have then moved on to a determination of whether there was consumer confusion. Thus, in a case in which competitors of auto insurer Geico purchased sponsored links using "Geico" as the keyword, the Court found there to be a use in commerce, but went on to uphold the practice, finding insufficient evidence of consumer confusion where the word "Geico" did not actually appear in the sponsored link, but it allowed a claim against Google for contributory infringement

---

[232] *E.g.*, *Australian Gold, Inc. v. Hatfield*, 436 F. 3d 1228 (10th Cir. 2006); *Amerigas Propane L.P. v. Opinion Corp. d/b/a Pissedconsumer.com*, 2012 WL 2327788 (E.D. Pa. 2012) ("gripe" website's use of trademarks to generate ads from trademark owner's competitors can cause initial interest confusion despite ease of recognizing and leaving site); *Shainin II LLC v. Allen*, 2006 WL 1319405 (W.D. Wash. 2006), *available at* http://pub.bna.com/ptcj/06420May15.pdf ; *TData, Inc. v. Aircraft Technical Publishers*, No. 2:03-cv-264, 411 F. Supp. 2d 901 (S.D. Ohio, Jan. 23, 2006); *but see, Designer Skin, LLC v. S & L Vitamins, Inc.*, 560 F. Supp. 2d 811 (D. Ariz. 2008) (explicitly disagreeing with the 10th Circuit's decision in *Australian Gold, Inc.*, and holding that no initial interest confusion was created by the defendant's mere use of the plaintiff's marks in the metagtags of the defendant's website where the website actually offered the plaintiff's products; no "bait and switch" had occurred); *Standard Process, Inc. v. Banks*, 554 F. Supp.2d 866 (E.D. Wis. 2008) (holding that because defendant's site sold genuine products of the plaintiff and the site owner was not a direct competitor of the plaintiff, the metatags were fair and there was no infringement); *Designer Skin, LLC v. S&L Vitamins, Inc.*, 560 F. Supp.2d 811 (D. Ariz. 2008) (holding that plaintiff's mark in defendant's metatags did not result in initial interest confusion where the marks were embedded to truthfully assist consumers in locating the plaintiff's products available for sale through the site, and where the defendant posted a disclaimer that it was not affiliated with, or authorized to sell plaintiff's products).

[233] *Compare Horphag Research Ltd. v. Pelligrini*, 337 F.3d 1036 (9th Cir. 2003), *cert. denied sub nom. Garcia v. Horphag Research Ltd*., 124 S.Ct. 1090, (2004*)* (use of trademark in metatag is likely to confuse consumers, precluding nominative fair use defense) *with J.K. Harris & Co. v. Kassel*, 253 F. Supp. 2d 1120 (N.D. Cal. 2002) (references to competitor's trademarks on site containing criticism of competitor were permissible nominative fair use). *See also Promotek Ind. Ltd. v. Equitrac Corp.*, 300 F.3d 808 (7th Cir. 2002) (amended opinion) (trademarks may be used in metatags only where use is legitimate, but not where use deceives consumers). *See also Playboy Enterprises, Inc. v. Welles*, 162 F. 3d 1169 (9th Cir. 2002) (former Playmate of the Year entitled to use Playboy trademarks in metatags as nominative use).

[234] According to Google, 97% of its revenue comes from advertisers. Viscounty, Barry and Olson, "Trademark as Keyword: It's Use, But Is It Confusing?," 77 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 688 (April 17, 2009).

[235] *See, e.g., Rescuecom Corp. v. Google, Inc.*, 562 F.3d 123 (2d Cir. 2009) (holding there was a "use in commerce" and remanding to the district court to determine whether a likelihood of confusion exists); *Network Automation Inc. v. Advanced Sys. Concepts Inc.* 638 F.3d 1137 (9th Cir. 2011) (agreeing with Second Circuit precedent that "use of a trademark as a search engine keyword that triggers the display of a competitor's advertisement is a 'use in commerce' under the Lanham Act"); *Tiffany (NJ) Inc. v. eBay Inc.*, No. 04 Civ. 4607, 2008 WL 2755787 (S.D.N.Y. July 14, 2008) (holding that eBay's visible use of the Tiffany mark was an actionable "use," and rejecting eBay's analogy to *1-800-Contacts* as only applicable to internal use of trademarks); *1-800 Contacts Inc. v. Lens.Com Inc.*, No. 2:07-cv-00591-CW-DN (D. Utah 2010), *reported in* "Invisible AdWords Were 'Uses' of Mark, But Only Text Could Generate Potential Confusion," 81 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 253 (Dec. 24, 2010) (holding that the Lanham Act does not require use *and* display of another's mark for it to constitute "use in commerce").

to proceed with respect to sponsors' links that contained the word "Geico" in the text of the advertisement itself.[236]

Other cases have taken a similar approach.[237] Such confusion has been found, for example, where a competitor not only purchases a holder's mark as a keyword, but also uses the mark in the resulting search display.[238] With respect to the liability of Google itself, however, a federal district court in California has held that Google itself could not be liable for "false designation of origin" under the Lanham Act[239] stemming from Google's sale of the plaintiff's trademarked name in the AdWords program.[240] In so holding, the California court found that Google "in no way directly represented that it is the producer of the [plaintiff's] product" and, accordingly, no confusion resulted. Finally, the law surrounding these issues remains unsettled in other jurisdictions. In one recent case from Kentucky, the defendants purchased the plaintiffs' "XGD" trademark as a search engine keyword. The district court denied the defendants' motion to dismiss, citing the "uncertain state of the law" on the issue.[241] But at least the Ninth Circuit is demonstrating increasing confidence in web users and their ability to avoid confusion. In a case involving Lanham Act claims over the purchase of a trademark displayed in the sponsored links section of Google and Bing, the Court held that established legal tests for trademark infringement should be construed loosely and practically when applied to evolving technologies, stating that

---

[236] *Gov't Employees Ins. Co. v. Google, Inc.*, 2005 WL 1903128 (E.D Va. August 8, 2005); 330 F. Supp. 2d. 700 (E.D. Va. 2004) (bench ruling), *transcript available at* http://pub.bna.com/ptcj/benchrulingDec15.htm.

[237] *E.g.*, *Hysitron Inc. v. MTS Sys. Corp.*, No. CIV 07-01533, 2008 WL 3161969, at *3 (D. Minn. Aug. 1, 2008) ("The language used in the definition suggests that a 'use in commerce' is not limited to affixing another's mark to one's own goods but also encompasses any use of another's mark to advertise or sell one's own goods and services;" disputed issue as to consumer confusion); *Venture Tape Corp. v. McGills Glass Warehouse*, 540 F.3d 56 (1st Cir. 2008) (competitor used manufacturer's marks by embedding the marks in its website, causing consumer confusion); *J.G. Wentworth, S.S.C. Ltd. Partnership v Settlement Funding LLC*, 2007 WL 30115 (E.D. Pa. 2007) (keyword purchase constitutes use in commerce, but no likelihood of confusion); *Google, Inc. v. American Blind & Wallpaper Factory, Inc.*, 2007 WL 1159950 (April 18, 2007) (not for citation) (finding use in commerce, disputed issues of fact as to likelihood of confusion); *Boston Duck Tours, LP v. Super Ducks Tours, LLC*, 527 F. Supp. 2d 205 (D. Mass. 2007) (holding that "sponsoring linking necessarily entails the 'use' of the plaintiff's mark as part of a mechanism of advertising," but finding no consumer confusion); *Buying for the Home v. Humble Abode LLC*, 459 F. Supp. 2d 310 (D.N.J. 2006), *available at http://pub.bna.com/ptcj/032783Oct20.pdf*;. *800-JR Cigar Inc.*, 437 F. Supp. 2d 273 (D.N.J. 2006) (finding use in commerce, material issues of fact as to likelihood of confusion); *Edina Realty Inc. v. TheMLSonline.com*, No. 04-4371, 2006 WL 737064 (D. Minn. Mar. 20, 2006), *available at* http://pub.bna.com/ptcj/044371Mar20.pdf (same); *Google, Inc. v. American Blind & Wallpaper Factory, Inc.*, 744 U.S.P.Q. 2d 1385, 2005 WL 832398 (N.D.Cal. 2005) (denying motion to dismiss).

[238] *North American Medical Corp. v. Axiom Worldwide, Inc.* 522 F.3d 1211 (11th Cir. 2008) (competitor's conduct amounted to a "use in commerce" and created a likelihood of confusion where competitor visibly used trademark holder's trademarks in the search results triggered by the Google search engine); *Standard Process, Inc. v. Total Health Discount, Inc.*, 559 F. Supp. 2d 932 (E.D. Wis. 2008) (confusion created by competitor's prominent use of trademark holder's name in advertising resulting from search engine); *Storus Corp. v. Aroa Marketing, Inc.*, No. C-06-2454, 2008 WL 449835 (N.D. Cal. Feb. 15, 2008) (summary judgment on plaintiff's trademark claims granted where competitor purchased trademark as a Google Adwords term, the related advertisements actually used the trademark name, and consumer diversion occurred); *but see*, *Designer Skin, LLC v. S & L Vitamins, Inc.* 560 F. Supp.2d 811 (D. Arizona 2008) ("[T]he mere fact the S & L Vitamins uses Designer Skin's marks in the metatags of its sites and as search-engine keywords does not result in initial interest confusion. Designer Skin must [also] show that these uses are deceptive.").

[239] 15 U.S.C. § 1125(a).

[240] *Jurin*, 695 F. Supp. 2d at 1122 (nor could the plaintiff assert a false advertising claim against Google because Google and the plaintiff were not "direct competitors").

[241] *T.D.I. International, Inc. v. Golf Preservations, Inc.*, No. 6:07-313-DCR, 2008 WL 294531 (E.D. Ky., June 12, 2008).

consumers know the difference between sponsored links and actual search results.[242] The Ninth Circuit determined that the most relevant factors for consideration in this case were: (1) strength of the mark, (2) evidence of actual confusion, (3) type of goods and degree of care likely to be exercised, and (4) labeling and appearance of the advertisements and content on the screen displaying the search results.[243]

In a setback for Google, a 2012 Fourth Circuit decision reversed summary judgment in favor of Google over its use of trademarks to trigger competitors' advertisements.[244] The district court in Virginia had declined to hold Google accountable for trademark infringement when it auctioned Rosetta Stone's trademarks in its advertisement platform.[245] The district court had held that Google's generalized knowledge that counterfeiters bid on trademarks to place advertisements does not amount to the sort of "specific contemporary knowledge" warranting a finding of infringement. The court further maintained that there was little Google could do beyond expressly prohibiting advertisements for counterfeit goods, taking down those advertisements when it learned of their existence, and creating a team dedicated to fighting advertisements for counterfeit goods.[246] Furthermore, the court stated that there was no likelihood of confusion as to the source of Rosetta Stone's goods, since users of Google's search engine understand the difference between "organic" search results and the separately labeled "Sponsored Links."[247] Reversing, the Fourth Circuit found disputed issues of fact over Google's intent to cause confusion, citing evidence of actual consumer confusion, Google in-house studies indicating a high likelihood of confusion, and an expert survey, all of which led the Court to "conclude that a reasonable trier of fact *could* find that Google intended to cause confusion in that it acted with the knowledge that confusion was very likely to result from its use of the marks."[248] The case between Rosetta Stone and Google eventually settled before being heard again in the District Court, leaving unresolved the question of how to prove liability where trademarks are used as keywords for online ads.[249]

Battles concerning similar trademark issues have been waged in foreign courts as well. French courts have held against Google France, finding, for example, that it was guilty of trademark infringement by selling sponsored links to online travel agencies that appear whenever users searched for phrases that were trademarks of competing travel agencies.[250] This French case poses serious problems for keyword advertising, as the trademark in question, "bourse de

---

[242] *Network Automation, Inc. v. Advanced Sys. Concepts, Inc.*, 638 F. 3d 1137 (9th Cir. 2011).
[243] *Network Automation, Inc. v. Advanced Sys. Concepts, Inc.*, 638 F. 3d 1137, (9th Cir. 2011).
[244] *Rosetta Stone Ltd. v. Google, Inc.*, No. 10-2007 (4th Circuit April 9, 2012), *available at* http://www.courthousenews.com/home/OpenAppellateOpinion.aspx?OpinionStatusID=32057.
[245] *Rosetta Stone Ltd. v. Google Inc.* 730 F. Supp. 2d 531 (E.D. Va. 2010).
[246] *Id.*
[247] *Id.*
[248] *Rosetta Stone Ltd. v. Google, Inc.*, No. 10-2007 (4th Circuit April 9, 2012), *available at* http://www.courthousenews.com/home/OpenAppellateOpinion.aspx?OpinionStatusID=32057. at 17.
[249] *See Tough Road For Keyword Ad Suits After Rosetta Stone Deal*, Law360 (Nov. 19, 2012), *available at* http://www.law360.com/m/ip/articles/395055 (subscription required).
[250] *Societé Luteciel v. Google France*, No. 03/00051 (Trib. de Gr. Inst. Nanterre Oct. 13, 2003), *reported in* 66 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 701 (Oct. 24, 2003); *see also Google France v. Louis Vuitton Malletier* (Cour d'Appel de Paris June 28, 2006), *reported in* WORLD COMM. REG. REP. (BNA) (Aug. 2006), *available at* http://www.legalis.net/jurisprudence-decision.php3?id_article=1661 (sale of online advertising triggered by plaintiff's trademarks constituted trademark infringement, unfair competition and false advertising; decision to be reviewed by the European Court of Justice (Case No. C 236/08).

voyages," simply means "travel exchange," and the keyword purchased was not the trademark, but simply "voyages" or "travel." That resulted in competitors' sites appearing when the trademark – which included the keyword – was entered as a search term. The case in effect would require Google to exclude sponsored links from appearing when a trademark was entered by a user, even if the purchased keyword is merely a part of the trademark. Given that no universal trademark database exists, the AdWords program becomes unmanageable. And in February 2010, eBay was fined €230,000 by a French court for infringement stemming from eBay's use of search engine keywords that were various *misspelled* versions of "Louis Vuitton,"[251] which was found to be misleading to consumers.

Courts in other nations have held similarly. In the United Kingdom, use of a trademark in a metatag to divert traffic was held to constitute trademark infringement.[252] Canadian courts have reached similar conclusions, finding the use of metatags identical to domain names or trademarks of others to constitute actionable "passing off."[253]

A German court enjoined a similar arrangement where trademarks of Estée Lauder, such as "Clinique," when used as search terms in the Excite Search engineer, would cause an ad for Fragrance Counter, an Internet seller of perfumes and cosmetics, to appear,[254] and a French court enjoined the use of metatags embodying a French company's registered corporate name on the website of a direct competitor.[255] The British High Court of Justice reached a similar conclusion.[256]

In March 2010, however, the European Court of Justice in Luxembourg handed down a far-reaching opinion that bolsters the legality of Google's AdWords program across Europe.[257] In a decision that applies to all 27 EU member countries, the ECJ held that Google does not "use" a mark in the course of trade when it sells the marks as keywords to thirty-party advertisers.[258] The court appeared to reason that Google itself – unlike the advertisers – does not use the mark in connection with any communication to consumers.[259] Rather, Google merely "stored" the

---

[251] *See French Court Finds For LVMH in EBay Keyword Spat*, Law360 (Feb. 11, 2010), *available at* http://www.law360.com/registrations/user_registration?article_id=149212&concurrency_check=false (subscription required).

[252] *Reed Executive Plc v. Reed Business Information Ltd.* (Eng. High Ct. Just. May 20, 2002) (unreported decision), reported in S. Burshtein, *Metatags in Canada*, WORLD INTERNET L. Rep. (BNA) at 12 (Jan. 2003).

[253] *Saskatoon Star Phoenix Group Inc. v. Nohon*, 12 C.P.R. 4th 4 (Sask. Ct. Q.B. 2001), *reported in* Bushtein, *supra*; *British Columbia Automobile Ass'nv. O.P.E.I.U. Local 378*, 10 C.P.R. 4th 423 (B.C. Sup. Ct. 2001), *reported in* Bushtein, *supra*.

[254] *In re Estée Lauder Cosmetics Ltd*. (Dist. Ct. Hamburg February 16, 2000).

[255] *S.F.O.B. v. Notter GmbH*, Paris Ct. App. (Mar. 13, 2002), *reported in* the l.i.n.k. Legal Infosoc News Kiosk (July-Aug. 2002) *available at* http://www.vocats.com.

[256] *Reed Executive PLC v. Reed Business Information Ltd.*, High Ct. Justice (May 20, 2002), *reported in* WORLD INTERNET L. REP (BNA) 22 (July 2002).

[257] *Google France & Google Inc. v. Louis Vuitton Malletier, Google France v. Viaticum & Luteciel and Google France v. CNRRH, Pierre-Alexis Thonet, Bruno Raboin & Tiger, franchisee Unicis*, Joined Cases C-236/08, C-237/08 and C-238/08.

[258] The ECJ Advocate General's September 22, 2009, advisory opinion stated that while there was a use within the "course of trade," "the use of trademarks is limited to selection of keywords that is internal to AdWords and concerns only Google and the advertisers" and "such a use cannot therefore be considered as being a use made in relation to good or services …." Advocate General's Opinion in Joined Cases C-236/08, C-237/08 and C-238/08, *Google France & Google Inc. v. Louis Vuitton Malletier, Google France v. Viaticum & Luteciel and Google France v. CNRRH, Pierre-Alexis Thonet, Bruno Raboin & Tiger, franchisee Unicis.*

[259] Cases C-236/08 to C-238/08 ("An internet referencing service provider which stores, as a keyword, a sign identical with a trademark and organises the display of advertisements on the basis of that keyword does not use that

keywords, in the court's view. Consequently, Google could not be liable for trademark infringement under the European Trademark Directive.[260] (The ECJ's holding that Google does not "use" the mark is contrary to the position adopted by most U.S. appeals courts.) The ECJ did, however, give warning to the third-party keyword advertisers, holding that such parties may be liable for infringement where they use the identical mark as a keyword and sell identical products if "normally informed and reasonably attentive internet users" are unable to easily discern the origination of the advertised goods, as determined by the national court before which the case appears.[261] Further, the court found that whether Google was eligible for protection under the E-Commerce Directive as an "internet referencing services provider" depended on whether Google played an active role of such a kind as to give it knowledge of, or control over, the data stored, which is also to be determined at the national-court level.[262] Thus, the court did not foreclose the possibility that Google may be liable for contributory trademark infringement or for violations of other laws.[263]

Indeed, recent international cases suggest a trend towards the legality of trademark use in advertisements under certain conditions. In 2010, the Paris Court of Appeals overturned the decision of a lower court against Google for trademark infringement in connection with the AdWords program, holding that Google qualified under the so-called host-provider liability exclusion under EU and French law.[264] And in Canada, British Columbia's top court upheld a

---

sign within the meaning of [the Trademark Directive]."

[260] Trade Mark Directive, Council Directive 89/104/EEC. As a result of this ruling, Google Inc. announced that it will soon allow advertisers in most European countries to select a third party's trademark as an AdWords keyword. While companies will be allowed to purchase the trademarked keyword, advertisers who own the trademark will be permitted to petition Google for review if they feel ad text is confusing users about the origin of their advertised goods and services. Dye, "Google to Allow Trademarked Ad Keywords in EU," *reported in* Law 360 (August 4, 2010), *available at* http://www.law360.com/prototype/ip/articles/185219/google-to-allow-trademarked-ad-keywords-in-eu (subscription required).

[261] *See also Portakabin Ltd v. Primakabin BV*, (Case C-558/08) (where the ECJ held that use of a trademark will not infringe, unless there is a legitimate reason which justifies the proprietor in opposing that advertising, such as use of the mark that gives the impression that the advertiser and the trademark proprietor are economically linked, or use that is seriously detrimental to the reputation of the mark); *see also Interflora v. Marks & Spencer plc*, *reported in* Drew and Joseph, "ECJ judgment in Interflora: keyword advertisers beware," (Sept. 28. 2011), Lexology, (ECJ held that the use of a flower delivery network's trademark "Interflora" as a Google Adword by a competing flower delivery site infringed on Interflora's trademark *if*, among other things, the keyword advertisement did not enable reasonably well-informed and observant internet users to ascertain without difficulty whether the goods and services referenced in the advertisement originated from the owner of the trademark or an undertaking economically connected to it; the ECJ also stated that the use of keywords is capable of constituting infringement under Article 9(1)(c) of the Community Trade Mark Regulation if such use amounts "to riding on the coat-tails of a trade mark with a reputation in order to benefit from its power of attraction…without paying financial compensation."), *available at* http://www.lexology.com/library/detail.aspx?g=233957b0-94a2-434d-a07f-6ae769927b2d,

[262] For example, in November 2011 the Tribunal de Grande Instance de Paris determined that Google could not avail itself of the protections of the E-Commerce Directive in connection with Google's AdWords service because, in the court's view, the company had played an "active role" in certain privacy violations at issue. In reaching its conclusion, the court noted that the express terms and conditions of the AdWords service provided, among other things, that the positioning of advertisements is at Google's discretion, that Google reserved the right to stop publishing the sponsored link for any reason, and that Google's instructions for drafting advertisements are part of the terms of use. Portolano and De Santis, "French court finds Google has editorial control over AdWords advertising," Portolano Colella Cavallo Studio Legale (Dec. 13, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=2ed7971e-e7e4-4184-97f0-2382e6c2327f.

[263] *Google Wins A Trademark Victory – But is it Pyrrhic?*, Steptoe & Johnson, *E-Commerce Law Week* (April 3, 2010).

[264] *See Google France v. Syndicat Francais de la Literie*, Paris Cours d'App., 11/19/10 *reported in* "Citing EU

lower court decision holding that competitive keyword advertising is legitimate as long as it is not "misleading."[265] The case involved Vancouver Career College (VCC) paying internet search engines such as Google and Yahoo for ad space making use of a competitor school's names as a keyword, resulting in VCC's name appearing first when entering the competitor's name in an online search. The court ruled that VCC did not represent itself in its Internet advertisements as anyone other than who it is, and that it did not use the "names of competitors or trademarked terms in the title line, description line or URL of its online advertisements."

In 2013, in two important victories for Google, the High Court of Australia found that Google was not responsible for publishing what Australia's competition and consumer commission deemed to be deceptive ads in connection with the AdWords program.[266] In a subsequent decision, the French Cour de Cassation (its Supreme Court) found that Google was protected by the limited liability regime for hosting service providers, and that Google advertisers could use a competitor's trademark as a keyword in AdWords in the absence of a showing of likelihood of confusion.[267]

Similar trademark and copyright issues also arise in the context of unauthorized pop-up advertisements triggered by visits to an unrelated or even competitive website. A group of newspaper and website publishers sued Gator, an on-line advertising company, in mid-2002 to prevent it from placing pop-up ads over their sites.[268] The plaintiffs argued that the pop-up ads appeared to be authorized by the publisher, creating confusion and trademark and copyright infringement. Sometimes the ads were for rival services, as when Gator caused an ad for HotJobs.com to appear when a Gator user visited Dow Jones' Career Journal.com.

A similar suit by Staples against Office Depot, charging that Office Depot was using Gator software to intercept Staples advertising to its on-line customers and placing its own pop-up advertising over the Staples website, and asserting that this conduct constituted deceptive advertising, copyright infringement and trespass, was settled before it could be heard,[269] but such conduct was held not to constitute infringement by the Second Circuit in *1-800-Contacts Inc. v.*

Precedent, French Court Finds Google AdWords Did Not Infringe Trademark," 81 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 153 (Dec. 3, 2010).

[265] *Private Career Training Institutions Agency v. Vancouver College (Burnaby) Inc. d.b.a Vancouver Career College and CDI College, Vancouver College of Art and Design*, 2010 BCSC 765 *reported in* "Canadian Court Rules Internet Advertisers Can Use Names of Competitors Online," 81 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 497 (Feb. 2, 2011).

[266] *Google Inc v. Australian Competition and Consumer Commission* [2013] HCA 1 (Austl.). ("[t]he technology which lies behind the display of a sponsored link merely assembles information provided by others for the purpose of displaying advertisements directed to users of the Google search engine in their capacity as consumers of products and services." Furthermore, the High Court found that "[t]he fact that the provision of information via the internet will – because of the nature of the internet – necessarily involve a response to a request made by an internet user does not, without more, disturb the analogy between Google and other intermediaries. To the extent that it displays sponsored links, the Google search engine is only a means of communication between advertisers and consumers.").

[267] Cour de Cassation, decision of January 29, 2013, 11-21011 and 11-24713, *Cobrason v Solutions*, *available at* http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000027024140&fastReqId=405377599&fastPos=1 and *discussed at* http://www.lexology.com/library/detail.aspx?g=98567fa9-a770-49f8-8c57-72cecce502e3.

[268] B. Tedeschi, "Publishers of Websites File Suit to Stop Pop-Up Ads," N.Y. TIMES (June 28, 2002).

[269] *Staples, Inc. v. Office Depot, Inc.*, 01 Civ. 9128 (DAB) (S.D.N.Y.) (complaint).

WhenU.com Inc., following two similar district court decisions,[270] because the court determined that the use of a trademark to trigger a pop-up ad's appearance on the user's screen is not "use in commerce" actionable under the Lanham Act.

Trademark issues also arise from the sale of allegedly counterfeited merchandise online. In a widely followed case, Tiffany sued eBay for "contributory infringement" of the Tiffany trademarks stemming from eBay's assistance with and profits from the sales of counterfeit Tiffany products.[271] Because eBay retained "significant control" over the transactions consummated on its website, and because eBay derived profits from such sales, the New York district court held that eBay could be liable *if* it allowed known Tiffany infringers to continue to use its online auction site. The court noted that Tiffany specifically wrote several times to eBay to complain about the problem of the counterfeit products. Tiffany also filed thousands of Notice of Claimed Infringement forms. Nevertheless, although eBay was found to have had a "generalized knowledge" of the infringement, "such generalized knowledge is insufficient … to impose upon eBay an affirmative duty to remedy the problem."[272] Moreover, the court held that Tiffany failed to prove "willful blindness," as eBay had instituted and invested millions in certain anti-fraud measures. Finally, the court warned that the "rights holders bear the principal responsibility to police their trademarks."[273] Thus the court found eBay not liable absent specific knowledge that individual users were continuing to infringe.[274] The district court's dismissal of Tiffany's trademark infringement and dilution claims was affirmed by the Second Circuit in April 2010.[275]

This ruling stands in stark contrast with one handed down by the Commercial Court of Paris.[276] In June 2008, the French court held that eBay was "negligent" and ordered it to pay almost $61,000,000 in damages resulting from the sale of counterfeit Louis Vuitton and Christian Doir Couture products on eBay. And in 2010, the Paris Court of Appeals upheld the lower court's decision that eBay failed to take effective measures to prevent the sale of counterfeit merchandise, and declined eBay's argument that it was merely providing hosting services. The

---

[270] 414 F.3d 400 (2d Cir. 2005), *cert. denied*, 126 S.Ct. 749 (2005); *U-Haul Int'l Inc. v. WhenU.com Inc.*, 279 F. Supp. 2d 723 (E.D. Va. 2003); *see also Wells Fargo & Co. v. WhenU.com*, 293 F.Supp.2d 734 (E.D. Mich. 2003), *reported in* 67 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 63 (Nov. 28, 2003).

[271] *Tiffany (NJ) Inc. v. EBay Inc.*, No. 04 Civ. 4607, 2008 WL 2755787 (S.D.N.Y. July 14, 2008).

[272] *Id.* at *38 ("[C]ourts have been reluctant to extend contributory trademark liability to defendants where there is some uncertainty as to the extent or the nature of the infringement.").

[273] *Id.* at *47.

[274] The court likened the issue to the Supreme Court's ruling in *Inwood Laboratories Inc. v. Ives Laboratories Inc*, 456 U.S. 844, 854 (1982) ("[If a manufacturer] continues to supply its products to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer … is contributorially responsible for any harm done as a result of the deceit.").

[275] *Tiffany (NJ), Inc. v. eBay, Inc.*, No. 08-3947-cv, 2010 WL 1236315 (2d Cir. 2010) (but remanding to the district court on Tiffany's false advertising claims where eBay advertised the sale of Tiffany goods on its website (from which counterfeit merchandise was sold), including by providing links to "Tiffany," "Tiffany & Co. under $50," and "find Tiffany items at low prices;" record unclear as to whether the advertisements would mislead or confuse consumers; "A disclaimer might suffice"). On November 29, 2010, the U.S. Supreme Court denied Tiffany's petition for writ of certiorari.

[276] General Docket Nº. 2006077799, 2006077807. In November 2009, the court ruled that eBay had failed to comply with its prior order, which required that eBay stop its users' sale of the plaintiffs' products and those items purporting to be the plaintiffs' products, and imposed a fine of €1.7 million. Notably, the court held that eBay's hiring of over 85 people to monitor its users was insufficient. *Reported in* 65 INTA Bulletin No. 3 (Feb. 1, 2010) at 9.

Court of Appeals did, however, reduce the damages award to $7,300,000.[277] The court reasoned that eBay assisted sellers in defining products and suggested ways to improve their visibility with the aim of promoting a transaction, thereby acting as a broker and not a passive hosting service provider.[278] Consequently, a mere "generalized" knowledge or nominally active involvement may be enough to state a claim in France. Similarly, a German court recently ruled that companies like eBay must take more active measures to block offers by third parties after being advised of obvious trademark infringement and must also take reasonable action to avoid future infringement.[279] On the other hand, in May 2009, the British High Court of Justice ruled that eBay was not liable for infringement stemming from counterfeit products sold by users of its website.[280] It is clear that international differences exist in addressing the issue.

With respect to infringing domain names themselves, the Internet Corporation for Assigned Names and Numbers ("ICANN") has adopted a Uniform Domain Name Dispute Resolution Policy ("UDRP") based on World Intellectual Property Organization ("WIPO") recommendations.[281] The policy provides for arbitration of disputes before WIPO or additional dispute resolution service providers. It requires registrants of domain names to represent that to their knowledge the domain name registration will not infringe or violate the rights of any third party and the registration is not for an unlawful purpose and will not knowingly be used in violation of applicable law. Under the policy, a registration will be canceled only upon authorization by the registrant, or upon receipt of a court order or arbitration panel order under the policy. Arbitration is mandatory for claims that a domain name is identical or confusingly similar to a trademark or service mark of the complainant, that the registrant has no rights or legitimate interests in the domain name, or the domain name has been registered and is being used in bad faith. Such arbitration has recently been determined not to be binding upon a federal court.[282]

Among the circumstances that constitute evidence of bad faith are registration primarily to sell, rent or transfer the domain name to the trademark owner or a competitor for valuable consideration; registration to prevent the trademark owner from reflecting its mark in a corresponding domain name; registration primarily to disrupt a competitor's business; and use of the domain name to attempt intentionally to attract users to a site for commercial gain by creating likelihood of confusion with the complainant's mark. On the other hand, use or preparations for use of the domain name for a bona fide offering of goods or services before any notice of the dispute; having been commonly known by the domain name; or the legitimate noncommercial or

---

[277] *See* Brush, "French Court Cuts Damages EBay Must Pay LVMH" Law 360 (September 3, 2010), *available at* http://www.law360.com/web/articles/191531 (subscription required).

[278] *eBay Inc. and eBay AG v. Louis Vuitton Malletier; eBay Inc. and eBay AG v. Parfums Christian Dior; eBay Inc. and eBay AG v. Christian Dior Couture (CA Paris, March 9, 2010, reported in* Bruneau, "Paris Appeals Court Confirms eBay's Liability for Selling Counterfeit and Unauthorized LVMH Perfumes on Auction Website" Lexology (November 20, 2010).
See Brush, "French Court Cuts Damages EBay Must Pay LVMH" Law 360 (September 3, 2010).

[279] *ricardo.de Aktiengesellschaft v. Rolex, S.A.*, I ZR 73/05 (Federal Court of Justice) (April 30, 2008) (holding that providers are obligated to make feasible and reasonable inspection efforts).

[280] *L'Oréa S.A. and others v. eBay Int'l A.G. and others*, [2009] EWHC 1094 (Ch), Arnold J, 22 May 2009 (holding that eBay had no legal duty to prevent infringement conducted by its users).

[281] The policy is available at http://www.icann.org/udrp/udrp.htm.

[282] *Weber – Stephen Products Co. v. Armitage Hardware and Building Supply Inc.*, 2000 WL 562470, 54 U.S.P.Q.2d (BNA) 1766 (N.D. Ill. 2000); *Sallen d/b/a J.D.S. Enterprises v. Corinthians Licenciamentos LTDA*, 273 F.3d14 (1st Cir. 2001) *reported in* WORLD INTERNET L. REP. (BNA) (Jan. 2002).

fair use of the domain name all serve to demonstrate a legitimate interest in the domain name.[283] The case law is mixed where "sucks" has been appended to a trademark, with some courts and arbitrators finding bad faith and others upholding the right to use such sites for legitimate criticism.[284]

Congress addressed the same problem of bad faith domain name registrations with the enactment of the Anticybersquatting Consumer Protection Act (the "ACPA").[285] This statute amends Section 43 of the Lanham Act,[286] to create a cause of action for trademark owners against those who have a bad faith intent to profit from the mark and register, traffic in or use a domain name that is (i) identical or confusingly similar to a distinctive mark[287] or (ii) identical or confusingly similar to, or dilutive of, a famous mark or (iii) is a mark protected by specified statutes, such as "Olympic" and "Red Cross."[288] Under the new law, a court may order the forfeiture, cancellation or transfer of the domain name, injunctive relief, actual damages, or statutory damages of $1,000 to $100,000 per domain name, as the court deems just.[289] The new statute also permits an *in rem* action by a trademark owner against a domain name, where the owner cannot obtain *in personam* jurisdiction over or cannot find the person who otherwise would have been a defendant under the statute.[290]

Like the ICANN dispute resolution policy, the ACPA establishes a number of non-exclusive factors that a court may consider. Factors suggesting bad faith include the person's intent to divert customers from the mark owner's site to a site under the domain name that could harm the mark's goodwill, either for commercial gain or with an intent to tarnish or disparage the mark by creating a likelihood of confusion; the person's offer to transfer sell or assign the domain name to the owner or a third party for financial gain without having used it or having an

---

[283] *See Toyota Motor Sales U.S.A. Inc. v. Tabari*, 9th Cir., No. 07-55344 (7/8/10) (holding that auto brokerage service was entitled to use the "Lexus" mark in its domain name, since use of the trademark was limited to refer to the trademarked goods and was found to be truthful, non-misleading speech, and the domain name did not actively suggest sponsorship or endorsement such that there would be no likelihood of confusion) *reported in* 80 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 336 (July 16, 2010).

[284] *Compare Koninklijke Philips Electronics N.V. v. Kim*, No. D2001-1195 (WIPO Arbitration & Mediation Center, Nov. 12, 2001) (UDRP protects against abusive registrations; domain name "philipssucks.com" was confusingly similar to the complainant's registered trademark "Philips") *reported in* WORLD INTERNET L. REP. (BNA) (Jan. 2002), at 26; and *Standard Chartered PLC v. Purge I.T.*, No. D2000-0681 (WIPO August 30, 2000) (finding bad faith in registering "sucks" sites for purposes of selling domain name to trademark owners, and finding likely confusion); *with Bally Total Fitness Holding Corp. v. Faber*, 29 F. Supp. 2d 1161 (C.D. Cal. 1998) (Bally Sucks website not likely to be confused with Bally's official site); *Lucent Technologies, Inc. v. Lucentsucks.com*, 95 F. Supp. 2d 528 (E.D. Va. 2000) (parody or criticism of a company undermines finding bad faith); *Wal-Mart Stores, Inc. v. Walmartcanadasucks.com*, No. D 2000-1104 (WIPO Nov. 23, 2000) (finding "sucks" websites are not confusingly similar and there is privilege for parody and criticism).

[285] Enacted Title III of the Intellectual Property and Communications Omnibus Reform Act of 1999, Pub. L. No. 106-113 (1999).

[286] 15 U.S.C. 1125.

[287] This test, which calls for a simple comparison of the domain name and the mark, was distinguished from the more comprehensive "likelihood of confusion" test for trademark infringement in *Northern Light Technology Inc. v. Northern Lights Club*, 97 F. Supp. 2d 96 (D. Mass. 2000).

[288] 15 U.S.C. § 1125(d)(1)(A).

[289] 15 U.S.C. §§ 1125(d)(1)(C), 1116(a), 1117(a), (d). *See, e.g., Sporty's Farm L.L.C. v. Sportsman's Market, Inc.*, 202 F.3d 489 (2d Cir. Feb. 2, 2000), *cert. denied*, 530 U.S. 1262 (June 26, 2000).

[290] An attempt to obtain a temporary restraining order against the register that issued a disputed domain name was dismissed on jurisdictional grounds, the court suggesting instead on *in rem* claim under the ACPA. *American Girl LLC v. Nameview Inc.*, 381 F.Supp.2d 876 (E.D. Wis. 2005), *available at* http://pub.bna.com/ptcj/050814Aug9.pdf.

intent to use it for the bona fide offering of goods or services; the person's provision of false or misleading contact information when registering the domain name, or intentional failure to maintain accurate contact information; and the person's registration or acquisition of multiple domain names which the person knows to be identical or confusingly similar to other marks of third persons.[291] Factors militating against bad faith include the person's trademark or other intellectual property rights in the domain name; the extent to which the domain name is the legal name of, or a name commonly used to identify the person; the person's prior use of the domain name for the bona fide offering of goods or services; and the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name.[292] Bad faith is not to be found where the person is found to have believed, with reasonable basis, that the use of the domain name was a fair use or otherwise lawful.[293] One district court has found the failure to perform a trademark search before registering a domain name suggests bad faith.[294]

The ACPA has already been applied in several notable cases. The Southern District of New York applied the in rem provisions of the Act to gain jurisdiction over a defendant who was found to have registered a domain name associated with the plaintiff's business in bad faith.[295] The court ordered the transfer of the domain name to the plaintiff.[296] The Fourth Circuit has held the in rem provisions could be used to gain jurisdiction in Virginia over domain names registered there in bad faith for purposes of trademark infringement and dilution claims as well as for the bad faith registration.[297] And the Ninth Circuit has held that an employee's intent to profit from a domain name by re-directing business to a different place demonstrated bad faith under the ACPA, regardless of the allegations of the employee that he was trying to recoup monies owed from his employer.[298]

Many domain name conflicts do not involve the bad faith that is a prerequisite to success under the ACPA or the ICANN Uniform Dispute Resolution Policy. A federal court in California recently issued a compromise of sorts with regard to confusingly similar names, requiring the owner of www.nissan.com, a computer-related website (Mr. Nissan) to display a prominent caption indicating that the website was not affiliated with the car manufacturer of the same name and providing the website address of the car manufacturer.[299]

Individual U.S. states may also be entering the fray, as evidenced by the Utah Senate Committee on Transportation, Public Utilities and Technology's recent approval of a bill (S.B. 26) prohibiting cybersquatting. The Utah E-Commerce Integrity Act – which if enacted would become the first state anti-cybersquatting law in the United States – would differ from the federal law in key ways, including by (i) protecting personal names, (ii) providing the owner of a mark

---

[291] *See*, *Reg Vardy PLC v. Wilkinson*, (Case No. D 2001-0593) WIPO Arb. and Med. Center (July 3, 2001) (disgruntled customer with intent to disrupt business had no right to domain name of business).

[292] 15 U.S.C. § 1125(d)(1)(B)(i). *See, e.g.*, Robin Kitzes Silk, "The Cybersquatting of Law Firm Domain Names: Think Before You Squat", 55 INTA Bulletin 11 (6/15/2000) p. 6 (injunction against bad faith registration of domain names incorporating law firm name).

[293] 15 U.S.C. § 1125(d)(1)(B)(ii).

[294] *Eurotech, Inc. v. Cosmos European Travels AG*, No. 01-1689-A (E.D. Va. July 23, 2002), *reported in* PATENT, TRADEMARK & COPYRIGHT J. (BNA) 356 (Aug. 9, 2002).

[295] *Broadbridge Media LLC v. Hypercd.com*, 106 F.Supp.2d 505 (S.D.N.Y. 2000).

[296] *Id*.

[297] *Harrods Ltd. v. Sixty Internet Domain Names*, 302 F.3d 214 (4th Cir. 2002).

[298] *DSPT International Inc. v. Nahum*, 2010 WL 4227883 (9th Cir., Oct. 27, 2010), *reported in* "First Sale, 'Scraping,' Applying Anti-Cybersquatting Act," New York Law Journal (Volume 244-No. 92, November 10, 2010).

[299] *Nissan Motor Co., Ltd. et al. v. Nissan Computer Corp.*, 89 F. Supp. 2d 1154 (C.D. Ca. 2000).

registered with the Patent and Trademark Office (or with the state of Utah) with the opportunity to file certain *in rem* civil actions, and (iii) exempting domain name registries from legal action, except in cases of bad faith or reckless disregard.[300] Under the bill, cybersquatters could be liable for any infringing activities without regard to the duration of infringement.

A separate issue arises where, rather than a trademark, the domain name is descriptive of services offered at the site. In one case, a German court held that where the owner of the domain name did not have a monopoly on the services offered, there was a possibility of unfair competition and the registrant was prohibited from using such a domain name unless they added a non-descriptive suffix.[301]

As a final note, at least one court has held that plaintiffs may not assert a trademark infringement claim under the Lanham Act for violations of privacy and reputation, absent commercialization of the plaintiff's identity. In *Stayart v. Yahoo! Inc.*[302], the plaintiff entered her name into the search engines provided by Yahoo! and other sites. The search results contained links to various pornographic and sexual dysfunction drug websites, among other things. When Yahoo! refused to take down the links in response to the plaintiff's requests, she sued Yahoo! and the other service providers for "false endorsement" under the Lanham Act.[303] The court held that the plaintiff could not state a false endorsement claim because she did not allege that she had made any attempt to "commercially market" her identity, finding that "Congress has not evinced an intent to create a federal 'false light' tort claim for misappropriation of image or identity, absent commercialization."[304] Moreover, because the plaintiff and her social circle found the material in the search results "perverse and abhorrent," the court held that no one who accessed the links could reasonably conclude that the plaintiff endorsed the products at issue. Consequently, there was no likelihood of confusion. Perhaps in anticipation of claims like these, Google has introduced a feature called "Google profile" which users can create so that personal information edited by the users appears on the first page of results of a U.S. name-query.[305]

G. *Regulation of Spam*

Regulation of spam, or unsolicited commercial e-mail, also raises choice of law and jurisdictional issues, because spam is often sent from one jurisdiction to another, and often routed through computers in still other jurisdictions.

In 2003, the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act (the CAN-SPAM Act) was signed into law.[306] This Act requires unsolicited commercial e-

---

[300] *See* 79 PATENT, TRADEMARK & COPYRIGHT J. 1953 (BNA) (Feb. 12, 2010) at 426.

[301] *Verein der Mitwohnzentralen v. Die Mitwohnzentrale et al.* (Hamburg, 1999), *reported in* WORLD INTERNET L. REP. (BNA) (3/00) (flat sharing agency's domain name was descriptive and therefore unfairly attracted internet users away from competitors).

[302] 651 F. Supp. 2d 873 (E.D. Wis. 2009).

[303] 15 U.S.C. § 1125(a).

[304] 651 F. Supp. 2d at 882.

[305] *Reported in* http:///www.time.com/time/business/article/0,8599,1893965,00.html?xid=rss=topstores. Profile page *available at* http://www.google.com/profiles/me/editprofile?#about.

[306] 15 U.S.C §§ 7701-7713 (2003). An FTC summary of the Act's requirements is available at http://www.ftc.gov/bap/conline/pubs/buspubs/canspam.htm. The FTC has issued regulations determining what constitutes commercial e-mail subject to the CAMSpam Act. 16 CFR Part 316.

mail messages to be labeled (though not by a standard method)[307] and to include opt-out instructions, as well as the sender's physical address.[308] Sending e-mail to a recipient who has requested (via such an opt-out mechanism) that it not be sent is prohibited, as are the use of deceptive subject lines and false headers in such messages. Automated harvesting of e-mail address from websites and so-called "dictionary" attacks, using automatically generated addresses, are prohibited, along with automated creation of multiple e-mail accounts and unauthorized use of computers to relay commercial e-mail. Bulk commercial e-mail sent through protected computers, and falsified headers and fraudulent registration for multiple e-mail accounts used for such e-mail, are criminalized. Businesses knowingly promoted by unlawful commercial e-mail are covered by the law, even if they do not themselves send the e-mail. The FTC was authorized, but not required, to establish a "do-not-e-mail" registry, and it has opposed the creation of such a registry.[309]

The FTC and states need not prove knowledge to obtain cease and desist orders or injunctive relief under CAN-SPAM, and also may seek monetary relief. Actions by internet service providers adversely affected by violations of the Act are also authorized. Criminal penalties are available, and sentencing guidelines treat spam offenses similarly to fraud, theft and destruction of property.[310] Enforcement efforts under the Act began promptly, as internet service providers sued major senders of spam,[311] the FTC began criminal actions,[312] and state enforcement efforts were initiated.[313] In 2007, however, the Western District of Washington rejected a claim by a spam recipient, saying recipients lacked standing under CAN-SPAM because they had not been adversely affected within the meaning of the Act by suffering network

---

[307] Sexually oriented e-mail must be labeled in the manner to be required by the FTC, and may not display sexually oriented material in the screen initially seen by the recipient. An FTC Report in June 2005 said that such labeling would not materially help to reduce or block spam. *See* http://ftc.gov/reports/canspam05/050616canspamrpt.pdf.

[308] The FTC announced new CAN-SPAM rules on May 12, 2008, which clarify that where a single email contains messages from multiple parties but only one sender is identified in the "from" line, that sender will be solely responsible for administering opt-out requests. Moreover, the new rules provide that a person requesting an opt-out may not be made to pay a fee or provide information other than an email address. The new rules became effective on July 7, 2008. *See FTC Adopts Final CAN-SPAM Rules*, Steptoe & Johnson, *E-Commerce Law Week* (May 22, 2008), *available at* http://www.steptoe.com/publications-5331.html.

[309] In a June 15, 2004 report to Congress, the FTC asserted that such a registry could not be effectively enforced, and might risk an increase in spam if spammers were able to get access to the registry and use it as a source of valid email addresses. Instead the FTC urged efforts to develop an email authorization system that would help identify spammers and make it more difficult for them to evade spam filters and law enforcement efforts. "National Do Not Email Registry: A Report to Congress," http://www.ftc.gov/reports/dneregistry/reports.pdf.

[310] P. Festan, "Stiff Spam Penalties Urged," CNETnews.com, http://news.cnet.com/Stiff-spam-penalties-urged/2100-1028_3-5191651.html?tag=mncol;1n (April 14, 2004).

[311] S. Hansell, "Internet Providers Sue Hundreds Over Unsolicited E-Mail, N.Y.Times, Mar. 10, 2004, *available at* http://web.mit.edu/21w.784/www/BD%20Supplementals/Materials/Unit%20Two/Spam/spam%20suits%20NYT.html.

[312] "FTC Announces First Can-Spam Cases," http://www.ftc.gov/opa/2004/04/040429canspam.htm; *FTC v. Phoenix Avatar, LLC*, TRADE CAS. (CCH) ¶ 24,507; *see Spam and Phishing – a matter for privacy regulations or law enforcement?*, WORLD DATA PROTECTION REPORT 11 (BNA) (Jan. 1, 2008) (reporting that the FTC has brought over 90 law enforcement actions against spam offenders, but warning that spammers now use sophisticated illegal hacking and harvesting techniques to overwhelm the FTC's capacity to effectively deal with the problem).

[313] "AG Reilly Sues Deceptive Spammers for Violating Massachusetts Law, Federal Can Spam Act," http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1257 (July 1, 2004).

or bandwidth slowdowns, demands on personnel or need for new equipment. The Court ordered the plaintiff to pay over $100,000 in legal fees to the defendant.[314]

Among the more controversial provisions of the CAN-SPAM Act is Section 5(b), which preempts all state laws that expressly regulate commercial e-mail, except to the extent that they prohibit falsity or deception.[315] (State laws not specific to e-mail are unaffected). This provision wipes out tougher anti-spam laws enacted in many states, such as California's anti-spam statute, which resulted in a $2 million judgment against a spammer less than two months before CAN-SPAM was enacted.[316] But state laws that are not preempted are often actively enforced, as evidenced by the nine year prison term imposed by Virginia on a North Carolina spammer who violated Virginia law prohibiting falsified header information in violation of an ISP's policies if more than specified numbers of messages were sent within a certain period.[317] (As discussed below, this Virginia law has since been invalidated, pending appeal.) New York convicted the notorious "Buffalo spammer" on forgery, identity theft and other charges.[318]

As of CAN-SPAM's enactment, at least 35 states had enacted laws regulating spam.[319] The statutes vary in nature. Often they required an indication in the subject line that the e-mail contains advertising, usually by requiring that the subject line begin with "ADV" or "ADV:ADULT," required a method for opting out of further messages, and prohibited falsified routing information and false or deceptive subject lines.[320]

Other state laws went much further. Delaware made it criminal to send unsolicited bulk commercial e-mail to recipients located in Delaware with whom the sender had no pre-existing business relationship if the sender knew the recipient's presence in the state to be a reasonable

---

314 *Gordon v. Virtumundo*, 2007 WL 2253296 (W.D. Wash. 2007).

315 For example, a Washington state law creating a civil right of action against those sending commercial emails with false header information or misleading subject lines was not preempted by the CAN-SPAM Act. *Gordon v. Impulse Marketing Group, Inc.*, 375 F.Supp.2d 140 (E.D. Wash. 2005), *reported in* INTERNET LAW NEWS (BNA) (July 28, 2005). On the other hand, a federal district court concluded that Michigan's anti-spam law, which prohibited commercial e-mails that misrepresent information concerning the transmission path of the message, was preempted because the misrepresented information did not rise to the level of *material* falsity or deception. *Hafke v. Rossdale Group, LLC*, 11-cv-22-0 (W.D.Mich. Oct. 7, 2011), *reported in* "CAN-SPAM Preempts Claims Under Michigan Anti-Spam Law," Steptoe & Johnson LLP (Issue 681 Nov. 5, 2011), *available at* http://www.steptoe.com/publications-7871.html. The FTC has obtained injunctive relief against companies that failed to comply. *FTC v. Global Net Solutions, Inc.*, No. CV-S-05-0002 – PMP-LRL (D. Nev 2005), *reported in* WORLD INTERNET L. REP. p. 25 (January 2005); Associated Press, "F.T.C. Files First Legal Case Against Sexually Explicit Spam," N.Y. TIMES, Jan. 12, 2005, *available at* http://www.nytimes.com/2005/01/12/technology/12porn.html; *See also Hypertouch v. ValueClick*, 2011 WL 454789 (holding that California's Anti-Spam Law regulating commercial e-mail is not preempted by the CAN-SPAM Act because it prohibits "falsity and deception").

316 "Attorney General Lockyer wins First-Ever Lawsuit Against Spammer," Cal. Atty. Gen'l Press Release (Oct. 24, 2003), http://oag.ca.gov/news/press_release?id=1152&y=2003.

317 "North Carolina Man Sentenced to 9 Years for Spam," *available at* http://news.cnet.com/2100-1024_3-5438340.html (Nov. 3, 2004).

318 "Man Convicted in Spam Case, "N.Y. TIMES (Apr. 2, 2004), p. C4.

319 *See e.g.*, Cal. Bus. Profs. Code §17538.4; Colo. Rev. Stat. §6-2.5-101; Idaho Code §48-603E; 815 Ill. Comp. Stat. 511; Iowa Code §§714E.1-.2; Nev. Rev. Stat. Ann. §§41.705-.735; R.I. Gen. Laws, §11-52-1; Tenn. Code Ann. §§47-18-1602, -2501; Va. Code §§ 18.2-152.2, -152.3:1, 152.4, -152.12 and -152.16; Wash. Rev. Code, tit. 19, Chap. 19.190.

320 *E.g.* Tex. Stat., tit. 4, §46,003.

possibility, or to fail promptly to stop sending unsolicited commercial e-mail after being requested to do so.[321]

The Virginia law referred to above made the sending of unsolicited bulk e-mail with falsified header information in violation of an ISP's policies a felony if more than specified numbers of messages were sent in any given 24-hour, 30-day or one-year period.[322] On September 12, 2008, the Supreme Court of Virginia struck down the state's anti-spam law as violative of the First Amendment right to freedom of speech.[323] In so holding, the court found that the law did not limit its restrictions to commercial or fraudulent spam. Rather, the law was drawn too widely and was found to infringe upon forms of lawful speech. Virginia's Attorney General Robert F. McDonnell has promised an appeal of the decision.

Other features of various state laws, now largely preempted, included:

- A prohibition on deceptive subject lines designed to evade spam-altering software.
- A prohibition on sending e-mail in violation of an ISP's policies.
- A requirement that the sender be identified, often with a physical address or telephone number.
- A requirement for a functioning reply feature.
- A requirement for an opt-out method that is honored.

Some state laws provided a private right of action for violations, with statutory penalties per violation, leading to claims ranging from one for $80 against Elizabeth Dole's North Carolina Senate campaign for eight violations of that state's anti-spam law[324] to one by law firm Morrison & Foerster against Etracks, an e-mail marketing company, for $50 per e-mail received, up to $25,000 per day, for 6,500 unsolicited e-mails received by its employees in violation of California anti-spam laws.[325] The 2004 Maryland Spam Deterrence Act imposes criminal penalties, with fines of up to $25,000, asset forfeiture and prison terms of up ten years.[326]

Summaries and the full text of state spam laws can be found at http://www.spamlaws.com/state/index.html.

In addition, ISPs have successfully sued spammers under state laws not specifically directed at e-mail, which remain valid after CAN-SPAM. For example, Virginia's Computer Crimes Act provides that "[a]ny person who uses a computer or computer network without authority and with the intent to [c]onvert the property of another shall be guilty of the crime of computer fraud" and authorizes a private right of action for violations.[327] AOL has successfully claimed that sending spam with "aol.com" headers through AOL's computer network was unauthorized, that the spammers intended to obtain services by false pretenses, obtained the unauthorized service of AOL's mail system, and obtained free advertising from AOL by shifting the cost of the e-mails to

---

321 Del. Code Ann., tit. 11, §§937, 938.
322 Va. Code §18.2:152.3:1.
323 *Jaynes v. Commonwealth of Virginia*, 276 Va. 443 (2008).
324 *See* http://www.cbsnews.com/stories/2002/10/09/national/main524957.shtml.
325 *See* http://www.siliconvalley.com/mld/siliconvalley/news/local/2861505.html.
326 Maryland SB604, signed into law May 26, 2004.
327 Va. Code § 18.2-152.3(3), -152.12

AOL, and that therefore the Virginia statute had been violated.[328] (Similar actions had also been brought successfully under the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.* (the "CFAA"), which provides for civil liability if one "intentionally accesses a protected computer[329] without authorization, and as a result of such conduct, causes damage …."[330] The CFAA also provides for *criminal* liability under certain circumstances.[331] And SMS text messages

---

[328] *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 D. (E.D. Va. 1998).

[329] In a case involving a sex offender's sentencing, the Eighth Circuit suggested that even a basic cell phone that cannot connect to the Internet could be a computer under the CFAA. *United States v. Kramer*, 631 F.3d 900 (February 8, 2011), *reported in* "Break the Coffeemaker, Go to Jail," Steptoe & Johnson LLP E-Commerce Law Week (Issue 646, Week Ending March 5, 2011), *available at http://www.steptoe.com/publications-7460.html*.

[330] 18 U.S.C. § 1030. *See, e.g., Craigslist Inc. v. 3Taps Inc.*, 942 F.Supp.2d 962 (N.D. Cal. 2013) (in an action alleging improper use of user-generated content, defendants' motion to dismiss was denied as to plaintiff's CFAA claim since the court held that "[plaintiff's] trespass claim adequately alleged injury" and "[d]efendants' continued use of [plaintiff's website] after the clear statements regarding authorization in the cease and desist letters and the technological measures to block them constitute[d] unauthorized access under the [CFAA]."); *Hotmail Corp. v. Van$ Money Pie Inc.*, 47 U.S.P.Q. 2d 1021, 1023-24 (N.D. Cal 1998) (use by spammers of falsified return addresses using ISP's domain resulted in customer complaints, replies and "bounced back" messages being sent to the ISP rather than to the spammer, causing harm to the ISP's computer system and online service and violated Computer Fraud and Abuse Act); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 450-451 (E.D. Va. 1998) (maintaining an account with ISP and extracting e-mail addresses from other ISP customers in violation of ISP's terms of service amounted to unauthorized access and obtaining of information from a protected computer, resulting in damages to the ISP, and so violated the Computer Fraud and Abuse Act). *See also P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore, LLC*, 428 F.3d 504, (3d Cir. 2005) (civil remedy available under CFAA where unauthorized access to computers causes damage or something of value is taken); *Mobile Mark, Inc. v. Paskosz*, No. 11-cv-2983 (N.D.Ill. 2011) (the cost of a business's investigation into an employee's alleged misconduct, and related lost sales opportunities, could be counted as losses for the purposes of the CFAA's $5,000 damages threshold for maintaining an action), *reported in* "Court Allows Recovery of Lost Business Investigation Costs Under CFAA," Steptoe & Johnson LLP E-Commerce Law Week (Issue 673, Sept. 10, 2011), *available at* http://www.steptoe.com/publications-7783.html. *But see Civic Center Motors, Ltd. v. Mason Street Import Cars, Ltd.* 387 F .Supp. 2d 378 (S.D.N.Y. 2005) (losses compensable under CFAA only if there is damage to computer system); *Garelli Wong & Assocs. v. Nichols*, 551 F. Supp.2d 704 (N.D. Ill. 2008) (CFAA plaintiffs must allege "damage," which involves the deletion or manipulation of information in a database); *Mintel Int'l Group, Ltd. v. Neergheen*, No. 08-cv-3939, 2010 WL 145786, *9-10 (N.D. Ill. 2010) ("copying, e-mailing or printing electronic files from a computer database is not enough to satisfy the damage requirement of the CFAA. Rather, there must be destruction or impairment to the integrity of the underlying data…. [Moreover], [b]ecause Mintel has not demonstrated that it suffered costs related to damage to its computer or that it suffered any service interruptions, it has failed to show any loss redressable under the CFAA."); *Costar Realty Information, Inc. v. Field*, 2010 WL 3369349*14 (D. Md., Aug. 23, 2010) (where the plaintiff made the fatal error of simply alleging lost profits as the basis for the $5,000 loss, which is only deemed to be a valid loss under the CFAA when the lost profits are incurred because of interruption of service); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (citing *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) but adopting "a narrow reading of the terms 'without authorization' and 'exceeds authorized access'" since the Court in *WEC* found that these terms apply "only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access"); *Cvent Inc. v. Eventbrite Inc.*, E.D. Va., No. 1:10-cv-481 (LMB/IDD, 9/15/10) *reported in* "`Scraping' of Website Data by Competitor Does Not Support Computer Crimes Claims," 80 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 734 (Oct. 1, 2010) (holding that there was no reasonable allegation that competitor had 'scraped' information without authorization in violation of the CFAA, since plaintiff's website's terms of use were buried in fine print and data was not subject to password protection or any other kind of access control); *compare Global Policy Partners, LLC v. Yessin*, No. 1:09cv859, 2010 WL 675241, *6 (E.D. Va. 2010) (where husband had allegedly accessed and intercepted wife's business e-mail account without authorization, issue of material fact existed as to whether costs incurred by wife in order to re-secure the system against access by husband was a "qualifying cost" under the CFAA).

[331] For instance, subsection (a)(4) of the CFAA subjects to criminal liability anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means

sent to cell phones have been found to be subject to the Telephone Consumer Protection Act, just like unsolicited faxes.[332] And just two days after CAN-SPAM was signed into law, the New York Attorney General announced suits against spammers under state fraud laws.[333]

Other nations are at various points along the road to regulation of spam. In North America, Canada passed the Fighting Internet and Wireless Spam Act (FISA) in 2010, which creates a comprehensive regulatory regime of offenses, enforcement mechanisms, and severe penalties covering all forms of electronic communication and designed to protect individuals and businesses engaged in electronic commerce.[334] The Canadian legislation, which comes into force in mid-2012, provides that entities sending commercial e-messages must obtain implied or express consent from the recipients before sending such messages, and carries non-compliance penalties up to C$10 million per violation.[335] In Asia, Japan enacted legislation in 2001 requiring labeling of unsolicited advertising and instructions on how to reject future messages and prohibiting the sending of large quantities of e-mail to non-existent addresses,[336] and strengthened the law in 2005 to cover spam directed to business email accounts, prohibiting false sender information and increasing penalties.[337] South Korea apparently requires labeling of spam in the subject line and a toll-free telephone number for spam recipients to opt out of further e-mails.[338] Australia adopted anti-spam legislation in December 2003 that requires recipient consent,

---

of such conduct furthers the intended fraud and obtains anything of value." However, the 9th Circuit Court of Appeals has held that an employee is not subject to criminal liability under the CFAA for violating an employer's computer usage policy – even when the employer's electronically-stored data are purposely misappropriated for the benefit of the employer's competitor. *See Nosal*, 676 F.3d at 854 (reasoning that a criminal CFAA violation is based upon the unauthorized *access* to (or alteration of) the computer or file, and not whether the employee misuses or misappropriates such computer or file); *see also Walsh v. Bishop Assocs., Inc. v. O'Brien*, No. 11-2673, 2012 WL 669069 (D. Minn. 2012) (holding that a defendant's CFAA civil liability is not based upon the use of electronic information, rather access to it); *but see, Guest-Tek Interactive Entertainment Inc. v. Pullen*, 665 F.Supp.2d 42 (D. Mass. 2009) (employee's copying of employer's files in planning a competitive business extinguished his authorized access under the CFAA); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (employee's use and abuse of employer's proprietary information exceeded employee's authorized access in violation of the CFAA).

[332] *Joffe v. Acacia Mortgage Corp*., 121 P.3d 831(Ariz. Ct. App. 2005), *available at* http://www.cofad1.state.az.us/opinionfiles/cv/cv020701.pdf.

[333] S. Hansell, "New York and Microsoft File Suits on E-Mail Spam," N.Y. TIMES (Dec. 19, 2003), http://www.nytimes.com/2003/12/19/technology/19spam.html.

[334] *Bill C-28.* Notable components of FISA include (i) a prohibition on sending commercial electronic messages unless the recipient has consented, whether expressly or implied, (ii) mandatory inclusion of information on commercial electronic messages, including information on how to unsubscribe, (iii) anti-malware provisions designed to prevent unauthorized use of another's computer system and (iv) fines for non-compliance of up to $1 million for individuals and $10 million for corporations.

[335] "Canada to Impose Stringent Limits on Commercial Electronic Messages," Steptoe & Johnson LLP E-Commerce Law Week (Issue 689, Jan. 7, 2012), *available at* http://www.steptoe.com/publications-7952.html. The regulations contain certain limited exceptions applicable to, among other things, e-messages sent between individuals who have a "family relationship" or "personal relationship" (defined as individuals that have met in a non-business context and exchanged communications with each other within the previous two years). Davenport and Setrakian, "Proposed Canadian Anti-Spam Regulations," Norton Rose (Aug. 8, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=b11903f8-aadc-466d-9ea0-a6a5baf54bb7.

[336] *See* "New Japanese Anti-Spam Rules," WORLD INTERNET L. REP. (BNA) (Mar. 2002).

[337] "Japan Strengthens Anti-Spam Law," WORLD INTERNET L. REP. (BNA) (July 2005)

[338] National Office for the Information Economy (Australia), "Spam: Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered" (April 2003) (hereafter "*Australian NOIE Report*"), Attachment C at p. 41 (noting source of South Korean information was a media release and questioning re liability of translation).

identification of the sender, and an opt-out mechanism.[339] Europe has perhaps the most developed set of anti-spam legislation, both on the EC level and in individual nations. The EC Directive on Privacy and Electronic Communications prohibits unsolicited e-mail without the consent of the recipient unless the sender has an existing commercial relationship with the recipient.[340] It also requires opt-out methods where prior relationships do exist, prohibits disguising or concealing the sender's identity, and requires a valid address for opt-out requests.[341] The EC Directive has been a useful tool in combating viral marketing.[342] (The Directive required implementing legislation in each Member State, but as of the summer of 2004, most had not done so, including Germany, France, Belgium and the Netherlands.[343])

Legislation requiring recipient opt-in before unsolicited commercial e-mail may be sent has been enacted in Austria, Denmark, Finland, France, Greece, Hungary, Italy, Norway, Poland, Slovenia Spain and the United Kingdom,[344] and is being considered in other countries. A Swiss Court held spam to be unfair competition and a deceptive practice, unless it is labeled as commercial, limited in number, offers an effective opt-out mechanism, and does not falsify its

---

[339] The Spam Act 2003, *reported in* Bayside Bulletin (Apr. 16, 2004), http://redland.yourguide.au. Further information available at http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf.

[340] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Recitals 40-43, Art. 13, *available at* http://www.dataprotection.ie/viewtxt.asp?m=&fn=/documents/legal/Directive2002_58.pdf. *See also* Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the internal market (Directive on electronic commerce), Recitals 30, 31, Art. 7 (unsolicited commercial e-mail should be clearly identifiable as such and should not increase recipient's costs; Member States permitting unsolicited commercial e-mail without prior consent must ensure senders regularly check opt-out registers by which individuals may register not to receive such e-mails), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.

[341] In Germany, for example, the German Supreme Court held that a "double opt-in" process (where a person clicks on a website once to indicate he or she wants to receive marketing and clicks again in a follow-up email to confirm that he or she wants to receive marketing) was not a foolproof way to ensure that the person who initially supplied information was the same person who was ultimately called. The fact that the double opt-in procedure used was insufficient assurance of indentity should cause companies that operate in Germany to re-evaluate their procedures for obtaining consent to marketing. "Germany Raises the Bar for 'Consent'," Steptoe & Johnson LLP E-Commerce Law Week (Issue 646, Week Ending March 5, 2011), *available at* http://www.steptoe.com/publications-7460.html.

[342] In the UK, for example, a company promoting its film, 'Stitch Up Mate', engaged in a marketing e-mail campaign where recipients were informed that they were at risk of criminal prosecution in a drugs operation. The subject of the email read 'CRIMINAL INVESTIGATION', and the email stated that a subject who had been arrested in the drugs operation gave the recipient's name as a 'habitual narcotics user'. The recipient was invited to click on a link to a website if they felt that the information had been wrongly supplied or wished to appeal against the notice, upon which the recipient would receive a message stating "You have just been stitched up by your friend." The UK Advertising Standards Authority found that the campaign breached the EC Directive and other data protection legislation, citing that, among other things, the company should have ensured that the recipient consented to receive the email. *See* "Adjudication against 'shifty' direct marketing is a useful reminder of data protection rules" (May 18, 2009) *available at* *https://www.eversheds.com/uk/home/articles/index1.page?ArticleID=templatedata%5CEversheds%5Carticles%5Cdata%5Cen%5CE80%5Ce80_adjudication_shifty_direct_marketing_18may09*.

[343] M. Breersma, "EU Legislation - No Market For Spam," eWeek (Aug. 26, 2004), www.eweek.com/print_article/0,1761,a=134119,00.asp.

[344] For listings of the status of anti-spam laws in European nations, with links to the text of enacted and pending legislation, see http://www.spamlaws.com/eu.shtml.

sender's identity.[345] The European Coalition Against Unsolicited Commercial E-mail ("EuroCAUCE") has surveyed the current status of spam law on a country-by-country basis, including enacted anti-spam legislation, proposed laws under consideration, and existing laws that may alleviate spam.

Finally, the United Nations has begun efforts to control spam, suggesting uniform anti-spam legislation that would facilitate cross-border enforcement cooperation.[346]

H. *Spyware*

Spyware or software downloaded on users' computers without their knowledge, often when other free software is installed, raises issues similar to spam. Legislation to combat spyware has been introduced in many states, and the FTC has acted against several companies that caused spyware to be installed on computers.[347]

Similar issues were raised by the hidden rootkit software installed without the user's knowledge when certain Sony BMG Music Entertainment CDs were played on computers. The software hid itself from the user, made the computer susceptible to viruses and worms and disabled the CD drives on the computer it removed. Sony recalled the affected CDs, but numerous lawsuits were filed, including a suit by the Texas Attorney General under the Texas Consumer Protection Against Computer Spyware Act, and private suits in New York, California and Canada.[348] In December 2006, Sony BMG settled with forty states and the District of Columbia, agreeing to pay $4.25 million to the states, up to $175 to each consumer for computer damage, discontinuance of use of the software and other relief, after similar settlements with Texas and California.[349] Then, in January 2007, Sony BMG settled with the FTC, agreeing to reimburse consumers up to $150 each for damage to their computers, clear disclosure on CDs, and a prohibition on installation of software without the user's consent.[350]

The FTC also charged DirectRevenue LLC with unfair and deceptive practices based on DirectRevenue's methods of downloading adware onto consumers' computers and preventing the consumer from removing it.[351] According to the FTC, DirectRevenue installed software on

---

345 District Court of Zurich (Decision of 6th December 2002, ZR 102, 2003, no. 39).

346 "UN Aims to Bring Spam Under Control Within Two Years," http://www.siliconvalley.com/mld/siliconvalley/news/editorial/9090561.htm.

347 *See* "FTC Testifies on Spyware," Federal Trade Commission Press Release (October 5, 2005) (describing several FTC proceedings against spyware-related practices), *available at* http://www.ftc.gov/opa/2005/10/spyware.htm; *Zango, Inc.*, File No. 052 3130 (FTC 2006) (Settlement providing for disgorgement of $3 million by adware distributor, agreement not to download software without consumer consent), http://www.ftc.gov/opa/2006/11/zango.htm.

348 "Sony Music's Hidden DRM Installations Draw Consumer Ire, Spyware Label, Three Lawsuits," 71 PAT., TRADEM. & COPYR. J. (BNA) 103 (Nov. 25, 2005); *complaints available at* http://pub.bna.com/ptcj/texagsony112105.pdf (Texas); http://pub.bna.com/ptcj/059575comp.pdf (New York); http://pub.bna.com/ptcj/be342359comp.pdf (California); "Class-Action Lawsuits target Sony BMG Anti-Piracy Software as Spyware," WORLD COMM. REG REP. (BNA) (Aug. 2006) at 3 (reporting on *Cheney v. Sony of Canada Ltd.*, No. 06-CV-033329 (Ontario Super. Ct. of Justice) (filed Jan. 4, 2006); *Jacques v. Sony of Canada Ltd.*, No. 06-0044 (Sup.Ct. of B.C.) (filed Jan.4, 2006)*Guilbert v. Sony BMG Music (Canada) Inc.*, No. 500-06-00318-051 (Quebec Super.Ct.) (filed Nov. 14, 2005).

349 "Sony BMG to Reimburse Consumers in 40 States, D.C. in Anti-Copying Software Dispute," 73 PAT., TM. & COPYR. J. (BNA) 232 (Jan. 5, 2007).

350 *Matter of Sony BMG Music Entertainment*, FTC File No. 062-3019, *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf.

351 *Matter of DirectRevenue, et. al.*, FTC File No. 052-3131, *available at*

consumers' computers to monitor internet use and to display pop-up ads. DiretRevenue accomplished this by offering free software such as screensavers, games and other programs without adequately informing the user of the spyware. Additionally, DirectRevenue made the adware exceedingly difficult to identify and remove. The FTC settled with DirectRevenue for $1.5 million and imposed certain obligations on DirectRevenue's future conduct. Specifically, the settlement requires DirectRevenue to (i) provide reasonable ways for consumers to locate and remove the spyware once installed, and (ii) prevent future downloads without clearly notifying and obtaining consent from the consumers.

Recently, the FTC settled with CyberSpy Software, LLC, prohibiting it from marketing its keylogging software that is a completely undetectable way to "spy on anyone, from anywhere."[352] As part of the settlement order, the company must (i) not assist a purchaser in falsely representing that the software is an innocuous file, (ii) cause an installation notice to be displayed which must include a description of the nature and function of the program to which the user must expressly consent and (iii) take measures to reduce the risk that the spyware is misused, including license and monitoring and policing affiliates.[353]

A recent study by researchers at Harvard has determined that Sears failed to adequately notify its customers of spyware installed onto their computers where the warning came on page 10 of a 54-page privacy statement. According to the study, the Sears program fails to meet the standards set forth by the FTC in *Zango* and *DirectRevenue*.[354] Consumer groups are closely watching to see whether the FTC takes action in the matter.

I. *Trespass*

A developing concept to address third party competitive use of a firm's website is that of trespass to chattels. As noted above at note 54, eBay successfully sued a competitor that used software to locate, retrieve, copy and aggregate its auction listings.[355] The decision hinged on the burden the unauthorized searching software placed on eBay's servers. In a later decision, however, the same court held that unauthorized use of a website alone was enough to state a trespass claim in a case in which metatags were copied from the plaintiff's website.[356] So long as the unauthorized use was the proximate cause of damage to the plaintiff, that was enough, even though the copying of the metatags itself would seem an insignificant burden on the plaintiff's systems.

Trespass has also been used with some frequency to support claims against mass e-mailers:

> "there may be recovery . . . for interferences with the possession of chattels which are not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels

---

http://www.ftc.gov/os/caselist/0523131/0523131do070629.pdf.

[352] *Forbes*, "FTC Settlement Bars Marketing of Spyware for Illegal Uses," *reported in* Lexology (June 15, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=9f97fe2a-418d-41e4-af8b-dc1d9c999c80 (subscription).

[353] *Id.*

[354] Goodwin, *Sears admits to joining spyware biz*, The Register (Jan. 3, 2008), *available at* http://www.theregister.co.uk/2008/01/03/sears_snoopware_disclosure/print.html.

[355] *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

[356] *Oyster Software, Inc. v. Forms Software, Inc.*, 2001 U.S.Dist. LEXIS 22520 (N.D.Cal. 2001).

> survives today, in other words, largely as a little brother of conversion."[357]

The transmission of electronic signals through a computer network has been held to be sufficiently physical contact to constitute trespass to property.[358] However, this concept was refined by the court in *Ticketmaster Corp. v. Tickets.com, Inc.*, which stated that for a signal from one computer server to another to constitute actionable trespass, there must be physical harm to the chattel or some obstruction of its basic function.[359] Some courts have held that harm may be proved by demonstrating that an unauthorized user occupies system capacity on the victim's website, regardless of whether there is physical damage.[360]

Thus, a number of courts have held that the burdens imposed on an ISP's resources by unsolicited bulk e-mail, to the extent that these resources are unavailable or less available to the ISP's customers, is sufficient to establish trespass, even in the absence of physical damage, at least where the plaintiff has tried unsuccessfully to use reasonable technological means to protect its systems.[361]

The use of this theory by spam recipients, however, was struck a serious blow in June 2003, when the Supreme Court of California, by 4-3 vote, reversed a lower court decision in favor of Intel Corp. against a former employee, Kourosh Kenneth Hamidi, who had flooded its systems with e-mails critical of Intel sent to thousands of Intel employees.[362] The California Supreme Court held that without damage to, or impaired functionality of, Intel's computer systems, a trespass claim was not established, because there was no interference with Intel's use or possession of, or other legally protected interest in, the personal property itself.[363]

The Court took pains to distinguish cases in which ISPs had prevailed against spammers "based upon evidence that the vast quantities of e-mail sent by spammers both overburdened the ISP's own computers and made the entire computer system harder to use for recipients, the ISP's customers." In those cases, the quantity of e-mail impaired the functioning of the ISPs' computer systems, while Intel claimed injury from the distraction caused to recipient employees by the

---

[357] *Prosser & Keeton, Prosser and Keeton on Torts*, §14, 85-86 (1984), quoted in *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1020 (S.D. Ohio 1997). For a case upholding a claim for the conversion of electronic property, *see Ali v. Fasteners for Retail, Inc.*, 544 F. Supp. 2d 1064 (C.D. Cal. 2008) (plaintiff successfully stated conversion claim where defendants physically copied source code, cost data, and part numbers from his laptop and email without authorization). Accordingly to Steptoe & Johnson, *E-Commerce Law Wee*k (May 10, 2008), the *Ali* decision follows similar rulings in the Ninth Circuit (*Kremen v. Cohen*, 325 F.3d 1035 (9th Cir. 2003)), the New York Court of Appeals (*Thyroff v. Nationwide Mutual Ins. Co.*, 8 N.Y.3d 283 (2007)) and a Massachusetts trial court (*Network Sys. Architect Corp. v. Dimitruk*, 2007 WL 4442349, No. 06-4717-BLS2 (Mass. Super. Ct., Suffolk Co., Dec. 6, 2007)).

[358] *America Online Inc. v. LGCM*, 46 F. Supp. 2d 444, 452 (E.D. Va. 1998); *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal Rptr. 2d 468 (Ct. App. 1996).

[359] *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 WL 1887522, No. 99 CV7654, *4 (C.D. Cal. Aug. 10, 2000).

[360] *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 250 (S.D.N.Y. 2000), citing *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).

[361] *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021-24 (S.D. Ohio 1997). *See America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D.Va. 1998); *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550-51 (E.D. Va. 1998); *see also Hotmail Corp. v. Van$ Money Pie Inc.*, 47 U.S.P.Q. 2d 1020 (N.D. Cal. 1998) (finding likelihood of success on trespass claim against spammer); *America Online, Inc. v. Prime Data Systems Inc*, 1998 WL 34016692 (E.D. Va. 1998).

[362] *Intel Corp. v. Hamidi*, 1 Cal Rptr. 3d 32, 30 Cal. 4th 1342, 71 P.3d 296 (Cal.Sup.Ct. 2003).

[363] *Id*. at 36.

contents of the e-mail, "an injury entirely separate from, and not directly affecting, the possession or value of personal property."[364] Hamidi's thousands of copies of six separate messages – some 200,000 e-mails in all – were contrasted with the tens of millions of messages in ISP trespass cases.[365]

Where an individual can show harm to his or her computer, as in the case of so-called "spyware" that is installed on computers without the users' contract, trespass has been found to be a viable claim. In *Sotelo v. DirectRevenue LLC,*[366] a Federal District Court allowed a trespass claim to proceed in a class action against a spyware purveyor whose product slowed down affected computers, depleted Internet bandwidth and computer memory, and took hours to remove. And in 2007, a North Carolina court found that a trespass claim was stated where unwanted pop-up advertisements were alleged to have caused actual or constructive possession of the goods in question and unauthorized, unlawful interference or dispossession of the property.[367]

J. *Privacy*

As the use of the Internet and mobile communication devices has become ubiquitous, companies are gathering more and more information regarding their customers and visitors to their websites. Databases of this information are a powerful business and marketing tool, but also raise a serious threat to the privacy of personal information. Governments around the world are addressing that threat through laws regulating the collection, disclosure and use of personal data. This paper addresses recent developments in this area, focusing on the United States and Europe. At the outset, it is worth noting that Europe has adapted extensive substantive regulation of the treatment of personal information. In contrast, in the U.S., substantive regulation has been limited to a few specific areas, such as children's information, medical information and financial services. Instead, the regulatory focus has been on matters such as transparency to the consumer with respect to the manner in which information will be used and shared and the security protections in place, as well as the procedures to be followed in the event of a security breach.

1. *The European Community Directive*

Use of personal data, such as medical information, credit card records, purchasing patterns and the like, by businesses that gather it, whether over the Internet or by other means, has been restricted in Europe by various privacy directives.[368] The European Community's 1995 Data Protection Directive[369] prohibits companies from transmitting data to countries that do not

---

[364] *Id*. at 37.
[365] *Id*. at 44.
[366] 384 F.Supp.2d 1219 (N.D. Ill. 2005).
[367] *Burgess v American Express Co. Inc.,* 2007 WL 70251, 2007 NCBC 15 (Gen'l Ct. of Justice, Super. Ct. Div. Polk Co. 2007), *available at* http://www.ncbusinesscourt.net/opinions/2007%20NCBC%2015.pdf.
[368] Whether the European approach actually results in greater privacy is open to question. *See, e.g.*, K. Jamal, M. Maier and S. Sunder, "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the U.S. and the U.K., Working Paper 03-8," AEI – Brookings Joint Center for Regulatory Studies (July 2003, *available at* http://aei.brookings.org/admin/pdffiles/phpWo.pdf; Lettice, "U.S. Full Marks, Europe, Null Points – Study," THE REGISTER (July, 28, 2003), http://www.theregister.co.uk/content/6/32018.html.
[369] 95/46/EC. The Directive is *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. The Directive broadly defines "personal data" to include information relating to an identified person or to an individual identifiable, directly or

adequately protect it.[370] The Directive applies to non-European companies with European customers, employees or others from whom personal data is collected. Thus, the collection of personal data by a U.S. company over its website could violate European law, given the lack of U.S. protection of such information, particularly if the data is collected through facilities or equipment located in Europe, including the use of cookies placed on European users' computers.[371]

The EC also enacted a Directive on Privacy in the Electronic Communications Sector (the "E-Privacy Directive") in 2002 that requires consumers to be given clear and precise information about the purposes of the cookies and an opportunity to refuse them before cookies may be used.[372] As amended in 2009, the E-Privacy Directive requires that consumers *actively* give consent to such cookies.[373] For instance, the EU Article 29 Working Party has rejected a privacy framework proposed by the Interactive Advertising Bureau (Europe) because, among other things, users could not be considered to have consented to receive cookies where they use an internet browser that allows cookies by default – in the absence of active informed consent, "[i]t cannot be concluded that users who have not objected to being tracked for the purposes of serving behavioural advertising have exercised a real choice."[374] Spyware, web bugs and similar

---

indirectly, by reference to his or her identification number or physical, physiological, mental, economic, cultural or social identity.

370 It is worth observing that, notwithstanding the Directive, the Supreme Court of France ordered France Telecom to provide its list of unlisted telephone numbers to a marketing company, holding that the exclusive use of the lists by France Telecom was an abuse of dominant position and rejecting privacy arguments. *France Telecom v. Lectiel*, Arret No. 2030, Cour de Cassation, Chambre Commerciale (Dec. 4, 2001), *reported in* WORLD DATA PROTECTION REP. (BNA) 25 (Jan. 2002).

371 *See* H. Rowe, "E.U. Data Protection Applies to Personal Data Processing on the Internet by Non-E.U. Based Websites?", WORLD INTERNET L. REP. 26 (Aug. 2002) (discussing May 30, 2002 working document of Working Party established under the Directive).

372 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Recitals (24)-(25) and Art. 5, sec. 3, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML. For suggestions on compliance for websites using cookies, see Dr. B. Goldman, "Europe Administers Diet for Cookies," WORLD INTERNET L. REP. 26 (Feb. 2004) at 16-24.

373 *Id.* The 27 EU Member States were required to enforce these changes by May 25, 2011, which has resulted in various approaches to implementation and enforcement. As anticipated, "Member States seem to be taking markedly different approaches to implementing the amendment, creating yet another 'regulatory patchwork' in the EU privacy area." Worlton, "EU Cookies – Where Did the Pieces Fall?", Wiley Rein LLP (July 2011) (noting also that many member states failed to enact implementing rules as of the compliance deadline), *available at* http://www.wileyrein.com/publications.cfm?sp=articles&id=7223. Overall, these changes may have a significant effect on international advertising and referrals. Nabarro LLP, *New European Laws Could Impact the Use of Cookies on Websites from May 2011* (March 5, 2010), *available at* http://www.nabarro.com/Downloads/Commercial-IT-Comms-European-changes-to-laws-on-cookies.pdf. As of June 2012 five EU member countries have been referred to the European Court of Justice as a result of their failure to meet the May 2011 deadline. The EU Commission has reportedly sought significant fines for non-compliant countries, ranging from $16,000 to $138,000 for each day of non-compliance. *See* Thomas, "EU refers five countries for failure to implement cookie directive," Winston & Strawn LLP (June 6, 2012), *available at* http://www.winston.com/index.cfm?contentID=19&itemID=272&itemType=25&postid=948. However, one of these countries – Portugal – has since enacted its own "cookie legislation," Law No. 46/2012 of 29 August. *See* "New Law on 'Cookies' and Processing of Personal Data Via Websites Imposes Fines that Can Reach up to €5,000,000," Abreu Advogados (Nov. 10, 2012).

374 Massey, Mattina, Schroder, Sheraton and Uphoff, "How the cookie crumbles: a clash of cultures on cookie regulation, McDermot Will & Emery (Nov. 3, 2011), *reported in* Lexology, *available at*

devices, that can store hidden information or trace user activities, are permitted only for legitimate purposes with the user's knowledge.[375] In April 2012 the Article 29 Working Party issued a "cookie consent exemption" opinion under the E-Privacy Directive.[376] Specifically, the opinion provides exemptions from the E-Privacy Directive's informed consent requirement where the cookie is either necessary "for the sole purpose of carrying out the transmission of a communication over an electronic communications network" or "necessary in order for the [functionality] of an information … service explicitly requested by the subscriber …." Importantly, however, third-party behavioral advertising cookies are unlikely to meet either exemption, according to the Opinion.

In an attempt to keep pace with technological innovation and emerging business practices, in July 2012 the Article 29 Working Party also issued an opinion concerning the privacy and security implications of cloud computing.[377] In the Opinion, the Working Party lays out a "checklist for data protection compliance by cloud clients and cloud providers." Among other things, the Opinion recommends that:

- client-organizations which control personal data, and therefore remain ultimately responsible for its safekeeping, should select a cloud computing service provider who guarantees compliance with the EU Data Protection Directive;

- client-organizations should insist on certain contractual safeguards concerning cloud providers, such as the disclosure of third parties (e.g., subcontractors) to whom the provider will communicate data and locations where the data will be sent; and

- cloud service providers should engage third-parties to audit and ensure compliance with their data protection protocols, reports concerning which should be available to potential clients.

In response to the E-Privacy Directive, the United Kingdom enacted new laws on cookies and e-commerce, effective May 2012, which apply to all data collected electronically, whether through cookies or other means, and whether constituting personal information or not.[378] Cookies and similar methods of gathering data may not be used without user consent given after having

---

http://www.lexology.com/library/detail.aspx?g=fba09f8d-9408-42d5-b64d-b3117a3a643e. France's Commission National de I'nformatique et des Libertés has also established guidelines implementing the E-Privacy Directive that reminds website operators that browser settings alone are not sufficient to fulfill EU privacy obligations in the absence of other express and informed consent. However, certain analytics cookies are exempted from the prior consent requirement. CNIL's guidance is *available at* http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/ (French).

[375] *Id*.

[376] Article 29 Working Party, *Opinion 04/2012 on Cookie Consent Exemption*, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2. The Opinion also provides, among other things, that such exempted cookies should remain on a user's terminal device for only as long as necessary for its exempted purpose. Moreover, where a cookies has multi-purposes, each separate purpose must be exempt to avoid the need to obtain user consent.

[377] Article 29 Working Party, *Opinion 05/2012 on Cloud Computing, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2*.

[378] "UK Cookies Update: New Laws on Cookies and E-commerce," *Duane Morris Alert* (April 25, 2012) *available at* http://www.duanemorris.com/alerts/UK_cookies_update_new_laws_on_cookies_and_e-commerce_4436.html.

received clear and comprehensive information about what the cookies or other means of data gathering are doing and what information is being stored. Notably, regulatory guidance indicates that consent requires communication by which the user knowingly indicates acceptance, such as clicking an icon, sending an email or subscribing to a service; the key is that the user understand that the by taking the action, he or she is providing consent. The guidance recommends minimizing situations that require a cookie to be set before the web page is displayed and to seek the consent as soon as possible, while being prepared to demonstrate that the site is doing all it can to provide the information and seek consent as promptly as possible.[379] The UK issued additional guidance in May 2012, clarifying that implied consent (as opposed to active consent) may be acceptable if appropriately obtained, such as by directing the individual's attention to a prominently-displayed link to a clear and well-drafted privacy policy.[380]

Canadian law is even more stringent. While the European E-Privacy Directive permits websites to condition access on acceptance of cookies, so long as their purpose is legitimate and the acceptance is well informed, the Canadian Privacy Commission found that an airline's denial of access to users who refused cookies was a violation of the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA).[381] This Canadian law applies to all companies – including U.S. companies – that collect, use or disclose personal information about Canadian citizens in the course of commercial activities.[382] PIPEDA's protections are broad enough to prohibit employers from using or considering even *publically-available* personal information concerning job candidates on social networking sites.[383]

Other nations are adopting broad privacy protections as well.[384]

---

379 *Id.*

380 *See* "Guidance on the rule on use of cookies and similar technologies," UK Information Commissioner's Office, (May 2012), *available at* http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies?hidecookiesbanner=true.

381 Commissioner's Findings, PIPED Act Case Summary #162, "Customer complains about airline's use of 'cookies' on its Web Site," (April 16, 2003), case summary *available at* http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_7_e.cfm, reported *in* "Canada: Airline Violated Privacy Law Using Computer Cookies," WORLD INTERNET L. REP. (BNA) at p.27 (July, 2003).

382 Guidelines issued in late 2011 by the Canadian Privacy Commission make clear that information collected by companies for online behavioural advertising (OBA) purposes will "generally constitute personal information" under the Canadian Protection of Personal Information and Electronic Documents Act. Consequently, advertisers using OBA must have an OBA policy that is accessible, easy-to-read, and accurate. Moreover, the guidelines provide that individuals must be made aware that information is collected for OBA before it is collected, and opt-ing out must be a simple process. Finally, the guidelines state that websites targeting children should avoid tracking activities. Salzberg, "Privacy Commissioner Releases New Online Behavioural Advertising Guidelines," McCarthy Tétrault LLP (Dec. 21, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=a882d79f-d2dc-49c4-b713-c2aab63bb699.

383 Muter, "New guidelines for social media background checks," Boughton Law Corp. (Jan. 7, 2012), *available at* www.boughtonlaw.com/.../Boughton-Law-New-Guidelines-for-Social-Media. pdf.

384 A notable example is India, through which a great volume of personal information passes, given its large role in the outsourcing of customer service and other functions. Hobby, Hollis, Johnson, Miller, Quittmeyer and Dodson, "India adopts new privacy and security rules for person information," Sutherland Asbill & Brennan LLP (Aug. 9, 2011), *reported* in Lexology, http://www.lexology.com/library/detail.aspx?g=9a9b9ec0-e390-45b8-a6f1-4363e29e9af3. Among other things, the Rules require that (i) privacy policies are published on the websites of collectors of personal information; (ii) reasonable steps are taken to inform the individual that his or her information is being collected, the purpose for which it is being collected, the intended recipients of the information, and the

The EU privacy regulations affect U.S. companies that wish to receive information about its European employees or customers, or respond to government demands for information about Europeans.

This concern was the subject of negotiations between the United States and the European Community. In 2000, the Department of Commerce issued the final version of an intergovernmental agreement[385] creating a "safe harbor" for U.S. companies that voluntarily and publicly agree to adhere to specified principles, including:

> (a) *Notice*: Notice to individuals of the purposes for which personal information is collected, the types of third parties to whom it is disclosed, and how individuals may limit such use and disclosure where it is for a purpose other than that for which the information was originally collected or later authorized;[386]
>
> (b) *Choice*: An opportunity for individuals to choose ("opt out") whether and how their personal information is used or disclosed to third parties, where such use is incompatible with the original purpose of collection; for sensitive information (e.g. medical information or information regarding racial or ethnic origin, political opinions, religious beliefs and the like, or information designated as sensitive by the source) individuals must be given an explicit choice ("opt in") before the information is disclosed to a third party or used for a purpose other than that for which it was originally collected;
>
> (c) *Onward Transfer*: A requirement that third parties, who are acting as agents of the a business, to whom personal information may be transferred by that business without Notice and Choice, must provide at least the same level of protection;
>
> (d) *Security:* Use of reasonable measures to protect personal information from loss, misuse, unauthorized access or disclosure, alteration or destruction;

---

name and address of the entity collecting or retaining the information; (iii) individuals must be provided the right to review and correct inaccuracies in their personal information and a grievance procedure must be established to rectify complaints within one month of their receipt; and (iv) personal information is securely maintained. Moreover, certain additional restrictions apply to "sensitive personal data." *Id*.

[385] For more information on the Safe Harbor Agreement see the Commerce Department's website at http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_018879.pdf.

[386] The notice must be specific. In a ruling dated January 13, 2005, the Spanish Data Protection Authority fined a Peugeot dealer for collecting data without "explicitly, precisely, and unequivocally in form[ing] the data subject about the purpose of collecting the data and the recipients of the information. Statements that data were collected "for commercial purposes" or "to send you offers about our products or services" were found inadequate, as were authorizations by the data subject to disclose "your data to the companies who are members of the Peugeot Group and of the Official Commercial Network." A more specific disclosure of purposes and recipients was required. Similarly, in March 2012 France's Commission Nationale de L'Informatique et des Libertés (CNIL) determined that Google's privacy policy was in violation of the Data Protection Directive because, according to CNIL, the policy "provides only general information about all the services and types of personal data Google process," making it "extremely difficult to know exactly which data is combined between which services for which purposes, even for trained privacy professionals." Halberstam, "The EU objection to Google's combined privacy policy explained – it's not what you do, it's the way that you do it," Kingsley Napley (March 14, 2012), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=f2df543d-6bec-4689-b6a2-faa4a6150c6b. In October 2012, CNIL informed Google that it would have "three or four months" to comply, or it would face enforcement action. However, as of April 2013, Google has "not implemented any significant compliance measures" and CNIL has called on national authorities to "carry out further investigations according to the provisions of its national law transposing European legislation." *See* CNIL website, *available at* http://www.cnil.fr/english/news-and-events/news/article/google-privacy-policy-six-european-data-protection-authorities-to-launch-coordinated-and-simultaneo/.

(e) *Data Integrity:* A prohibition on processing personal information in a way that is incompatible with the purposes for which it is collected or subsequently authorized;

(f) *Access:* Giving individuals reasonable access to information about them and the opportunity to correct or delete inaccurate information; and

(g) *Enforcement:* A mechanism for enforcing compliance with these principles.[387]

A comprehensive checklist is available on the Department of Commerce's Safe Harbor website, www.export.gov/safeharbor/index.html.

The EC has recognized the Federal Trade Commission (under § 5 of the FTC Act) and the Department of Transportation (under 49 U.S.C. § 41712, relating to unfair and deceptive practices by air carriers and ticket agents) as government bodies empowered to investigate complaints and obtain relief against unfair or deceptive practices or non-compliance with the safe harbor principles.[388] (Businesses not subject to FTC or DOT jurisdiction such as telecommunications, banking, insurance and non-profit companies, cannot take advantage of the Safe Harbor program.) The FTC has sued and entered into consent orders with several US companies that have falsely claimed to comply with the Safe Harbor framework in violation of § 5 of the FTC Act.[389]

Moreover, private damage actions have been filed in U.S. courts for the improper collection, use and transfer of personal information, albeit with little success to date.[390]

United States companies should consider bringing themselves within the safe harbor if they collect personal data from individuals in the EC.[391] This means certifying to the Department

---

[387] See www.ita.doc.gov/td/ecom/shprinciplesfinal.htm.

[388] See J. Clausing, *Europe and U.S. Reach Data Privacy Pact*, N.Y. TIMES, Mar. 15, 2000.

[389] In November 2009 and January 2010, the FTC issued consent orders settling charges that six US companies (World Innovators, ExpatEdge Partners, Onyx Graphics, Directors Desk, Collectify and Progressive Gaitways) falsely claimed to have complied with the Safe Harbor framework in violation of section 5 of the FTC Act. The orders, which each remains in effect for a period of 20 years from the most recent date the U.S. or the FTC files a complaint alleging a violation of such order, require that the companies in question (i) not misrepresent expressly or by implication the extent to which they are a member of, adhere to, comply with, are certified by, are endorsed by or otherwise participate in any privacy, security or other compliance program sponsored by the government or any other third party, (ii) file with the FTC written reports regarding the manner and form of their compliance with the orders and (iii) maintain and upon request make available to the FTC copies of all documents relating to compliance with the orders for 5 years. The companies also could be subject to civil penalties if they engage in any such misrepresentations going forward. Krasnow, Glazer and Bildsten, "U.S. Companies Misrepresenting EU Data Protection Directive Safe Harbor Compliance Risk Federal Trade Commission Enforcement Action" *reported in* Lexology (May 11, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=71ce5496-4d5f-417f-be06-5e776df7d04d.

[390] *See, e.g., Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001) (summary judgment for defendant); *In re Doubleclick Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (summary judgment for defendant); *Rivera v. Match Logic, Inc.*, No. 00-K-2289 (D. Colo.) (filed Nov. 20, 2000), *reported in* 79 ANTITRUST & TRADE REG. REP. (BNA) 569 (Dec. 15, 2000).

[391] Although the European Parliament called for the suspension of the safe harbor data privacy agreement with the United States last year in the wake of the alleged spying and data collection activities undertaken by the U.S. National Security Agency, the EC did not act to suspend the agreement and, instead, proposed a new data protection mandate to strengthen the current data privacy agreement. Jennifer Baker, *EU will not suspend safe harbor data privacy agreement with the US*, PC World, Nov. 27, 2013, *available at* http://www.pcworld.com/article/2067480/eu-will-not-suspend-safe-harbor-data-privacy-agreement-with-the-us.html. Some proposed regulations include, among other things, increased fines for data processors that violate the regulations, tighter restrictions on transferring data outside the EU, and an expanded right of data subjects to have certain personal data erased by those controlling the

of Commerce their adherence to the safe harbor principles and implementing privacy policies that comply with those principles.[392]

A Commission Staff Working Document report analyzing the compliance of participating companies found substantial non-compliance, as a result of failure of companies to have publicly posted privacy policies, or policies that did not fully and clearly comply with the seven privacy principles.[393] The report suggested that European data protection authorities use their power to suspend distributors if they find a substantial likelihood that the principles are being violated. To assist companies in creating compliant, easy to understand privacy policies, the EU has adopted a plan calling for companies to use "very short," "condensed," or "complete" privacy policies in a common format.[394] Major companies are beginning to use the format.[395]

Outside the boundary of the safe harbor, businesses that collect or receive personal data from EU persons risk violation of EC law,[396] although other means of compliance may be elected.

---

data. *See* E-COMMERCE LAW WEEK (Oct. 26, 2013), *available at* http://www.steptoe.com/publications-9144.html; *see also* Press Release, European Commission, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, Jan. 25, 2012, *available at* http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.
In 2013, the EU began requiring that telecom companies and internet service providers that serve European customers report data breaches within 24 hours where personal data has been lost, stolen or "otherwise compromised". Usually companies will have to disclose the nature and size of the breach within 24 hours, but where this is not possible they must submit "initial information" within this time and provide full details within three days. *See* Press Release, European Commission, Digital Agenda: New specific rules for consumers when telecoms personal data is lost or stolen in EU, June 24, 2013, *available at* http:// http://europa.eu/rapid/press-release_IP-13-591_en.htm

[392] As of May 2014, there were over 3,500 companies on the Department of Commerce's certified list, *see* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list. Obviously, statements by companies that they comply must be truthful. Although FTC enforcement as to the Safe Harbor framework appeared to have slowed in 2013, in the first quarter of 2014, the FTC has settled approximately 14 separate actions with a wide range of companies that falsely self-certified under the EU/U.S. Safe Harbor Framework, including three National Football League teams and a prominent clothing retailer. *See In re Atlanta Falcons Football Club, LLC*, File No. 142 3018, Agreement Containing Consent Order, Jan. 21, 2014, *available at* http://www.ftc.gov/sites/default/files/documents/cases/140121atlantafalconsagree.pdf; *In re Tennessee Football, Inc.*, File No. 142 3032, Agreement Containing Consent Order, Jan. 21, 2014, *available at* http://www.ftc.gov/sites/default/files/documents/cases/140121tennesseefootballagree.pdf; *In re PDB Sports, Ltd., d/b/a Denver Broncos Football Club*, File No. 142 3025, Agreement Containing Consent Order, Jan. 21, 2014, *available at* http://www.ftc.gov/sites/default/files/documents/cases/140121denverbroncosagree.pdf; *see also In re American Apparel, Inc.*, File No. 142 3036, Agreement Containing Consent Order, May 9, 2014, *available at* http://www.ftc.gov/system/files/documents/cases/140507americanapparelagree.pdf.

[393] Commission Staff Working Document, "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC (2004) 1323 (Oct. 20, 2004).

[394] "Opinion on More Harmonised Information Provisions," Article 29 Data Protection Working Party, 11987/04/EN, WP100 (Nov. 25, 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf; "EU Issues Guidance on Privacy Notices," DMNEWS (Jan. 5, 2005), http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=31430.

[395] J. Vijayan, "Companies Simply Data Privacy Notices," COMPUTERWORLD (Jan. 10, 2005), http://www.computerworld.com/s/article/98812/Companies_Simplify_Data_Privacy_Notices.

[396] For example, Directive 95/46/EC of October 24, 1995, prohibits the unauthorized access to or the transfer out of the EU of an individual's personal data without consent. On January 19, 2008, the Working Party published its conclusion that "[s]earch engines fall under the EU Data Protection Directive 95/46/EC if there are controllers collecting users' IP addresses or search history information, and therefore have to comply with relevant provisions." The group concluded that the Directive applies to the search engines of companies who have "an establishment" in a European Union member state or that use automated equipment based in a member state for processing personal

One option – perhaps impractical – is obtaining the informed consent of every individual whose information is to be transferred. Another option for such businesses is to choose to use binding contracts that conform to EC Directive requirements with those who provide them with personal data and anyone to whom they transfer such data. To facilitate this, the EC has adopted standard contract forms, under which the data transferred is treated in compliance with EU data protection standards.[397] Note that companies that outsource data processing to third parties remain responsible for breaches of privacy occurring at the third parties' hands.[398] Another option is the development of "binding corporate rules" (BCR) for internal governance within multinational data processing or data controlling organizations. Such binding rules must be legally enforceable and subject to audit, and require the approval of data protection authorities.[399] Once in place, BCRs are designed to ensure that protected data will not be compromised as a result of transfers within a corporate group to countries outside of the EU.[400]

European actions indicate that enforcement of privacy rules can be expected. The European Court of Justice found that a website published by a Swedish woman that included names of her colleagues, job descriptions and some telephone numbers and other personal information, constituted the processing of personal data under the Data Protection Directive.[401] In 2013, the Federal Court of Justice in Germany required Google to delete negative suggestions generated by the company's autocomplete search function (here, associating the plaintiffs name with "fraud" and "scientology"), after notice from the complainant on the grounds that such negative autocomplete suggestions violated "personality rights."[402]

---

data. Press Release of the Article 29 Data Protection Working Party (Feb. 19, 2008), *available at* http://ec.europa.eu/justice/policies/privacy/news/docs/pr_18_19_02_08_en.pdf.

[397] *See* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/851&format=HTML&aged=1&language=EN&guiLanguage=en; http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/12&format=HTML&aged=0&language=EN&guiLanguage=en; "standard contractual clauses for the transfer or personal data to third countries – Frequently asked questions," MEMO/05/3 (Jan. 7, 2005), http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=0&language=EN. In February 2010, the European Commission approved a new set of model contract clauses for the transfer of personal data. *See* E-COMMERCE LAW WEEK (February 18, 2010), *available at* www.steptoe.com.

[398] "Outsourced Data Must Be Protected, Says U.K. Privacy Chief", The Register, July 17, 2006), http://www.theregister.co.uk/2006/07/12/outsourced_data_protection/.

[399] M. Watts, "Transferring Personal Data from the E.U.: Are Binding Corporate Rules the Answer?" 4 WORLD DATA PROTECTION REPORT (BNA) No. 3 (March 2004) at 1. Binding corporate rules are submitted for approval to the lead data protection agency – generally in the country where the business has its European headquarters – which then consults with data protection agencies in all affected EU countries before providing comments to the applicant for revision. M.L. Jones, "Data Protection – The E.U./U.S. Data Divide, WORLD TAX and LAW REP. (BNA INT'L) No. 22 (Sept. 2005). The EU in 2005 set forth procedures for approval in two documents, "Working Documents Establishing a Model Checklist Application for Approval of Binding Corporate Rules," Article 29 Working Party, 05/ENWP/08 (April 14, 2005), *available at* http://www.steptoe.com/publications/352f.pdf; and "Working Document setting forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From Binding Corporate Rules," Article 29 Working Party, 05/EN WP/07 (April 14, 2005) *available at* http://www.steptoe.com/publications/352g.pdf.

[400] In June 2012, the Article 29 Working Party adopted WP 195, which sets forth BCR requirements for data processors, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/. The BCRs concept had previously only applied to data controllers as established by WP 153.

[401] *Lindquist*, Case C-101/01 (Eur. Ct. Justice Nov. 6, 2003), *available at* http://curia.eu.int/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET.

[402] BGH, VI ZR 269/12, *available at* http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2013&Sort=3&nr=64071&pos=0&anz=86 and *discussed at* http://www.lexology.com/library/detail.aspx?g=270623e1-fcf0-4176-94ec-64a0e3539334.

An EC investigation into whether Microsoft's Passport Internet authorization system violates EU rules[403] was settled in 2003 by Microsoft's agreement to make a "radical change" to its .NET Passport system, providing users with more information and choices as to the data they want to provide and how it will be used by Microsoft and other websites on a site-by-site basis.[404]

In another example of European privacy enforcement, a German state Interior Ministry found that certain Hewlett-Packard printer driver software violated German data protection law by transmitting technical information, including IP addresses and printer model numbers, to a Hewlett-Packard server outside Germany without appropriate user consent.[405] Hewlett-Packard agreed to remedy the problem. However, The High Court of Ireland has held that IP addresses are not always personal data.[406] In upholding a settlement agreement between the nation's largest ISP, Eircom, and four music record companies in connection with Eircom's failure to take action to discourage peer-to-peer copyright infringement on its networks, Eircom agreed to implement a graduated response mechanism with its infringing customers managed by a third party service provider who would get access to the IP addresses of such customers. The Court held that that transfer of IP addresses was not personal information and therefore not in violation of Irish privacy law because the third party service provider would not have the "means" or "motivation" to find out the names or addresses of the persons corresponding to the IP address, the customers consented to Eircom's terms of use, and the graduated response mechanism was implemented in furtherance of a legal contract.[407]

French authorities have warned that sharing of credit and payment histories must conform to French privacy law. While such information may be used for internal and intra-industry purposes, it may not be shared with other industries, and must comply with privacy practices, such as offering a right of redress to the subject of the information.[408] Norway has recently enacted security rules requiring all Norwegian employers subject to Norwegian tax laws to encrypt paycheck stubs sent via e-mail to employees' personal accounts.[409] And in Spain, authorities are charging Google for collecting personal information via Wi-Fi "interceptions" by Google Street View trucks and conveying that information to the United States in violation of the Spanish Information Protection Law.[410]

The United Kingdom's Information Commissioner's Office (the "ICO") announced that where laptops containing unencrypted personal information are lost or stolen, enforcement action may be commenced against even private individuals under the U.K.'s Data Protection Act of 1998 (c. 29) which applies to any person who controls and loses personal data.[411] The

---

403 "Microsoft Faces European Commission Inquiry on Privacy Concerns," N.Y. TIMES, May 28, 2002, at p. C4.

404 "European Union Microsoft 'Passport' – Commission Will Not Impose Sanctions," WORLD INTERNET L. REP (BNA) at 30 (Feb. 2003).

405 Hunton & Williams, Privacy and E-Commerce Alert (March 14, 2003).

406 http://www.hldataprotection.com/2010/04/articles/international-compliance-inclu/irish-court-ip-addresses-not-personal-data/.

407 *Id*.

408 "Privacy: French Agency Decries Bad-Credit Blacklist, Citing Sharing of Data Beyond Affected Sector," BANKING DAILY (BNA) (December 17, 2003).

409 *See* E-COMMERCE LAW WEEK (March 20, 2010), *available at* www.steptoe.com/E-CommerceLawWeek.

410 Baker, "Spanish cases against Google serve as a reminder of the need to take steps to allow data transfers from Europe to the US," *reported in* Lexology (November 8, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=b863f2b5-669a-4044-ac26-8dc015a87eae.

411 *See Data Security – Information Commissioner's Office Guidance*, WORLD DATA PROTECTION REP. 8 (BNA) (Jan. 2008).

announcement is consistent with EC privacy policy, which requires that possessors of data use reasonable measures to protect personal information from loss or unauthorized access. Moreover, as of April 6, 2010, the ICO will have authority to impose monetary penalties up to £500,000 on organizations for serious breaches of the Data Protection Act.[412]

The U.S. Sarbanes-Oxley Act's requirement of anonymous corporate whistleblower hotlines has been held to conflict with European data protection laws. Under Sarbanes-Oxley, public companies must provide at least one confidential, anonymous method for employees to submit complaints about questionable accounting matters.[413] French and German decisions have held that such methods may violate European Law.

A German Labor Court held that an anonymous hotline could not be implemented by WalMart without first consulting with the works council, which had a right to participate in "matters relating to the rules of operation of the establishment and conduct of employees."[414] In 2005, the French data protection agency, the Commission Nationale d' Information et des Libertées ("CNIL") found that anonymous hotlines would "reinforce the risk of slanderous denunciations" and "was disproportionate to the objectives sought."[415] In addition, a French court ordered the French subsidiary of a U.S. company to discontinue a whistleblower hotline, on similar grounds.[416] In December 2009, the French Supreme Court considered the validity of a corporate code of conduct implemented by a company in order to comply with Sarbanes-Oxley. The Court found that the scope of the company's code of conduct was too broad, since not only did it invite employees to report violations relating to more than just finance, accounting and anti-corruption matters, but also intellectual property rights, confidentiality, discrimination, conflicts of interest and harassment outside the scope of the CNIL 2005 decision.[417]

European data protection laws require that individuals have notice of what data is collected about them and that it be processed fairly. Anonymous tips, about which the employee complained about is not informed, and cannot contradict, raise significant data protection and privacy issues under European law. Recognizing the conflict with U.S. law, CNIL issued guidelines in November 2005.[418] The CNIL guidelines, among other things, require that whistleblowing systems be limited in scope: employees should not be required, but merely encouraged to use them: and anonymous reports should be discouraged, and, when received,

---

412 *See* The Data Protection Regulations 2010 No. 31, *available at* http://www.opsi.gov.uk/si/si2010/pdf/uksi_20100031_en.pdf.

413 Sarbanes Oxley Act of 2002 §301; SEC Rule 10A-3(b)(3).

414 Arbeitsgericht Wuppertal, Court order dated June 15, 2005, 5 BV 20/05.

415 CNIL Decision 2005-110 of May 26, 2005 (Exide Technologies).

416 CE Bsn Glasspack, Syndicat CGT/Bsn Glasspack, Tribunal de grande instance de Libourne Ordinance de référé 15 Septembre 2005, *available at* http://www.legalis.net/jurisprudence-decision.php3?ID_article=1497.

417 While French companies were already required to obtain CNIL approval for whistleblowing that exceeded the scope of the 2005 decision (see footnote 405, above), the French Court's decision helped to clarify exactly when such approval is available; namely, in matters related to accounting, finance, banking, anti-corruption, competition, Section 301(4) of Sarbanes-Oxley and the Japanese Sarbanes-Oxley. Martin, "French Data Protection Agency Restricts the Scope of the Whistleblowing Procedures: Multinational Companies Need to Make Sure They are Compliant," Lexology (December 15, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=1d2fe56a-92c1-4d12-9436-cd9b9e21f26a.

418 CNIL, "Guideline document adopted by CNIL on 10 November 2005 for the implementation of whistleblowing systems….,"*available at* http://www.cnil.fr/fileadmin/documents/en/CNIL-recommandations-whistleblowing-VA.pdf.

must be handled with precautions. Critically, the individual who is the subject of the report must be notified promptly.

The EU Article 29 Working Party followed with a preliminary opinion in 2006[419], which recognized that companies subject to Sarbanes-Oxley "are subject to heavy sanctions and penalties" for failure to comply with the Act's whistleblowing requirements, but face "risks of sanctions from EU data protection authorities if they fail to comply with EU data protection rules." The preliminary report stresses that "whistleblowing schemes must be implemented in compliance with EU data protection rules" and that the individual accused by a whistleblower is entitled to the rights guaranteed by European data protection law. It observed that "whistleblowing schemes entail a very serious risk of stigmatisation and victimisation . . .within the organisation" and that "[t]he person will be exposed to such risks even before the person is aware that he/she has been incriminated and the alleged facts have been investigated."

The report does recognize Sarbanes-Oxley whistleblowing rules as a legitimate initiative to protect the interests of shareholders, so long as adequate safeguards are in place. The report suggests a number of steps that may be taken in this vein:

- Possible limits on the number of persons who may report alleged misconduct
- Possible limits on the categories of persons who may be incriminated
- Promotion of identified and confidential reports rather than anonymous reports
    - The report indicates that anonymous reports are particularly problematic and that only identified reports should be used. Whistleblowers should be informed that their identity will be kept confidential and not disclosed to third parties, including the accused. Only if despite this step, the person making the report wants to remain anonymous should the report be accepted. Anonymous reports should be treated with special caution, and perhaps investigated more quickly because of the risk of misuse.
- Clear definition of the limited types of information to be communicated
- Compliance with strict data retention periods
    - Generally data should be deleted promptly, usually within two months of completion of the investigation, unless legal or disciplinary proceedings are taken.
- Provision of clear and complete information about the whistleblowing scheme
- Respecting the rights of the accused to be informed of the charges against him as soon as possible, and how to exercise his rights of access and rectification
    - The report recognizes that where such notice would jeopardize the investigation, it may be delayed, and that the whistleblower's identity should not be disclosed unless the whistleblower is found to have made a malicious false statement.
- Adequate security measures to protect the security and confidentiality of the data

[419] ARTICLE 29 Data Protection Working Party, "Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime," Document 00195/06/EN, WP 117, adopted Feb. 1, 2006, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

- Establishment of a specific, separate management structure for the whistleblowing scheme, with data generally remaining in the country in which it is reported.

In addition, whistleblowing schemes need to comply with the requirements of notification to national data protection agencies under the data protection laws of individual EU nations.

U.S. companies caught between the conflicting mandates of Sarbanes-Oxley and the EU data protection laws need to establish hotline programs that comply with these requirements, for example by providing for informing employees accused of improprieties of the details of the complaints and offering them an opportunity to respond, excepting European employees from the program, and treating the complaint's content as personal information of the employee complained about, subject to the applicable privacy rules.

Concerns have also been raised that the EU's data protection Safe Harbor is incompatible with the USA PATRIOT Act. For instance, in 2011 Microsoft announced that, in some circumstances, it may be required to disclose to U.S. authorities the personal data of EU residents, and that such disclosures may be kept secret from EU authorities and data subjects, in accordance with the USA PATRIOT Act. Of course, such disclosures would likely violate the Safe Harbor, which requires that self-certified U.S. companies inform the EU of such requests for personal data. Accordingly, U.S. companies may find themselves with a Hobson's choice of violating either the USA PATRIOT Act or the EU Data Protection Directive.[420]

Even something as routine as an electronic interoffice telephone directory for a multi-national company can require significant legal compliance work to avoid violation of European privacy laws. General Motors spent six months on just such a project, working under the rubric of the Safe Harbor Program. This meant mapping where the directory might be used and by whom, notifying employees in Europe that their phone numbers would be exported to other offices and obtaining agreement of hundreds of affiliates around the world not to misuse or disclose the information.[421] Many major U.S. companies are adapting global privacy standards based on the EU model. Proctor & Gamble, Dupont and General Electric are examples.[422] Indeed, a number of corporations, such as P&G and AXA Financial Services, take the approach of complying with the strictest applicable privacy requirements.[423] (In addition to influencing major companies, the EU model has also caused numerous other countries to consider strengthening their online privacy laws.[424])

---

[420] Armstrong, Burnett and Davis, "Storms Gather for Data Protection in the Cloud," CMS Cameron McKenna (Aug. 16, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=8089feda-5f7f-4a0b-b75d-0f83dba64130. In its 2012 *Opinion on Cloud Computing*, discussed *supra*, the Article 29 Working Group expressed doubt that the U.S.-EU Safe Harbor Framework would adequately protect EU data stored with U.S.-based cloud service providers.

[421] D. Scheer, "Europe's New High Tech Role: Playing Privacy Cop to the World," WALL STREET JOURNAL (October 10, 2003), *available at* http://cryptome.org/eu-data-cop.htm.

[422] *Id*.

[423] See L. Conley, "Refusing to Gamble on Privacy," Fast Company, No. 84 (June 2004), http://www.fastcompany.com/magazine/84/essay_hughes.html; J. Vijayan, "Privacy Potholes," COMPUTERWORLD (March 15, 2004), http://www.computerworld.com/printthis/2004/0,4814,91108,00.html).

[424] According to Steptoe & Johnson, *E-Commerce Law Week* (Aug. 28, 2008), new data protection requirements were being considered in Australia, Mexico, Turkey, South Korea, Peru and Vietnam, among other places. Many of these proposed laws would require mandatory notification to individuals affected by data breaches. *Available at* http://www.steptoe.com/publications-5495.html.

The EU's Data Protection Directive[425] has also led to a conflict between U.S. discovery obligations and European privacy obligations:

> Both U.S. discovery laws and E.U. data protection laws provide severe sanctions for non-compliance. Accordingly, companies subject to U.S. discovery demands for personal data located in the E.U. may find themselves between the proverbial rock and a hard place.[426]

A party's U.S. discovery obligations are found in the Federal Rules of Civil Procedure and similar state provisions that allow a party to request non-privileged information germane to a claim or defense.

Conversely, the Data Protection Directive places "severe restrictions in the processing of personal data."[427] Specifically, "for documents within the scope [of the EU Directive], compliance with EU law will typically require a basis under EU law for (1) collection; (2) disclosure; and (3) analysis in the EU; a basis for (4) transfer to the U.S.; and a basis for (5) analysis; (6) disclosure; and (7) use in the U.S."[428] Some authors believe that one solution to finding a basis for transferring the information out of the EU into the U.S. may be compliance with the safe harbor procedures described above.[429] But it is unclear if bases exist under EU law to satisfy the other six requirements. For example, EU law would allow disclosure of private data in certain circumstances such as where dissemination is a "necessity."[430] One "necessity" is for compliance with a legal obligation imposed by EU member state law or international law. But it is questionable whether a discovery obligation arising U.S. rules would be sufficient.[431] And other grounds for disclosure under the Directive are unlikely to provide a route for enforcement of the discovery requirements.[432] Accordingly, "it may be quite difficult, and even impossible to comply with both U.S. and E.U. law [in] collecting documents …."[433]

If U.S. case law is a guide, courts grappling with a conflict between U.S. discovery rules and foreign privacy laws may engage in a form of interests balancing.[434] However, a U.S. federal

---

[425] Directive 95/46/EC. The Directive governs "processing" and "exporting" of "personal data." "Personal data" is defined broadly under the Directive, i.e., "any info relating to an indentified or identifiable natural person." *Managing the EU-U.S. Discovery Conflict*, http://www.law360.com/articles/72082/managing-the-eu-us-discovery-conflict (Oct. 16, 2008).

[426] *U.S. Discovery and E.U. Privacy: Irresistible Force vs. Immovable Object?*, WORLD DATA PROTECTION REPORT (BNA) 19 (Jan. 2008). *See also* R. Davis, *European Privacy Laws An E-Discovery Stumbling Block*, Law360 (July 23, 2009), *available at* http://www.law360.com/articles/112287.

[427] *U.S. Discovery and E.U. Privacy: Irresistible Force vs. Immovable Object?*, WORLD DATA PROTECTION REPORT (BNA) 19 (Jan. 2008).

[428] *Id.*

[429] *Id.*

[430] *Id.*

[431] *Id.*

[432] *Id.*

[433] *Id.*

[434] *Id.* at 21, citing *Volkswagen, AG v. Valdez*, 909 S.W.2d 900 (Tex. 1995) (balancing the factors set forth in Section 442 of the Restatement (Third) of Foreign Relations Law); *Société Nationale v. Rogers*, 357 U.S. 197 (1958) (balancing the Congressional intent underlying the Trading with the Enemy Act with more protective Swiss privacy laws); *Richmond v. Timer Falling*, 959 F.2d 1468 (9th Cir. 1992) (balancing the factors set forth in Section 442 and applying the *Société Nationale* standard); *Strauss v. Credit Lyonnais*, 2000 Dist. LEXIS 38378 (E.D.N.Y. May 25, 2007) (balancing the factors set forth in Section 442 and denying the plaintiff's request for bank records as prohibited by French privacy laws). The factors set forth in Section 442 are (1) the importance to the investigation or litigation of the information; (2) the degree of specificity of the request; (3) whether the info originated in the

district court has held that E.U. requirements to delete user data once it is no longer necessary for legitimate business purposes do not excuse companies from their U.S. electronic evidence preservation obligations.[435]

In the Americas, U.S. litigants seeking to acquire information from a Mexican party will face new hurdles with the recent amendment to Article 16 of the Mexican Constitution concerning privacy protection, which was modeled after the Spanish Data Protection Law promulgated in response to the EU Data Protection Directive.[436] Accordingly, U.S. litigants will likely face similar complications where discovery requires the disclosure of the personal information of Mexican citizens. Uruguay's privacy law, an opinion recently made public by the EU's Article 29 Working Party determined, are on par with the EU Data Protection Directive.[437]

Meanwhile, in 2011 Israel received a determination from the European Commission that Israel's data protections laws are in conformance with the EU Data Protection Directive.[438] The Commission has so far recognized Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, the U.S. Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Records to the United States' Bureau of Customs and Border Protection as providing adequate protection.[439]

Finally, and as if the foregoing was not enough to consider, the European Commission in early 2012 released onerous draft data protection rules that would entirely repeal and overhaul nearly two-decade old data protection framework (i.e., the EU Data Protection Directive) currently in place.[440] The proposed rules included provisions to regulate privacy and data protection from the EU level as well as a Directive, in contrast with the current Directive alone, which leaves the task of regulation implementing legislation in individual Member States. The new proposal would increase penalties for violations, allowing fines of up to €1 million or 2% of

---

U.S.; (4) the availability of alternative means for securing the info; and (5) the extent noncompliance would undermine foreign interests. *Id.*

435 *IO Group Inc., et al. v. GLBT Ltd., et al.*, No. C-10-1282 MMC (DMR), 2011 U.S. Dist. LEXIS 120819 (N.D.Cal. 2011) (holding that a British website operator's destruction of e-mails in accordance with the U.K. Data Protection Act of 1998 would not excuse noncompliance with U.S. laws regarding spoliation), *reported in* "EU Privacy Law is No Excuse for Spoliation of Evidence," Steptoe & Johnson LLP E-Commerce Law Week (Issue 683, Nov. 19, 2011), *available at* http://www.steptoe.com/publications-7896.html.

436 "Mexico's Constitution: for US Litigation Involving Mexican Entities, New Data Protections Could Create New Hurdles," *available at* http://www.dlapiper.com/latinamerica/publications/detail.aspx?pub=4469.

437 "Uruguay's and Israel's Data Privacy Laws: Good Enough for Europe," *reported in* Steptoe & Johnson LLP E-Commerce Law Week (Issue 629, Week Ending October 30, 2010) *available at* http://www.steptoe.com/publications-7240.html.

438 *See Commission Decision*, 2011/61/EU (31 Jan. 2011) (pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:EN:PDF.

439 *See* "Commission decisions on the adequacy of protection of personal data in third countries," E.C., *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

440 European Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, *supra* note 392; *see also* Keating, "Draft Regulation Prepared by the European Commission Proposes Fundamental Changes in European Union Privacy and Data Security Standards," Alston Privacy and Security Blog (Dec. 5, 2011), *available at* http://www.alstonprivacy.com/blog.aspx?entry=4485. Among other things, the proposed data rules would clarify the standards for obtaining and using subject data; limit permitted processing of personal data to the minimum amount necessary; contain a new right to be "forgotten" (i.e., have one's personal information erased upon demand); and contain new data breach notification standards. *Id*.

a company's annual turnover; provide a "right to be forgotten" that would permit individuals to demand the deletion of records about them; impose data breach reporting requirements; and increase regulation of sensitive areas, such as data mining, health end epidemiological data, genetic and biometric data and closed circuit television video. Moreover, the proposed rules would apply to any company based outside the EU which provides goods and services to EU residents.[441] The Commission's proposal was sent to the European Parliament and Member States for consideration, and the rules would take effect two years after adoption.[442] In 2013, the privacy reforms were still being negotiated and debated, including reported lobbying efforts by the U.S. FTC to encourage the interoperability and consistency of trans-Atlantic rules.[443] By 2014, the EU reported that the European Parliament had voted in favor of the Directive.[444] However, implementation of the reforms has been delayed by the current political climate in the EU, as well as differing views of certain member states as to the effects of the Directive as enacted.[445] Nevertheless, in an unexpected decision, the European Court of Justice interpreted the "right to be forgotten" proposal to permit individuals to request that search engines remove links to out of date or inaccurate news articles, court judgments and other documents in search results for their name.[446] In keeping with this interpretation, the EU Court held that an internet search engine operator could be required to remove links to outdated information that was prejudicial to an objecting individual, even though the information was lawfully published in the first instance, so that the website containing the prejudicial information could not itself be required to remove it.[447]

2. *U.S. Online Privacy Regulation*

a. Federal Trade Commission Regulation

Events in recent years suggest that the American regulators' laissez-faire approach to consumers' privacy may be coming to an end.[448] The Federal Trade Commission has become the

---

[441] Goetz, "A new world of EU data protection," Faegre Baker Daniels (Feb. 2, 2012) (also reporting that all such non-EU companies would have to appoint a representative in the EU unless it employs fewer than 250 workers), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=60b40d08-486a-41a5-8c72-8cf40e1278bb.

[442] *See supra* note 441.

[443] *Reported in* Frances Robinson, *U.S. to EU: U.S. Data Law is Brill*, Wall Street Journal (April 19, 2013), *available at* http://blogs.wsj.com/brussels/2013/04/19/u-s-to-eu-u-s-data-law-is-brill/.

[444] *See* Press Release, European Commission, Progress on EU data protection reform now irreversible following European Parliament vote, Mar. 14, 2014, *available at* http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

[445] *Power struggles delay EU data protection reform*, Deutsche Welle, May 13, 2014, *available at:* http://www.dw.de/power-struggles-delay-eu-data-protection-reform/a-17631222.

[446] *See* James Kanter and Mark Scott, *Google Must Honor Requests to Delete Some Links, E.U. Court Says*, N.Y. TIMES, May 13, 2014, *available at* http://www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html?_r=0; *see also* Press Release, Court of Justice of the European Union, May 13, 2014, *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

[447] ECJ Judgment of 13 May 2014, Case C-131/12 – *Google Spain et al. v. Agencia Española de Protección de Datos*, *available at* http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d54a440110b07142bfb156c5e5ae3a69c1.e34KaxiLc3eQc40LaxqMbN4OaNmNe0?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=298949

[448] This evolution in consumer privacy is further evidenced by the fact that insurers offer CyberSecurity policies for the purpose of covering losses arising from data security breaches. *See, e.g.*, www.chubb.com/businesses/cs/chubb822.html.

principal federal agency enforcing privacy concerns, under its mandate to regulate unfair or deceptive practices. The FTC in June 1998 issued "Privacy Online: A Report to Congress,"[449] asserting four core principles of fair information practice: "that consumers be given *notice* of an entity's information practices; that consumers be given *choice* with respect to the use and dissemination of information collected from or about them; and that the consumers be given *access* to information about them collected and stored by an entity; and that the data collector take appropriate steps to insure the *security* and integrity of any information collected."[450] A similar FTC report to Congress in 2000 emphasized the same four key elements known as the Fair Information Practice Principles.[451]

These four principles also led to the FTC's February 2009 Self Regulatory Principles for Online Behavioral Advertising and the implementation of the "Do Not Track" mechanism in 2010 (described below). According to the FTC, "behavioral advertising is the tracking of a consumer's activities online – including the searches the consumer had conducted, the Web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests."[452] The Self-Regulatory Principles also include four key principles: (i) every website where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that data is being collected to provide ads targeted to the consumer and give consumers the ability to choose whether or not to have their information collected for such purpose; (ii) any company that collects or stores consumer data for behavioral advertising should provide reasonable security for that data and should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need; (iii) companies should obtain affirmative express consent from affected consumers before using data in a manner materially different from promises the company made when it collected the data; and (iv) companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising.[453]

In March 2012, the Obama administration, with the FTC's support, called on Congress to codify and establish a "Consumer Privacy Bill of Rights."[454] The proposed Bill of Rights articulates seven broad principles to address online privacy challenges:

- Individual Control. Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency. Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context. Consumers have a right to expect that companies will collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data.

---

449 See www.ftc.gov/reports/privacy3/priv-23a.pdf.

450 1998 Privacy Report, at Executive Summary (emphasis in original).

451 *See* www.ftc.gov/reports/privacy2000/privacy2000.pdf; www.ftc.gov/reports/privacy2000/pitofskystmtonlineprivacy.html.

452 *FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising, February 2009, available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

453 *Id*.

454 *Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, the White House (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

- Security. Consumers have a right to secure and responsible handling of personal data.
- Access and Accuracy. Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- Focused Collection. Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Accountability. Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

And in February 2013, the FTC issued non-binding guidelines, "Mobile Privacy Disclosures: Building Trust Through Transparency," which aim to encourage privacy disclosures from companies in the mobile marketplace.[455]

However, given the current partisan atmosphere in Washington, D.C., the prospects of Congress passing legislation to enact the FTC's guidance remain unclear; consumers may have to rely on industry group standards and FTC enforcement action to protect online privacy.[456]

b. FTC Enforcement Actions and Developments

In 2001, then FTC Chairman Timothy Muris outlined the FTC's current and future privacy initiatives and announced the FTC's plan to increase resources devoted to protecting consumer privacy by 50%.[457] Among the issues on the FTC's pro-privacy agenda are enforcing the privacy promises posted on websites,[458] investigating complaints of U.S. companies failing to provide privacy protections they had promised under the European Safe Harbor Principles and encouraging strong security for personal information collection.

FTC activities have included an announcement that, in the absence of clear statements to the contrary, a company's online privacy policy would be considered to apply equally to a company's offline collection and use of data,[459] and its settlement of charges against two

---

[455] *Available at* http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm. Among other things, the staff report makes a series of recommendations to mobile marketplace companies, including providing just-in-time disclosures; obtaining affirmative express consent to collect sensitive personal information; making accurate privacy disclosures multiple times; cooperating with other stakeholders to develop a do-not-track function; ensuring business partners have satisfactory privacy practices; and complying with self-regulatory and trade group programs.

[456] For instance, several prominent Internet companies, including Google, Microsoft and Yahoo, have entered into an agreement to voluntarily create a "Do Not Track" button to opt out of behavioral tracking and block cookies. The agreement will be enforced by the FTC. Sasso, *Google, Microsoft, Yahoo aim to defuse privacy issue with 'Do Not Track' button*, The Hill (Feb. 23, 2012), *available at* http://thehill.com/blogs/hillicon-valley/technology/212257-google-microsoft-yahoo-aim-to-defuse-privacy-issue-with-commitments.

[457] *Protecting Consumers' Privacy: 2002 and Beyond: Remarks of FTC Chairman Timothy J. Muris*, at The Privacy 2001 Conference, Oct. 4, 2001, available at http://www.ftc.gov/speeches/muris/privisp1002.htm.

[458] One example of such a case is noteworthy because of its bankruptcy context. The FTC sued to enjoin the bankrupt Toysmart from selling, in bankruptcy, its customers' personal information in violation of its privacy policy promise never to share that information. *FTC v. Toysmart.com*, Civ. No. 00-1134-RGS (D. Mass., filed July 10, 2000). A settlement would have permitted transfer of the customer data to a purchaser who bought the entire business; otherwise, the data was to be destroyed. The bankruptcy court did not approve the settlement, finding it unduly restrictive, but left the door open for objections, the FTC once a potential buyer was on the scene.

[459] *See* WORLD DATA PROTECTION REPORT (BNA) (January 2002) at 17.

companies that collected personal data from high school students and sold them to commercial marketers despite promises not to do so.[460]

The FTC has also acted against Gateway Learning Corp., the publisher of "Hooked on Phonics," for changing its privacy policy to allow it to share customers' personal information, in violation of an explicit promise in its former policy, and then applying the looser standard to customers without affording them the opportunity to opt out. The settlement forbids Gateway from applying changes to its privacy policy retroactively without the affirmative opt-in consent of the affected customers, and to disgorge the $4,600 it gained from renting its customer data.[461]

In early 2002, the FTC settled an action against Eli Lilly and Co. for alleged inadvertent violation of its privacy policy.[462] A Lilly employee had unintentionally sent an e-mail to all subscribers to a Prozac-related e-mail service, placing their e-mail addresses in the "To:" field, and thereby making the addresses visible to all. The FTC charged that Lilly's inadequate internal security procedures rendered its privacy policy deceptive. The settlement required implementation of a security program to protect consumer's personal information from reasonably foreseeable threats to its security, confidentiality or integrity and from unauthorized access, use or disclosure.

Also in 2002 the FTC settled charges with Microsoft that alleged that it had misled consumers as to the security and privacy of personal information in its Passport online authentication system.[463] While no actual security breaches had been found in the FTC's investigation, the security claims that Microsoft had made were not substantiated – a standard like that for any advertising claims. Similarly, when retailer Guess Inc. failed to block a well-known security hole on its website, exposing some 200,000 customer names and credit card numbers to those who know how to exploit the vulnerability, the FTC brought charges that Guess had violated its privacy policy, which claimed that credit and numbers were "stored in an unreadable, encrypted format at all times." Guess settled, agreeing to adopt a comprehensive security program, including independent audits.[464] A similar case was settled in 2004 by Tower Records and Petco Animal Supplies, with a similar security program required by the FTC.[465] And in December 2005, DSW, Inc., the shoe retailer settled charges by the FTC that security failures that gave hackers access to customer credit card and checking account data were an unfair practice in violation of the FTC Act.[466] Perhaps the most notorious security breach involved data broker ChoicePoint Inc. in early 2005, in which criminals gained access to tens of thousands of names and associated personal information. In early 2006, ChoicePoint settled with the FTC, agreeing to pay a $10 million fine and establish a $5 million fund for consumer redress, as well

---

460 *National Research Center for College and University Admissions*, FTC No. 022 3005 (Oct. 2, 2002) *reported in* 83 ANTITRUST & TRADE REG. REP. (BNA) 316 (Oct. 4, 2002).

461 *Gateway Learning Corp.*, FTC File No. 042-3047, Trade Cas. (CCH) ¶15,617 (2004).

462 *In re Eli Lilly and Co.*, FTC No. 0123214 (Jan. 18, 2002) *reported in* WORLD DATA PROTECTION REP. (BNA) at 12.

463 83 Antitrust & Trade Reg. Rep (BNA) 137, 193 (2002). The European Commission had undertaken a similar investigation. "Microsoft Faces European Commission Inquiry on Privacy Concerns," N.Y. TIMES (May 28, 2002) at p. C4.

464 Guess?, Inc. and Guess.com, FTC Docket No. C-11091 (July 30, 2003); *see* B. Tedeschi, "F.T.C. Increases Focus on Privacy," N.Y. TIMES (June 30, 2003), http://www.nytimes.com/2003/06/30/technology/30ECOM.html.

465 "Pet Shop's Data Security Breached Own Privacy Policy," (Nov. 19, 2004), http://www.out-law.com*; MTS, Inc. d/b/a/ Tower Records*, FTC Docket No. C-4110 (June 2, 2004).

466 FTC File No. 052-3096 (December 1, 2005), complaint, agreement, press release and related documents available at http://www.ftc.gov/os/caselist/0523096/0523096.htm.

as to implement procedures to ensure that consumer data is released only to those with a permissible purpose under the Fair Credit Reporting Act, and to establish a comprehensive data security program with biennial third party audits for twenty years. And in May 2006, the FTC settled with a real estate services company that had promised to maintain "physical, electronic and procedural safeguards" to protect consumer data, but then threw consumer loan applications in a dumpster and failed to maintain adequate computer security, thereby allowing a hacker to gain access to the company's computer network where consumer information was stored. The settlement required adoption of a comprehensive security program an biennial independent audits over a twenty-year period.[467]

In 2008 the FTC took action against Life is Good, Inc. ("LIG") in connection with its failure to deliver on promises made in its online privacy statement. Specifically, LIG promised to store consumer data in a "secure file." In practice, however, LIG failed to encrypt the information and a hacker was able to steal sensitive personal data on thousands of consumers. After an investigation, the FTC filed a complaint[468] against LIG, alleging it engaged in deceptive practices. While LIG settled[469] with the FTC, the action further underscores the Commission's active role in the preservation of online consumer information security.

Similarly, in 2008 the FTC also took action against TJX – the parent company of T.J. Maxx and Marshalls – for its "failure to employ reasonable and appropriate security measures to protect personal information…."[470] TJX's alleged failure to develop sufficient security measures (such as limiting access to its network, using stronger passwords and firewalls, and conducting security investigations) led to a hacker obtaining tens of millions of credit and debit card numbers, resulting in millions of dollars in fraudulent charges. As a consequence, the FTC claimed TJX engaged in unfair acts or practices in violation of Section 5(a) of the Federal Trade Commission Act.[471] The action resulted in a settlement, pursuant to which TJX has agreed, among other things, to be subject to 20 years of independent security monitoring. Notably, the TJX action was coordinated with the attorneys general of 39 states.[472] The breach also resulted in private class action suits.[473]

In 2009, the FTC ordered Sears to destroy all of the customer data that it had collected through the unfair use of online tracking software.[474] According to the FTC, Sears failed to

---

467 Press Release, "Real Estate Services Company Settles Privacy and Security Charge," Federal Trade Commission (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/nationstitle.htm; *Matter of Nations Titel Agency, Inc., Nations Holding Company and Christopher M. Likens*, File No. 052 3117.

468 *In Re Life is Good, Inc.*, FTC Docket No. C-4218 (April 2008); complaint *available at* http://www.ftc.gov/os/caselist/0723046/080418complaint.pdf.

469 Consent Order *available at* http://www.ftc.gov/os/caselist/0723046/080117agreement.pdf. The settlement includes 20 years of FTC monitoring and oversight.

470 *See* Complaint, *In Re The TJX Companies, Inc.*, FTC Docket No. C-4227 (July 2008); agreement, press release and related documents *available at* http://www.ftc.gov/os/caselist/0723055/index.shtm.

471 15 U.S.C. § 45(a).

472 *See* http://www.ftc.gov/os/caselist/0723055/index.shtm.

473 *See* Steptoe and Johnson, *E-Commerce Law Week* (Feb. 10, 2007, May 12, 2007, Oct. 6, 2007 and Dec. 8, 2007), *available at* http://www.steptoe.com; "Mass. AG leads multistate probe into TJX breach," COMPUTERWORLD (Feb. 8, 2007), http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010884&source=NLT_PM&nlid=8.

474 *In re Sears Holdings Management Corporation*, FTC Docket No. 082-3099 (June 2009); complaint, agreement, press release and related documents *available at* http://www.ftc.gov/os/caselist/0823099/index.shtm.

adequately disclose the scope of its tracking software's data collection. Although Sears customers were warned that software would track their browsing, the software actually tracked the customers' browsing on third-party websites and collected personal information transmitted during secure sessions. Sears settled the case with the FTC and agreed to inform users clearly and prominently, before downloading any software, what data would be collected. The Sears settlement represents "a warning shot to companies that thought their privacy policies protected them" and indicates a significant shift in the FTC's enforcement policies.[475] More recently, in an FTC action that was settled with LifeLock, Inc., the FTC outlined particular preventive security measures that LifeLock failed to take, which the FTC may deem standard protocol going forward.[476]

In 2010, the FTC settled charges with Dave & Busters stemming from the FTC's accusations that the company left 130,000 consumers' credit and debit card information vulnerable to hackers, resulting in fraudulent charges.[477] Specifically, the company allegedly failed to detect and prevent unauthorized access to its network, monitor and filter outbound data traffic, and use available security measures to limit access to its computer networks. As a condition of the settlement, Dave & Busters agreed to put into place a comprehensive information security program. Moreover, the company must obtain professional audits every other year for ten years to ensure the security of its systems.

Also in 2010, the FTC intervened in a bankruptcy case where customer data collected online was in the process of being sold in violation of established privacy policies and reached a settlement precluding disclosure.[478] In a separate FTC action, the agency mandated a series of

---

[475] *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES (August 4, 2009), *available at* http://www.nytimes.com/2009/08/05/business/media/05ftc.html. For an additional discussion of the potential changes in the FTC's enforcement policies under Mr. Vladeck, *see An Interview With David Vladeck of the F.T.C.*, N.Y. TIMES (August 5, 2009), *available at* http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc.

[476] *See* E-COMMERCE LAW WEEK (March 20, 2010), *available at* www.steptoe.com/E-CommerceLawWeek. According to the FTC, LifeLock engaged in a number of practices that failed to provide appropriate security. Among them, the FTC said that LifeLock: "[c]reated an unnecessary risk to personal information by storing it on the network and transmitting it over the network and the internet in clear readable text; [f]ailed to require employees, vendors, and others with access to personal information to use hard-to-guess passwords or to implement related security measures, such as periodically changing passwords or suspending users after a certain number of unsuccessful log-in attempts; [f]ailed to limit access to personal information stored on or in transit through its networks only to employees and vendors needing access to the information to perform their jobs; [f]ailed to use readily available security measures to routinely prevent unauthorized access to personal information, such as by installing patches and critical updates on its network; [d]id not adequately assess the vulnerability of the network and web applications to commonly known and reasonably foreseeable attacks, such as SQL injection attacks; [f]ailed to employ sufficient measures to detect and prevent unauthorized access to the corporate network or to conduct security investigations, such as by installing antivirus or anti-spyware programs on computers used by employees to remotely access the network or regularly recording and reviewing activity on the network; [d]id not implement simple, low-cost, and readily available defenses to commonly known and reasonably foreseeable attacks; and [f]ailed, from at least December 2006 until February 2007, to secure paper documents containing personal information that were received by facsimile in an open and easily accessible area." *See LifeLock, Inc.*, FTC File No. 072 3069 (2010); complaint *available at* http://www.ftc.gov/os/caselist/0723069/index.shtm.

[477] *In the Matter of Dave & Busters, Inc.*, FTC File No. 082 3153 (2010). The FTC's press release concerning the settlement is *available at* http://www.ftc.gov/opa/2010/03/davebusters.shtm.

[478] On August 3, 2010, in response to the FTC's concerns, the U.S. Bankruptcy Court for the District of New Jersey approved the parties' settlement agreement that stipulated that bankrupt XY magazine's personal data of 500,000 to 1,000,000 subscribers would be destroyed and not be subject to acquisition by the purchaser. Kurana, "When You Wrote Your Privacy Policy, Were you Thinking About 'The End'?" *reported in* Lexology (August 25, 2010)

data security procedures for three resellers of consumer reports that failed to safeguard adequately consumers' personal information on their clients' networks, suggesting that companies are not only responsible for security lapses in their own networks, but may also be responsible for lapses on their customers' networks, at least where the companies fail to take appropriate steps to secure the personal information they maintain and sell.[479] Additionally, the micro-blogging service Twitter agreed to implement a new security program and submit to a security audit from a third party as part of a settlement agreement with the FTC over security breaches the company experienced in 2009.[480]

Most recently, in what will surely go down as a landmark ruling in the area of data security enforcement power by governmental authorities in the United States, the United States District Court for the District of New Jersey held that the FTC's enforcement powers under Section 5 of the FTC Act extends to data breaches.[481] With this confirmation of the FTC's authority in this area, their brethren at the state level may well seek monetary relief from violators of state unfair and deceptive trade practices statutes similar to the FTC Act, as well as seeking relief under state data breach notification statutes. We discuss privacy regulation at the state level in detail below.[482]

With the use of mobile apps on the rise, the FTC settled enforcement actions with two mobile app makers based upon the allegations that they misrepresented the security of their apps and transmitted sensitive user information without adequate security measures in place.[483]

In 2013, in what was probably one of the largest data breaches in history, approximately 40 million credit card numbers and 70 million addresses, phone numbers, and other pieces of personal information were hacked from Target's security and payment systems.[484] As a result, more than 90 lawsuits have been filed against the company not just by customers, but by financial institutions as well.[485] The ensuing fallout resulted in the resignation of Target's CEO, a thirty-five year veteran of the company[486] and the FTC has confirmed the company is currently under investigation.[487]

---

available at http://www.lexology.com/library/detail.aspx?g=d5409488-5030-4c00-97c7-55e78faea847.

[479] The three companies were SettlementOne Credit Corp, ACRAnet Inc., and Statewide Credit Services. *In the Matter of ACRAnet, Inc.*, File No. 0923088, documents available at http://www.ftc.gov/os/caselist/0923088/index/shtml. *See also "FTC Holds Consumer Report Resellers Responsible for 'Downstream' Data Protection Failures" reported in* Steptoe & Johnson LLP E-Commerce Last Week (Issue 643, Week Ending February 12, 2011), *available at* http://www.steptoe.com/publications-7399.html.

[480] http://www.wired.com/threatlevel/2010/06/twitter-settles-with-ftc/; *See also* Kim and Serwin, "FTC Reaches a Settlement With Twitter Regarding Privacy Breaches," *reported in* Lexology (March 15, 2011), *available at* http://www.lexology.com/library/detail.aspx?g=1d403f94-38ec-4e71-a370-038283be5106. As an aside, in May 2010 a fake account which posted tweets under the name of "BPGlobalPR" was created in Twitter. BP knows about the account and is not happy about it, but a few of the tweets are available at http://bit.ly/btrTql.

[481] *F.T.C. v. Wyndham Worldwide Corp.*, CIV.A. 13-1887 ES, 2014 WL 1349019 (D.N.J. Apr. 7, 2014).

[482] *See infra* section c.

[483] *In re Fandango LLC*, File No. 132 3089 Agreement Containing Consent Order, Mar. 28, 2014, *available at* http://www.ftc.gov/system/files/documents/cases/140328fandangoorder.pdf; *In re Credit Karma*, File No. 132 3091 Agreement Containing Consent Order, Mar. 28, 2014, *available at* http://www.ftc.gov/system/files/documents/cases/140328creditkarmaorder.pdf.

[484] http://www.businessweek.com/printer/articles/189573-missed-alarms-and-40-million-stolen-credit-card-numbers-how-target-blew-it.

[485] *Id.*

[486] http://bigstory.ap.org/article/targets-chairman-and-ceo-out-wake-breach.

[487] http://www.usnews.com/news/articles/2014/03/26/ftc-investigates-target-data-breach.

The FTC has also been active in investigating whether various companies' online marketing programs violated Section 5 of the FTC Act.

First, an official Netflix contest – which allowed contestants access to 480,000 "anonymous" Netflix's users' data – was under investigation because some of the competitors were able to identify certain users based upon their viewing histories and preferences.[488] Then-FTC Commissioner Pamela Jones Harbour indicated that the FTC will be more actively involved in combating companies' privacy-violating online marketing programs in the future.

In March 2011, Google agreed to settle with the FTC over its Google Buzz social networking program, which automatically made users' Gmail and chat contacts public and created difficulty and uncertainty among users as to how they could limit the sharing of their personal information and opt to leave the social network.[489] The FTC also alleged that Google misrepresented its treatment of personal information from the European Union, and that it falsely claimed to adhere to the Safe Harbor principles of the US-EU Safe Harbor privacy framework. The landmark settlement was the first time the FTC has required a company to implement a comprehensive privacy program to protect the privacy of consumers' information.[490] The peace between Google and the FTC was short-lived, however. In August 2012, the FTC filed a complaint alleging that Google had violated the settlement by misrepresenting to users of Apple Inc.'s Safari Internet browser that they would be automatically opted-out of receiving tracking "cookies" or served with targeted ads.[491] Notably, the FTC further alleged that Google violated the 2011 settlement by misrepresenting that it would comply with industry group "compliance programs," such as Network Advertising Initiative's (NAI) self-regulatory code of conduct (which requires members to "clearly and conspicuously post notice on its website that describes its data collection"). Although Google denied the allegations, it quickly agreed to disable all tracking cookies and pay a $22.5 million civil penalty – the largest civil fine in FTC history for a consent order violation.

In December 2011, Facebook agreed to settle FTC charges of deceptive trade practices stemming from the company's sharing of user information without consent. Under the terms of the settlement, Facebook agreed to make substantial changes to its privacy policies and to undergo related audits for 20 years.[492] The FTC gave final approval to the settlement in August 2012.[493]

In late 2011 the FTC also settled charges with ScanScout after alleging that the company's privacy policy contained false and misleading statements. Specifically, ScanScout's privacy policy stated that users could opt-out of receiving cookies, which was accurate with

---

[488] Baker, "Think about the privacy implications of that clever marketing plan," Wiley Rein LLP, *reported in* Lexology (April 6, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=64d71eae-a6cc-4f00-a15b-ed6664410ea7. Netflix has announced a settlement of the FTC's investigation and a class action lawsuit (*In re: Netflix Privacy Litigation*, No. 5:11-CV-00379 (N. Dist. Cal)) stemming from the allegedly improper disclosures. Netflix has agreed to pay up to $9,000,000 to settle the class action suit.

[489] "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network" *available at* http://www.ftc.gov/opa/2011/03/google/shtm.

[490] *Id.*

[491] *U.S. v. Google, Inc.*, FTC Docket No. C-4336; press release, complaint, and consent decree *available at* http://ftc.gov/opa/2012/08/google.shtm.

[492] "Facebook Settles FTC Changes Over Unfair and Deceptive Privacy Practices," Steptoe & Johnson LLP E-Commerce Law Week (Issue 686, Dec. 10, 2011), *available at* http://www.steptoe.com/publications-7924.html.

[493] *See* FTC press release, *available at* http://www.ftc.gov/opa/2012/08/facebook.shtm.

respect to traditional HTTP cookies, but not Flash cookies.[494] The FTC seems to be seeking to promote online consumer privacy through enforcement actions targeting deceptive or misleading privacy policies.

MySpace's privacy policy was the subject of a 2012 FTC complaint, which alleged that the social networking service misrepresented the protections afforded to users' personal information.[495] Specifically, the FTC charged that, contrary to MySpace's written policy that it would not share users' personal information, MySpace provided advertisers with certain users' unique "Friend ID", with which the advertisers could then locate a user's MySpace profile to obtain personal information. MySpace ultimately settled with the agency, agreeing, among other things, to implement a new comprehensive privacy policy and to be subject to regular, independent privacy audits for the next 20 years.

The FTC has required designated personnel to be responsible for information security, identification of security risks, implementation of security safeguards to control those risks and ongoing monitoring of the security program for effectiveness.[496] Similar approaches appear in the information security guidelines adopted as Recommendations by the Organization for Economic Cooperation and Development Council on July 25, 2002[497] and the FTC's final rule establishing information security standards for customer information under the Gramm-Leach-Bliley Act,[498] discussed below in Section I.I.3.b.iii., and the HIPAA security standards, discussed below in Section I.I.3.c.

Another FTC Rule, effective in 2005, requires businesses and individuals to destroy all private consumer information (whether in electronic or paper form) obtained from credit bureaus and other information sources for credit, leasing or employment purposes.[499] In 2007, the FTC proposed guidelines urging advertisers to disclose voluntarily the extent to which they monitor online conduct and personalize ads using that data.[500]

In 2010, the FTC proposed the implementation of a "Do Not Track" mechanism so that consumers can choose whether to allow the collection of data regarding their online searching and browsing activities.[501] This "Do Not Track" mechanism is intended to simplify consumer choices about, and make more transparent to consumers, the information practices of website operators as to personal information they collect about consumers and their online activity for advertising or other purposes. The report calls for companies to include reasonable security for

---

494 Bhargava and Heidelberger, "Online Advertiser settles with FTC for Use of Flash Cookies without Adequate Disclosure," Winston & Strawn LLP (Nov. 9, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=a23af29d-a860-4a77-9557-58238f0695d0.

495 *In the Matter of Myspace LLC*, FTC File No. 102 3058 (2012). The FTC also alleged that MySpace misrepresented that it was in compliance with the U.S.-EU Safe Harbor. The FTC's press release and complaint, and the consent order, are *available at* http://ftc.gov/opa/2012/09/myspace.shtm.

496 83 Antitrust & Trade Reg. Rep (BNA) 137 at 194.

497 *See* www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html.

498 *See* www.ftc.gov/opa/2002/05/safeguardrule.htm.

499 16 C.F.R. Part 682 (2005).

500 "Online Behavioral Advertising – Moving the Discussion Forward to Possible Self-Regulatory Principles," Statement of the Bureau of Consumer Protection (Dec. 20, 2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

501 "FTC Staff Issues Privacy Report Offers Framework for Consumers, Businesses, and Policymakers" *available at* http://www.ftc.gov/opa/2010/12/privacy.shtm.

consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy. Moreover, the report states that consumers should be presented with choice about the collection and sharing of their data at the time and in the context in which they are making decisions, and not after having to read long, complicated disclosures that they often cannot find.[502]

These developments demonstrate that a company's consumer privacy initiatives cannot begin and end with the issuance of a privacy policy. First, the company must do what it says – the privacy policy is an enforceable promise. Even in the face of a subpoena, a company may not be permitted to disclose customer data, at least without notice and an opportunity to opt out.[503]

Second, businesses must actively review and monitor their offline and online privacy programs and take appropriate measures to preclude unauthorized access to or dissemination of its customers' private information, even inadvertently. The Yale University admissions database, protected in 2002 only by the applicants' social security number, and thus accessible to a wayward Princeton admissions officer,[504] seems plainly inadequate, for example. Another area of concern is outsourced data processing. The experience of one medical transcription firm is illustrative of the risks. Transcription services outsourced by the University of California San Francisco Medical Center, and then subcontracted twice more, found their way to Pakistan, where a transcriber who asserted she had not been paid for her services threatened to post patient records on the Internet if she was not paid.[505]

The law of privacy thus has developed to include a requirement for data security, in the form of an ongoing process of risk assessment, development of a security program to address the risks identified, monitoring and testing to ensure effectiveness, and continual review and adjustment in light of changes in risks identified. The program should be audited regularly, and must include oversight of any third party service providers who are given access to private information.[506]

Finally, recognizing that security will never be perfect, plans to respond when breaches occur are essential. The FTC itself acknowledges that "breaches can happen…."[507] A Deloitte Touche Tohmatsu survey found in 2006 that 78% of the world's top 100 financial services firms suffered a security breach from outside the organization in the last year,[508] and another survey

---

[502] In testimony before the Senate Committee on Commerce, Science and Transportation, the FTC told Congress that, in response to the "Do Not Track" report, two of the major Internet browsers (Microsoft and Mozilla) have recently announced the development of new choice mechanisms for online behavioral advertising that seek to provide increased transparency, greater consumer control, and improved ease of use. *"FTC Testifies Before Senate Commerce Committee on Privacy; Industry Efforts to Implement 'Do Not Track' System Already Underway"* www.bespacific.com.

[503] *See Union Planters Bank, N. A. v. Gavel*, 2003 WL 1193671, 2003 U.S. Dist. LEXIS 3820 (E.D. LA. 2003), *rev'd on other grounds*, 369 F.2d 457 (5th cir. 2004).

[504] *See* J. Schwartz, "Surveillance 101—Privacy vs. Security on Campus," N.Y. TIMES, Week in Review (Aug. 4, 2002).

[505] D. Lazarus, "A Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF Over Back Pay," SAN FRANCISCO CHRONICLE (October 22, 2003), http://sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/10/22/MNGCO2FN8G1.DTL.

[506] See T.J. Smedinghoff, "Trends in the Law of Information Security," WORLD INTERNET L. REP. (BNA) (August 2004) at 13.

[507] *Protecting Personal Information – A Guide for Business*, FTC, *available at* www.ftc.gov/infosecurity/.

[508] D.Kaplan, "Three of four financial institutions suffered external breach in past year," SC Magazine (June 14, 2006), http://www.scmagazineus.com/three-of-four-financial-institutions-suffered-external-breach-in-past-

found that 84% of 642 large North American organizations suffered a security incident in the previous year.[509] A study released in 2009 by the Ponemon Institute ("Ponemon") found that 85% of the businesses surveyed had been the victim of some form of data breach, which was an increase of 25% from the 2008 study.[510] Ponemon also conducted a study that concludes that the average organizational cost of a data breach in 2010 increased to $7.2 million and cost companies an average of $214 per compromised record, compared to $204 in 2009.[511] Furthermore, a 2010 analysis based on information provided by the Privacy Clearinghouse, a nonprofit that tracks publicly disclosed U.S. data breaches, concludes that there was nearly a 200% increase in data breaches in the United States from 2009 to 2010.[512] In its 2012 study, Ponemon noted that 94% of healthcare organizations surveyed suffered at least one data breach over the prior two years which would result in an average of $7 billion in costs annually.[513] And another study by the nonprofit Identity Theft Resource Center shows that 51% of publicly reported data breaches disclosed the total number of records compromised, and showed a total of 16.1 million records breached, not including the half of all reported data breaches that failed to reveal the number of compromised records.[514] Most recently, 91 of the 100 of the largest retail companies in the United States cited risk factors related to security breaches in their regulatory filings.[515] Plans to deal with a breach need to include notification of affected customers in compliance with state breach notification laws, discussed below, as well as remedial steps to be

---

year/article/33528/.

[509] "New Study Finds That More Than 84% of North American Enterprises Suffered a Security Breach in Past Year," CA Press (July 5, 2006), http://www3.ca.com/press/PressRelease.aspx?CID=90751&culture=en-us. *See also*, *Data Breaches Have Surpassed Level for All of '07, Report Finds* Washington Post (Aug. 26, 2008), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/08/25/AR2008082502496.html. According to the Washington Post report, 449 U.S. businesses, government departments and educational institutions have reported the loss or theft of consumer data thus far in 2008, compared with 446 breaches for all of 2007.

[510] *85 Percent of U.S. Businesses Breached*, InternetNews.com (July 13, 2009), *available at* http://www.internetnews.com/security/article.php/3829391/Report+73+Percent+of+US+Businesses+Breached.htm. More specifically, a recent data breach of Heartland Payment Systems, Inc., a payment processor in New Jersey, has affected hundreds of financial institutions in 40 states, as well as in Canada, Bermuda and Guam. S*ee* "More Than 150 Banks Affected By Heartland Data Breach Thus Far," ComputerWorld (February 11, 2009), *available at* http://www.computerworld.com/s/article/9127822/Web_site_More_than_150_banks_affected_by_Heartland_data_breach_thus_far. Similarly, Royal Dutch Shell recently suffered a massive data breach when its contact database for 176,000 employees was copied and forwarded entities and individuals opposed to the company's activities in Nigeria. *See* "Shell Hit By Massive Data Breach," The Register (February 15, 2010), *available at* http://www.theregister.co.uk/2010/02/15/shell_data_loss.

[511] "Report: 2010 U.S. cost of a Data Breach" *available at* http://www.bespacific.com/mt/archives/026771.html#026771.

[512] Vernick, "Data Breach Report Card 2010: Data Breaches up 194%, Compromised Records Down 95%," *reported in* Lexology (December 16, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=811c7c85-16af-43ee-b3ff-026e7807babb.

[513] The Ponemon Institute, *Third Annual Benchmark Study on Patient Privacy & Data Security*, December 2012, *available at* http://www.ponemon.org/library/third-annual-patient-privacy-data-security-study (registration required).

[514] http://www.infosecurity-use.com/view/14910/us-racked-up-662-reported-data-breaches-in-2010/?elq_mid=12287&elq_cid996107

[515] *See Data Breaches Growing Worry for Retailers, Report Says*, Law360 (May 16, 2014), *available at* http://www.law360.com/articles/538218/data-breaches-growing-worry-for-retailers-report-says (subscription required) and *discussed at* Press Release, "Retail Industry Growth Opportunities Fuel New Risks, BDO USA Report," BDO USA, LLP (May 14, 2014), *available at* http://www.bdo.com/news/pr/3233.

taken, such as offering free credit monitoring service. The FTC also advises that businesses designate a senior staff member to coordinate and implement a breach response plan.[516]

The Federal Communications Commission (the "FCC") and the Commerce Department have also addressed privacy and cybersecurity. The FCC recently announced the creation of a "Cybersecurity Roadmap" to identify vulnerabilities to communications networks and to develop countermeasures and solutions in preparation for, and in response to, cyber threats and attacks.[517] Such a Roadmap was recommended in the FCC's National Broadband Plan as an "initial step" toward cybersecurity. Meanwhile, the Commerce Department unveiled its own privacy framework, which proposes creation of a "Privacy Policy Office" within the Department to develop more comprehensive policies for personal data protection, a fine-tuning of current privacy protections, and FTC enforcement of voluntary industry codes of conduct.[518]

c. State Privacy Protection

Privacy regulation is not limited to the federal level. The states have entered the arena as well, both with new legislation and enforcement actions. In 2002, for example, Minnesota and North Dakota enacted new privacy laws. The Minnesota statute requires internet service providers to inform Minnesota customers if they plan to disclose personal information, including e-mail and physical addresses, telephone numbers and websites that the customer visited, what the information would be used for, and how the customer could act to prevent the disclosure, whether on an opt-out or opt-in basis.[519] North Dakota voters overwhelmingly voted in June 2002 to repeal a 2001 law allowing financial institutions to share customer data unless the customer opted out, reinstating an opt-in regime in which advance permission to share information was required.[520] Alaska, California, Connecticut, Illinois and Vermont have also adopted financial privacy legislation,[521] although the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act),[522] enacted in December 2003, revises the federal Fair Credit Reporting Act and contains provisions preempting state consumer protection laws in certain areas, including identity theft.[523]

---

[516] *Protecting Personal Information – A Guide for Business*, *supra*.

[517] "FCC Seeks Comment on Creating a "Cybersecurity Roadmap" *reported in* Steptoe & Johnson LLP (Issue 619, Week Ending August 14, 2010), *available at* http://www.steptoe.com/publications-7119.html.

[518] "Commerce Department Releases Report on Personal Data Security" *reported in* Steptoe & Johnson LLP (Issue 636, Week Ending December 25, 2010), *available at* http://www.steptoe.com/publications-7321.html.

[519] Minn. Laws 2002, ch.395; for text see http://www.spamlaws.com/state/mn.shtml.

[520] N.D. Century Code §6-08.1-01. *See* "North Dakota Tightens Laws on Bank Data and Privacy," N.Y. TIMES, June 13, 2002 at A286.

[521] *E.g.*, Vt. Dep't of Banking, Insurance, Securities & Health Care Admin., Banking Div'n Regulation B-2001-01 (Privacy of Consumer Financial and Health International Regulation). For text see http://www.bishca.state.vt.us/reg-bul-ord/privacy-consumer-financial-and-health-information-regulation. *See* J. 8.Lee, "California Law Provides More Financial Privacy," N.Y. TIMES (August 29, 2003), http://www.nytimes.com/2003/09/28PRIV.html. *See generally* J. Plummer, "Mandating Opt-In May Cause Consumers to be Left Out," http://www.nccprivacy.org/online/CR0205.htm.

[522] Pub. L. 108-159.

[523] The FACT Act's rules regarding identity theft are commonly referred to as the "Red Flag Rules." In October 2008, the FTC announced that it would suspend enforcement of the Red Flag Rules to give creditors and financial institutions additional time to initiate identity theft prevention programs. On October 30, 2009, the FTC further announced that it was delaying the enforcement of the Red Flag Rules until June 1, 2010. *See FTC Extends Enforcement Deadline for Identity Theft Red Flag Rules*, FTC Press Release (October 30, 2009), *available at* http://www.ftc.gov/opa/2009/10/redflags.shtm.

The FTC and the Board of Governors of the Federal Reserve System have adopted joint interim final rules that establish December 31, 2003, as the effective date of the provisions of the FACT Act that preempt state laws,[524] while many of the substantive provisions of the FACT Act may not become effective until as late as December 2004.

The FACT Act is intended to provide a unified approach to dealing with identity theft and consumer protection issues to replace a web of varying state laws. However, the disparity in effective dates between the preemption provisions and the substantive provisions of the FACT Act has led to a potential gap in the protection of consumers in states that already had consumer protection laws similar to those contained in the FACT Act. For example, California gives identity theft victims the right to place a security alert on their credit report to prevent further fraudulent activity.[525] The FACT Act contains a comparable provision[526] and thus arguably preempts the victim's rights under the California law, which would leave California consumers with no right under either state or federal law to place an alert on their credit report until that provision of the FACT Act goes into effect in June 2004.[527]

California was the first state to address the security of customer information in a law that became effective July 1, 2003.[528] All businesses (including individuals) that do business in California must notify California residents of any security breaches to their unencrypted personal information, defined as name and any combination of social security number, driver's license number, account number or debit or credit card number. After the ChoicePoint security breach, a spate of state legislative proposals were introduced.[529] Similar breach notification bills have been passed in most states.[530] Some states have gone further and specifically require that businesses use encryption to protect information.[531] And, under Texas's breach notification law, consumer notification obligations apply not only to affected Texas residents, but also to residents of other states that have not enacted their own breach notification laws.[532] The private bar has gotten into

---

[524] 16 C.F.R. § 602.1.

[525] Cal. Civil Code § 1785.15.

[526] FACT Act of 2003, Pub. L. 108-159, § 112.

[527] *See* "Attorney General Lockyer Urges Delay in Preempting State Laws Protecting Victims of ID Theft," Press Release of CA Office of Atty. Gen., Dec. 30, 2003 (as president of the National Association of Attorneys General Bill Lockyer warned that the immediate start of the FACT Act would leave consumers unprotected).

[528] California Civil Code §1798.82.

[529] *See* T. Zeller, Jr. "Breach Points Up Flaws in Privacy Laws," N.Y. TIMES, February 24, 2005, http://www.nytimes.com/2005/02/24/business/24datas.html; Reuters, "Lawmakers Promise Action on Identity Theft," http://msl1.mit.edu/furdlog/docs/2005-02-24_reuters_lawmakers_id.pdf.

[530] As of May 2014, 47 states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands have passed such laws – the only states without any breach notification requirement were Alabama, New Mexico and South Dakota. *See* report of the National Conference of State Legislatures, *available at* http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx. While several federal bills have been introduced, the only federal breach notification legislation governs the Veterans Administration. E-COMMERCE LAW WEEK (Jan. 7, 2007). The EU has proposed a directive requiring breach notifications. Proposal for a Directive of the European Parliament and the Council, COM (2007) 698, *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/dir_citizens_rights_en.pdf Although the EU has only proposed data breach notification requirements, Germany recently amended the German Federal Data Protection Law to require breach notification. *See* E-COMMERCE LAW WEEK (October 15, 2009), *available at* www.steptoe.com. Other countries such as Canada and New Zealand, have issued voluntary breach notification guidelines. WORLD DATA PROT.REP. (BNA) (Sept., 2007)

[531] *See, e.g.*, E-COMMERCE LAW WEEK (Feb. 2, 2008) (discussing bills passed and pending in Nevada, Massachusetts, Washington and Michigan), *available at* http://www.steptoe/publications-5118.html.

[532] Mathews, "Breach Notification Obligations in All 50 States?", Proskauer Rose LLP (Aug. 16, 2011), *reported*

the act, with at least one negligence action filed against a health care firm for negligence in failing to safeguard healthcare records.[533] Moreover, the First Circuit has held that, under Maine law, the reasonably foreseeable costs of mitigating potential losses stemming from a data breach (such as credit monitoring and payment card replacements costs) could constitute recoverable damages in support of a negligence and breach of implied contract action against a business suffering a breach.[534]

Massachusetts enacted regulations that became effective on March 1, 2010, considered by many to be the most comprehensive and far-reaching security laws imposed on businesses by a state. The Standards for the Protection of Personal Information of Residents of the Commonwealth (the "Regulations") were enacted to protect the security and confidentiality of the "personal information" of Massachusetts residents.[535] Not unlike other states' security laws, the Regulations require businesses to implement a comprehensive written security program and encrypt all personal information that is stored on portable devices, transmitted over public networks and transmitted wirelessly.[536] Further, the Regulations require that the businesses implement and maintain administrative, technical and physical safeguards that are tailored to the business's size, the amount of stored data, the amount of resources available to the business, and the need for security and confidentiality of both consumer and employee information.[537] These safeguards include, but are not limited to: designating employees to maintain the security program; identifying and assessing reasonably foreseeable risks to security and confidentiality of records; imposing disciplinary measures for violations; preventing terminated employees from accessing records; implementing restrictions and oversight of third-party service providers; implementing reasonable restrictions on physical access to records; and, regularly reviewing the security program and upgrading the safeguards when necessary. These Regulations are significant to businesses outside of Massachusetts because they apply to *all* businesses "that own, license, store or maintain personal information about a resident," regardless of where any such business may be located.[538] Therefore, even though a business may not be located or have a presence in Massachusetts, it may still be required to comply with the Regulations if it has employees or contractors that are residents of Massachusetts.

---

in Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=45e70f08-d093-435d-b120-908fc952e75c. As a reaction to the fact that other states did not have their own breach notification law, Texas enacted S.B. 1610, which makes it clear that businesses must notify affected residents of *every* state, though notification that complies with another state's law will also satisfy Texas' requirements. *See* E-COMMERCE LAW WEEK (July 11, 2013), *available at* http://www.steptoe.com/publications-8938.html; *see also* S.B. No. 1610 (Tex. 2013), *available at* http://www.legis.state.tx.us/tlodocs/83R/billtext/html/SB01610F.htm.

[533] *See* E-COMMERCE LAW WEEK (Feb. 12, 2006), *available at* http://www.steptoe.com/publications-1305.html (reporting on class action complaint by former patient against Providence Health System in Oregon Circuit Court, Multnomah County).

[534] *Anderson v. Hannaford Bros., Co.*, 659 F.3d 151 (1st Cir. 2011), *reported in* "Data Breach Mitigation Costs Can Constitute Cognizable Damages," Steptoe & Johnson LLP (Issue 682, Week Ending Nov. 12, 2011), *available at* http://www.steptoe.com/publications-pdf.html/pdf/?item_id=7887.

[535] 201 CMR 17.00, *et seq.* Under the Regulations, personal information is defined as a resident's first name or initial and last name in combination with the resident's (a) social security number, (b) driver's license or state-issued identification card number, or (c) financial account number, or credit or debit card number, with or without any required security or access code or password.

[536] *Id.*

[537] *Id.*

[538] *Id.*

These developments highlight the importance of effective planning to prevent security breaches, and to respond to them in accordance with applicable law if they do occur. The existence of such a policy may serve to protect against liability even where certain security precautions are absent. A federal district court in Minnesota dismissed a case in which a student loan company was charged with failure to encrypt customer data that was stolen. The court found that the firm's written security policy and proper safeguards to protect customer information indicated that the company had acted with reasonable care despite the lack of encryption.[539]

Another California law, the California Financial Institution Privacy Act (S.B.1) requires customer opt-in by California residents before financial institutions may disclose customer data to unaffiliated third parties, one of several stiffer standards than those of the opt-out regime of the federal Gramm-Leach-Bliley Act, discussed below.[540] The 2004 California Online Privacy Protection Act, or "CalOPPA," requires commercial operators of websites and online services, including mobile and social apps, that collect personally identifiable information from California residents to conspicuously post a detailed privacy policy in a means "reasonably accessible" to consumers, informing them about what data will be collected and how it will be used or shared.[541] And under the California Song-Beverly Act, businesses may not request and record personal identification information of customers when they make a purchase, other than information set forth on their credit cards.[542]

These California laws may encourage a wave of lawsuits stemming from companies' mishandling of sensitive personal information. Thus, in *Ruiz v. Gap, Inc.*,[543] the plaintiff applied online for a position with Gap for which he supplied his social security number. One year later, Gap announced that two laptops containing non-encrypted personal data – including plaintiff's information – were stolen from a third-party vendor with whom Gap had contracted. The plaintiff filed a class action suit against Gap, asserting violations of the California Civil Code.[544] The court held that the plaintiff had established standing based on the risk of future harm. The court so held notwithstanding the Ninth Circuit's pronouncement that to "confer standing, the threat of future injury must be credible rather than remote or hypothetical."[545] Similarly, in February 2013, a

---

[539] D. McCullagh, "Judge: Firm not negligent in failure to encrypt," C|net news.com (February 14, 2006), http://news.com.com/2100-1030_3-6039645.html.

[540] Calif. Financial Code, Division 1.2. (The 9th Circuit held that provisions restricting disclosure to affiliates were preempted by federal law. *American Bankers Assoc. v. Howard Gould*, 412 F.3d 1081 (9th Cir. 2005)).

[541] Cal. Bus & Prof. Code § 22575 *et seq.* In December 2012, California's Attorney General commenced the first ever CalCOPPA lawsuit against Delta Airlines, Inc., alleging that the carrier failed to conspicuously post a privacy policy on its "Fly Delta" mobile app, which also failed to provide reasonable access to the privacy policy on Delta's website. California's suit seeks to enjoin Delta from distributing its app without a privacy policy and penalties of up to $2,500 for each violation. *See California v. Delta Airlines, Inc.*, No. CGC-12-526741 (Cal. Super. Ct., Dec. 6, 2012); related press release and complaint are *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure. CalCOPPA is enforced by California's newly-created Privacy Enforcement and Protection Unit.

[542] Interpreting the Song-Beverly Act, the California Supreme Court in *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal.4th 524 (February 10, 2011) held that a customer's zip code was considered protected personal information that could not be collected. *See* "Zip Code is 'Personal Information' Under California Law," *reported in* Lexology (March 4, 2011).

[543] 540 F. Supp.2d 1121 (N.D. Cal. 2008).

[544] § 1798.85 provides that "a person or entity may not … [r]equire an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site."

[545] *Hartment v. Summers*, 120 F.3d 157, 160 (9th Cir. 1997).

blood bank operator agreed to settle a privacy class action lawsuit in California, stemming from the theft of an employee's laptop, external hard drive, USB drive, and other materials containing unencrypted sensitive personal information of nearly 300,000 consumers.[546] The estimated settlement value reaches into the tens of millions of dollars.

In another notable decision based upon a California statute, the United States District Court for the Northern District of California found that California's Unfair Competition Law (the "UCL") [547] encompassed claims made regarding website privacy policies.[548] The Court in *In re LinkedIn User Privacy Litigation*[549] granted in part and denied in part defendant's motion to dismiss a putative class action concerning LinkedIn's alleged misrepresentations regarding its privacy policy. The court held that plaintiffs met the standing requirements under the UCL since they adequately alleged causation and injury under the statute in connection with a 2012 security breach that resulted in approximately 6.5 million hacked passwords of LinkedIn users.[550] The lead plaintiff claimed that her injury arose from the purchase of LinkedIn's premium services package based upon the company's privacy policy statement which provided that her information "w[ould] be protected with industry standard protocols and technology." The lead plaintiff alleged that had she known that LinkedIn did not use industry-standard protocols, she would have tried to either negotiate a discounted price for the website's premium package or not have purchased these services at all, and thus she suffered injury. The Court noted that California defines "advertising" broadly and held that different standing requirements for labeling and advertising compared to alleged misrepresentations in website privacy statements would contravene California's broad consumer remedies, such as those available under the UCL. The Court additionally found that LinkedIn's privacy policy fell "within the scope of….labeling/advertising cases."[551]

On the enforcement side, DoubleClick, an on-line advertising company, settled an investigation by ten state attorneys general by accepting tight privacy restrictions and paying $450,000 to cover the States' investigative costs. DoubleClick had tracked users' web-surfing by means of cookies – small files placed on the user's computer – allowing it to select the ads to display based on the user's preferences. The settlement requires DoubleClick to give users access to their profiles maintained by DoubleClick and imposes restrictions on the use of the information it gathered.[552] In 2002, California adopted legislation, effective July 1, 2003, requiring firms that conduct business in California to disclose promptly any breaches of security

---

[546] *Johansson-Dohrmann v. CBR Sys. Inc.*, No. 3:12-cv-1115 (S.D. Cal. 2012). The private class action settlement is in addition to a similar enforcement action brought by the FTC, *In the Matter of CBR Systems, Inc.*, FTC file No. 112 3120. Following a public comment period, the FTC approved a final order settling charges that CBR failed to protect the security of customers' personal information and that its inadequate security practices led to a breach exposing the social security numbers and credit card information of 300,000 individuals. As part of the FTC settlement, CBR agreed to establish a comprehensive security program and submit to independent audits for the next 20 years.

[547] Cal. Bus & Prof. Code §17200 et seq.

[548] -- F.Supp.2d --, 2014 WL 1323713 (N.D. Cal. Mar. 28, 2014).

[549] *Id.*

[550] *Id.*

[551] *Id.*

[552] "DoubleClick Settles Privacy Inquiry," N.Y. TIMES (Aug. 27, 2002) at C3.

affecting personal data of a California resident to that resident.[553] The new law provides for private actions for damages, and injunctive relief.[554]

Victoria's Secret and Barnesandnoble.com both settled charges brought by the New York Attorney General as a result of security gaps that customers' personal information available to third parties. Victoria's Secret had promised that its customer data was kept "in private files on our server" protected by "stringent and effective security measures."[555] Barnesandnoble.com paid $60,000 as a result of a design flaw that allowed third party access to customer accounts and personal data, and allowed them to make purchases using other customers' accounts.[556] And Datron Media, an email marketer that purchased information on six million consumers from other companies with knowledge of the companies' promises not to lend, sell or give out their information and the used that information to send unsolicited e-mails, settled with the New York Attorney General in 2006, agreeing to pay $1.1 million and to take steps to ensure privacy compliance in the future, including appointing a Chief Privacy Officer to oversee those efforts.[557]

In Indiana, the attorney general's office is suing health insurance giant WellPoint Inc., asserting a $300,000 claim for waiting months to notify customers that their medical records, credit card numbers and other sensitive information may have been exposed online in violation of a state law that requires businesses to provide notification of data breaches in a timely manner.[558]

And, in an indication that the FTC and state authorities will cooperate in the privacy area, student survey firms simultaneously settled FTC and New York Attorney General charges that they deceptively gathered personal information from millions of students, claiming it would be used for educational purposes, and instead sold the information to commercial marketers.[559]

3. *Specific Areas of Regulation*

a. Privacy of Children's Personal Information − COPPA

As a result of the 1998 Privacy Report, the FTC recommended greater incentives for industry self-regulation and proposed legislation regulating the collection and use of information from children. Such legislation was enacted in the Children's Online Privacy Protection Act of 1998 ("COPPA"),[560] which required the FTC to issue regulations governing operators of websites and online services who know they are collecting personal information from children under the age of 13 and provided for enforcement actions by the FTC and state attorneys general.

---

[553] Cal. Civ. Code §§ 1798.29, 1798.82-.84.

[554] *See* Cal. Civ. Code §§ 1798.84(b)-(e).

[555] J. Schwartz, "Victoria's Secret Reaches a Data Privacy Settlement," N.Y. TIMES (October 21, 2003), http://www.nytimes.com/2003/10/21/technology/21priv.html.

[556] L. Rosencrance, "Barnesandnoble.com Hit with Fine for Online Security Breach," COMPUTERWORLD (April 30, 2004), http://www.computerworld.com/s/article/92804/Barnesandnoble.com_hit_with_fine_for_online_security_breach.

[557] Press Release , "Investigation Reveals Massive Privacy Breach," Office of New York State Attorney General Eliot Spitzer (March 13, 2006), *available at* http://www.ag.ny.gov/media_center/2006/mar/mar13a_06.html.

[558] *See* http://www.businessweek.com/ap/financialnews/D9J5JNK00.htm

[559] "Student Survey Firms Settle Charges FTC of Selling Data to Marketers," 84 ANTITRUST & TRADE REG. REP. (BNA) 80 (January 31, 2003).

[560] 15 U.S.C. §§ 6501 *et seq.*

The FTC regulations,[561] require a clear and prominent list on a website's home page and each page where personal information is collected from children, stating the name and contact information of each operator of the site, the types of personal information collected, how it is used and whether it is disclosed to third parties. The notice must state that a child's participation in an activity may not be conditioned on disclosing more information than is reasonably necessary, and that a parent can review a child's personal information, have such information deleted and refuse to permit further collection or use of the child's data. By 2001, 91% of children's websites posted privacy policies, compared with only 24% in 1998.[562]

The regulations adopted a sliding scale for parental consent, initially for two years, but later extended to April 21, 2005. A reliable method of consent is required for activities that pose the greatest risk to children, such as disclosing personal information to third parties or making it publicly available in chat rooms. Examples of such methods include mailing or faxing a signed printout, use of a credit card[563] or a toll-free number, digital signatures, and e-mail with a PIN or password. For internal uses of information, such as marketing back to the child, e-mail consent is sufficient, so long as additional steps are taken to confirm that the parent is providing consent. Eventually, the more reliable methods of consent will be required for all uses, unless the Commission determines otherwise. Parents must be given the option of permitting the collection and use of the child's personal information without consenting to disclosure to third parties. The rule also provides for certain exceptions to the prior consent requirement, and for a "safe harbor" program for industry groups who create self-regulatory programs approved by the Commission.

In its first enforcement action under COPPA, the FTC imposed fines totaling $100,000.[564] The FTC has continued to be active in its protection of children's privacy, filing four civil penalty actions in 2001 to enforce COPPA and pursuing active investigations on additional matters.[565] The FTC settled a case against a company which was using its website to target young girls and which, after having been warned, continued to collect information from underage girls in violation of COPPA. The company paid $30,000 as a civil penalty and is barred permanently from committing future violations of COPPA.[566]

In April 2002, the FTC settled charges against the Ohio Art Co., the makers of Etch-A-Sketch, alleging that it collected names, addresses, e-mail addresses and birth dates from children registering for "Etchy's Birthday Club". Ohio Art instructed the children to "get your parents or guardian's consent first," but did nothing to verify parental consent. The FTC also charged that Ohio Art collected more information then was necessary for participation in the "club" and that its privacy policy did not comply with COPPA's requirements. The settlement required a

---

561 16 CFR Part 312 (1999); TRADE REG. REP. (CCH) No. 575 Part 2 (April 28, 1999).

562 *3 Web Operators Settle COPPA Charges For Unauthorized Collection of Personal Data*, 80 ANTITRUST & TRADE REG. REP. 2004 (BNA) (Apr. 20, 2001), at 357.

563 The use of a credit card as a method of establishing verifiable parental consent, 16 CFR §312.5(2) seems curious, given that children may carry supplemental credit cards provided by their parents, and in any event requiring a credit card number would appear to sacrifice some of the parent's privacy in the name of protecting the child's.

564 Henry Beck & Victoria Guest, *Violations of COPPA continue*, THE NAT'L L.J. (Aug. 20, 2001) (the websites fined were girlslife.com, insidetheweb.com and bigmailbox.com).

565 *Protecting Consumers' Privacy: 2002 and Beyond: Remarks of FTC Chairman Timothy J. Muris*, at The Privacy 2001 Conference, Oct. 4, 2001, located at http://www.ftc.gov/speeches/muris/privisp1002.htm.

566 *Manufacturer of Popular Girls' Toys Settles FTC Charges of Violating COPPA*, 81 ANTITRUST & TRADE REG. REP. 2027 (BNA) (Oct. 5, 2001).

$35,000 civil penalty and the deletion of all personal information improperly collected for the past two years.[567]

In 2003, Mrs. Fields Cookies and Hershey Food Corporation paid civil penalties of $100,000 and $85,000 respectively, to settle charges of collecting personal information from children without the necessary advance parental consent and failing to post adequate privacy policies, to provide direct notice to parents of the information collected and its intended use, and to provide parents a reasonable way to review information collected from their children and prevent its further use. In particular, the Hershey site instructed children to have their parents fill out an online consent form, but took no steps to ensure that a parent actually completed the form, and collected information from children even if a parent or guardian did not submit information on the consent form.[568] Similar actions against UMG Recordings, Inc. and Bonzi Software, Inc. led to fines of $400,000 and $75,000 respectively, for failure to obtain verifiable parental consent before collecting personal information from children under 13. The FTC found that collection of birthdays in the sites online registration process established actions knowledge of the collection of data from children under 13.[569]

In April 2003, the Electronic Privacy Information Center and other privacy and consumer advocacy groups requested that the FTC investigate alleged violations of COPPA by Amazon.com in its "Toy Store," operated with Toys R Us. The groups charged that while Amazon's privacy policy restricts use of its website to those over 18 unless a parent or guardian is involved, its Toy Store pages are aimed at children, using "colorful and childlike fonts," child models and "child-oriented cartoon characters."[570] The complaint asserted that Amazon's site reflects numerous registered users under 13 who provided names and e-mail addresses, and some who posted names, ages, gender and street addresses, without complying with COPPA. Amazon succeeded in persuading the FTC that its site was not aimed at children and thus was not subject to COPPA, with the FTC finding that the vocabulary and language on the site appeared to be directed to adults.[571]

In 2009, the FTC settled charges against Iconix Brand Group, Inc. ("Iconix"), an online apparel marketer. According to the FTC, Iconix violated COPPA by knowingly collecting children's personal information without first obtaining parental permission. As part of the settlement, Iconix agreed to a civil penalty of $250,000, and provided a link to the FTC's webpage on its websites.[572]

---

[567] 82 ANTITRUST & TRADE REG. REP. (BNA) 365 (April 26, 2002).

[568] "FTC Receives Largest COPPA Penalties to Date in Settlements with Mrs. Fields Cookies and Hershey Foods," FTC Press Release (February 27, 2003), http://www.ftc.gov/opa/2003/02/hersheyfield.html.

[569] "UMG Recordings, Inc. to pay $400,000, Bonzi Software, Inc. to pay $75,000 to Settle COPPA Civil Penalty Charges," Federal Trade Commission (Feb. 18, 2004), http://www.ftc.gov/opa/2004/02/bonziumg.htm.

[570] *Matter of Amazon.com, Inc.*, EPIC Complaint and Request for Injunction, Investigation and for other Relief (April 22, 2003), http://www.epic.org/privacy/amazon/coppacomplaint.html; *see also* "Consumer Groups Accuse Amazon.com of Violating Children's Online Privacy Act," 84 ANTITRUST & TRADE REG. REP. (BNA) 400 (April 25, 2002); L.J. Flynn, "New Economy," N.Y. TIMES p. C4 (May 12, 2003).

[571] TRADE REG. REPORTS (CCH) No. 871, at 8 (December 2004); D. McCullagh, "Amazon Keeps Kids' Data Under Wraps, Regulators Say," CNetNews.com (Nov. 29, 2004), http://news.com.com/2100-1038_3-5470145.htm1.

[572] *In re Iconix Brand Group, Inc.*, FTC Docket No. 0923032 (October 2009); complaint, consent decree and news release *available at* http://www.ftc.gov/os/caselist/0923032/index.shtm.

The FTC in 2011 settled charges against skidekids.com (the "Facebook and Myspace for Kids") stemming from its operator's collection of personal information from approximately 5,600 children without parental consent in violation of COPPA.[573] Specifically, the FTC alleged that Skid-e-kids allowed children to register their birth date, gender, username, password and e-mail address without requesting a parent's e-mail address, in violation of COPPA's requirement that website operators notify parents and obtain their consent before collecting, using or disclosing personal information from children under 13 years old.[574]

The privacy of young fans of music stars Justin Bieber, Rihanna, Demi Lovato, and Selena Gomez was at issue before the fan website operator Arist Arena LLC agreed to pay $1 million to settle FTC charges that it violated COPPA by illegally collecting children's information without parental consent.[575] According to the FTC's allegations, Artist Arena operated various websites – such as www.RihannaNow.com, www.DemiLovatoFanClub.net, www.BeiberFever.com, and www.SelenaGomez.com – where children registered for fan clubs, created profiles and posted on members' walls. Children also supplied personal information in order to subscribe to fan newsletters. Artist Arena allegedly falsely claimed that it would not collect children's personal information without prior parental consent and that it would not activate a child's registration without parental consent. In actuality, the FTC alleged, Artist Arena knowingly registered over 25,000 children under age 13 and collected and maintained personal information from almost 75,000 additional children who began, but did not complete, the registration process.

The FTC has also entered into settlements involving alleged violations of COPPA by a provider of iPhone and other mobile applications. According to the FTC's complaint, W3 Innovations, LLC violated COPPA by unlawfully collecting and disclosing personal information of tens of thousands of children younger than 13 without obtaining parental consent.[576] Similarly, in January 2013 the operator of an iOS social networking app, Path, settled an FTC COPPA enforcement action for $800,000 and agreed to be subject to 20 years of independent privacy assessments. Among other things, the FTC had alleged that Path unlawfully collected personal information from app users' mobile phone directories without their knowledge or consent – including the personal information of approximately 3,000 children under 13 without parental consent. In bringing the enforcement action, the FTC advised that app developers should prompt users to provide affirmative consent to access their mobile directories through "just-in time, opt-in" consent, *i.e.*, when the user is most likely to notice and understand it.[577] Accordingly, mobile application providers must also be cognizant of their obligations under COPPA.

---

[573] "FTC Settles COPPA Violation Charges Against Children's Social Networking Website," Hunton & Williams LLP (Nov. 9, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=f7a5b188-d28f-4e63-8b8e-2bf9c827e37a.

[574] *Id*.

[575] *U.S. v. Artist Arena*, FTC File No. 112 3167; complaint, consent decree, and press release *available at* http://www.ftc.gov/opa/2012/10/artistarena.shtm. "Marketers need to know that even a bad case of Bieber Fever doesn't excuse their legal obligation to get parental consent before collecting personal information from children," said FTC Chairman Jon Leibowitz in connection with the settlement.

[576] "FTC Settles COPPA Charges Against Mobile Application Developer," Steptoe & Johnson E-Commerce Law Week (Issue 670, Aug. 20, 2011), *available at* http://www.steptoe.com/publications-7746.html.

[577] *U.S. v. Path, Inc.*, FTC File No. 122 3158; complaint, consent decree and news release *available at* http://www.ftc.gov/opa/2013/02/path.shtm.

In addition to its formal actions, the FTC has issued dozens of warning letters to the operators of children's websites for non-compliance with COPPA.[578] It has also established a safe harbor program under COPPA, under which industry groups and others can request FTC approval of self regulate guidelines to govern participants, so that participating web sites would first be subject to discipline by the safe harbor program rather than FTC enforcement.[579]

In February 2012 the FTC released a staff report criticizing mobile application stores and developers for failing to provide information that parents need to determine what data is being collected from their children, how it is being shared, and who will have access to it.[580] According to the FTC report, "Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing," there are currently approximately 500,000 apps in the Apple App Store and 380,000 apps in the Android Market – compared to about a total of 600 available apps in 2008 – and young children and teens are increasingly embracing smartphone technologies. Accordingly, the report recommended:

- All members of the "kid app ecosystem" – the stores, developers and third parties providing services – should play an active role in providing key information to parents.
- App developers should provide data practices information in simple and short disclosures. They also should disclose whether the app connects with social media, and whether it contains ads. Third parties that collect data also should disclosure their privacy practices.
- App stores also should take responsibility for ensuring that parents have basic information concerning data collection and sharing practices.

Finally, the report notes that industry participants should take steps to convey their data collection practices in plain language and in an easily accessible way on the small screens of mobile devices.

The FTC released a second report on mobile apps for children on December 11, 2012, largely to convey its belief that the industry has made "little progress" in alleviating the agency's concerns.[581] In the follow-up study, "Mobile Apps for Kids, Disclosure: Still Not Making the Grade," the FTC expressed frustration that most child-directed apps "failed to provide *any*

---

[578] 82 ANTITRUST & TRADE REG. REP. (BNA) 365 (April 26, 2002).

[579] *See, e.g., Privo, Inc.*, TRADE CAS. (CCH) ¶ 15,637 (2004). *See also* Press Release, "FTC Seeks Public Comment on Program to Keep Web Site Operators in Compliance With the Children's Online Privacy Protection Rule," Federal Trade Commission (January 6, 2010), *available at* http://www.ftc.gov/opa/2010/01/isafe.shtm.

[580] *FTC Report Raises Privacy Questions About Mobile Applications for Children*, FTC Release (Feb. 23, 2012), *available at* http://ftc.gov/opa/2012/02/mobileapps_kids.shtm.

[581] *Mobile Apps for Kids, Disclosures: Still Not Making the Grade*, FTC Release (Dec. 10, 2012), *available at* http://www.ftc.gov/opa/2012/12/kidsapp.shtm . The survey studied the privacy policies, app functionality, and web traffic for 200 apps from the Apple Store and 200 from the Google Play store. Many apps (nearly 60 percent of the apps surveyed) were found to be transmitting information from a user's device back to the app developer or to an advertising network, analytics company, or other third party. In conclusion, the FTC urged the industry to: incorporate privacy protections into the design of mobile products and services; offer parents easy-to-understand choices about the data collection and sharing through kids' apps; and provide greater transparency about how data is collected, used, and shared through kids' apps.

information about the data collected through the app, let alone the type of data collected, the purpose of the collection, and who would obtain access to the data" (emphasis in original). The "troubling" findings also revealed that many of these apps were, without parental consent, sharing with third-parties "device ID, geo-location, or phone number" information and contained features such as in-app purchases and links to social media. With respect to the privacy policies reviewed by the agency, the majority were described as lengthy, filled with irrelevant information, or lacking in basic details on the collection and use of personal information. Consequently, and as a result of its "alarming" findings, the FTC is now poised to conduct "multiple nonpublic investigations to determine whether certain entities in the mobile app marketplace have violated [COPPA], or engaged in unfair or deceptive trade practices …."

Thus, it is hardly surprisingly that one week later, on December 19, 2012, the FTC adopted revisions to COPPA's implementing regulations, which become effective July 1, 2013.[582] The long-awaited changes seek to keep up with rapidly changing technologies such as mobile devices and social networking sites and broaden the definition of protected "personal information" to include geolocation information, certain videos, audiofiles, and photographs, and "persistent identifiers" such as IP addresses and device IDs. Moreover, the definition of "operators" covered by COPPA has been expanded to close a known loophole and now includes child-directed sites or services that utilize third-party services (such as plug-ins or advertising networks) to collect personal information on their visitors. The amendments also add various additional methods that operators may use to obtain verifiable parental consent, including electronic scans of signed parental consent forms; video-conferencing; use of government-issued identification; and alternative payment systems, such as debit cards and electronic payment systems. Finally, the new regulations require operators to take reasonable steps to make sure that children's personal information is released only to third parties that are able and agree to commit to maintain the confidentiality of such information and to retain children's personal information for only as long as is reasonably necessary.

b. Financial Services − The Gramm-Leach-Bliley Act

i. Privacy Regulation

The 1999 Gramm-Leach-Bliley Act, which deregulated the financial services industry, imposed privacy regulations on any company that engages in financial activities under the Bank Holding Company Act of 1956. These activities cover a broad range of companies, potentially including all companies that extend credit to consumers. Title Five of the Act contains the Act's privacy provisions, which protect nonpublic personal information of natural persons (whether gathered offline or online), require disclosure of privacy policies in specified areas and restrict the disclosure or sharing of such information with third parties.

This Act requires "financial institutions" to establish privacy policies and disclose these policies when they first begin a relationship with a customer and then yearly after that. It also requires these institutions to give to customers the right to decide whether they want to block the

[582] 16 C.F.R. Part 312; FTC press release and Federal Register text *available at* http://www.ftc.gov/opa/2012/12/coppa.shtm. The new rules, among other things, also strengthen the FTC's oversight of self-regulatory safe harbor programs and require operators to adopt reasonable procedures for data deletion.

sharing of their confidential information with other third parties. In effect, the Act uses an "opt-out" provision for certain non-public information.

These financial institutions are unconditionally barred from sharing credit card or other account numbers or access codes of customers with third parties for the purpose of direct mailings, telemarketing or Internet marketing. "Financial Institutions" are defined with respect to the guidelines in Section 4(k) of the Bank Holding Company Act. Activities included within the Act include lending, insurance underwriting and sales, as well as securities underwriting and sales. Companies engaging in these activities − not only banks − are subject to these privacy provisions of the Gramm-Leach-Bliley Act. Indeed, the FTC sought to enforce the Act against lawyers who provide services in areas such as real estate settlements, tax planning and tax preparation, although this position was rejected by the courts.[583]

The provisions of the Act were phased in over time. The Act gave most affected business six months to issue and disclose their privacy policies.

In addition, the Gramm-Leach-Bliley Act designated specific federal regulatory agencies to oversee the implementation of Title Five in particular sectors of the financial industry. The Federal Trade Commission has jurisdiction over financial institutions that are not otherwise regulated by another federal regulatory body.[584] The FTC final Rule on the implementation of the Gramm-Leach-Bliley Act imposed the requirements generally called for by the Act:

- A "financial institution" must provide to its customers a clear and conspicuous notice about its privacy policies and practices. The notice must describe when and where the "financial institution" may disclose nonpublic information to unaffiliated third parties.
- A "financial institution" must also provide to its customers a clear and conspicuous annual notice of its privacy policies.
- Finally, a "financial institution" must provide its customers with a reasonable chance to "opt out" of disclosures of their nonpublic information to unaffiliated third parties. This opt out must be available at all times.

In December 2005, the major federal bank regulators, issued a Small Entity Compliance Guide for their Interagency Guidelines Establishing Information Security Standards.[585] (The Compliance Guide applies to all financial institutions, not merely "small entities," and indeed may be followed by the FTC in its enforcement actions against even non-financial businesses under the FTC Act, and so are worthy of review by all companies.)

ii. FTC Enforcement

In June of 2000, the FTC entered into a settlement with two information brokers who violated §5 of the FTC Act by "pretexting" (lying about their identity to obtain private financial information about individual consumers from financial institutions) in a deceptive manner. The proposed settlement barred the brokers from engaging in future deceptive practices and also prohibited them from "pretexting," "except where permitted by the Gramm-Leach-Bliley Act." In

---

583 *N.Y. State Bar Association v. FTC*, 2004 WL 964173, 2004 TRADE CAS. (CCH) ¶ 74,383 (D.D.C. 2004).

584 Other regulators include the SEC, the CFTC, the Comptroller of Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Directors of the Office of Thrift Supervision, the Board of the National Credit Union Administration, and state insurance regulators. These agencies have issued similar regulations.

585 *Available at* http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/attachment.pdf.

addition, the brokers were required to post a privacy policy on their website, disclosing the information they are collecting. This is one of the first reported cases to implement the Act in a forward-looking settlement. Over the following year the FTC examined hundreds of websites and ads for companies offering financial services and issued over 200 warning letters and commenced several federal court actions for pretexting.

iii. The Safeguards Rule

As part of its implementation of the Gramm-Leach-Bliley Act, in May 2002, the FTC issued final rules implementing Section 501(b) of the Gramm-Leach-Bliley Act (the "Safeguards Rule").[586] The purpose of the Safeguards Rule is to establish standards relating to administrative, technical and physical information safeguards as required by Section 501(b) of the Gramm-Leach-Bliley Act. Such standards are intended to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records on information that could result in substantial harm to a customer.

Pursuant to the Safeguards Rule, a financial institution must adopt a written information security program ("ISP").[587] With respect to its ISP, a financial institution must cover the following five elements:

- Designate an employee or employees to coordinate the ISP;
- Conduct risk assessment to identify internal and external risks to security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction of such information. Moreover, the FTC considers three areas to be the "most relevant" when conducting risk assessment: (i) employee training; (ii) information systems design, processing, storage, transmission and retrieval; and (iii) preventing, detecting and responding to attacks, intrusions or system failures;
- Design an ISP and detail the plans to monitor the ISP;
- Require third-party service providers that a financial institution has retained, by contract, to implement and maintain information safeguards; and
- Evaluate and adjust the ISP in light of changes to a financial institution's business operations or the results of its monitoring and security tests.[588]

The fourth element requires a financial institution to ensure that its third-party service provider comply with the Safeguards Rule if such a service provider receives a customer's nonpublic personal information.[589] Pursuant to the Safeguards Rule, a financial institution must

---

[586] *See* Standards for Safeguarding Customer Information; final rule, 16 C.F.R. 314, *available at* http://www.ftc.gov/privacy/glbact; "FTC Issues Financial Information Safeguards Rule," FTC Release (May 17, 2002). *See also* Federal Trade Commission – Business Alert, "Safeguarding Customers' Personal Information: A Requirement for Financial Institutions," *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/safealrt.htm. Again, other financial regulatory agencies have similar rules, the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. part 30 app. B, part 208 app. D.2, part 225 app. F, part 368 app. B, and part 570 app. B.

[587] *See* 16 C.F.R. 314.3(a).

[588] *See* 16 C.F.R. 314.4(a)-(e).

[589] *See* 16 C.F.R. 314.4(d)(2).

require its service provider, *by contract*, to implement and maintain information safeguards. As such, a financial institution will have to review an administrator's information operations and then negotiate and enter into a contract that obligates an administrator to adopt the same provisions under the Safeguards Rule. How administrators will react to this regulatory burden remain to be seen.

Financial institutions were required to implement their ISPs by May 23, 2003.[590] As such, financial institutions have the next seven months to evaluate their operations and to develop an ISP. Furthermore, there was a transition rule for contracts entered into by June 23, 2002 between financial institutions and third-party service providers.[591] This transition rule gave financial institutions two years to require their service providers, by contract, to implement an ISP.[592] Accordingly, financial institutions have until May 23, 2004 to bring service contracts with administrators into compliance with the Safeguards Rule. To assist financial institutions in complying with the Safeguards Rule, the FTC has issued guidance on how to implement and monitor an ISP and on how to oversee a third-party service provider in the near future.[593] The FTC has brought charges under the Safeguards Rule for failure to have reasonable protection for customers' sensitive information.[594]

Several financial regulatory agencies have proposed regulations to govern financial institution responses to breaches of customer information security.[595] Financial institutions would be required to develop response programs to address reasonably foreseeable risks to the security of its customer information, including procedures for notifying customers and regulatory and law enforcement agencies of unauthorized access to customer information that would result in substantial harm or inconvenience, to contain and control the situation, and to act to mitigate the harm to individual customers, including certain specified steps.

Finally, the FTC implemented new Identity Theft Red Flag regulations under the FACT Act effective as of December 31, 2010.[596] The Identity Theft Red Flag regulations require financial institutions and creditors that hold consumer accounts to develop and implement an Identity Theft Prevention Program for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to (i) identify relevant patterns, practices and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Program; (ii) detect red flags that have been incorporated into the Program; (iii) respond appropriately to any red flags that are

---

590 *See* 16 C.F.R. 314.5(a). *See also* FTC Commentary to 16 C.F.R. 314. The Safeguards Rule will take effect one year from the date on which the final rule is published in the Federal Register which was May 23, 2002. See FTC Commentary to 16 C.F.R. 314.

591 *See* 16 C.F.R. 314.5(b). *See also* FTC Commentary to 16 C.F.R. 314. Contracts between financial institutions and nonaffiliated third-party service providers are given two years to bring service provider contracts into compliance with the Safeguards Rule as long as the contract was in place 30 days after the date on which the final rule was published in the Federal Register which was May 23, 2002. *See* FTC Commentary to 16 C.F.R. 314.

592 *See* 16 C.F.R. 314.5(b). See also FTC Commentary to 16 C.F.R. 314.

593 Federal Trade Comm'n, "Financial Institutions and Customer Data: Complying with the Safeguards Rule" (September 2002), *available at* http://www.ftc.gov/bcp/conline/pubs/bspubs/safeguards.pdf.

594 *See Sunbelt Leading Services, Inc.*, TRADE CAS. (CCH) ¶ 15,678 (2004).

595 Notice and Request for Comment, Interagency Guidance or Response Programs for Unauthorized Access to Customer Information and Customer Notice, 68 FED. REG. 47954 (August 12, 2003).

596 16 CFR Part 681.

detected to prevent and mitigate identity theft; and (iv) ensure the Program is updated periodically to reflect changes in risks from identity theft.[597]

iv. The SEC's Proposed Amendments

In 2008, due to the increase in reported security breaches, the SEC proposed amendments to its privacy regulations[598] under the Gramm-Leach-Bliley Act. The amendments would require covered entities to develop and implement privacy and record-keeping policies relating to customer data. The rule also requires such businesses to develop a preparedness plan for responding to breaches, which may include the duty to notify the Commission and affected individuals immediately. The proposed regulations indicate the SEC's desire to parallel similar protections mandated by the FTC.[599]

c. Medical Records − HIPAA

Privacy of individually identifiable health information is regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[600] and regulations promulgated under HIPAA. HIPAA regulates "covered entities, which include health care providers, health plans and "health care clearinghouses"[601] that maintain or transmit health information using electronic media.

Under the original HIPAA regulations adopted at the end of the Clinton administration, use of an individual's health information required the individual's consent, regardless of the use. Consent was required before medical data could be used for treatment, payment, marketing or a variety of other activities.[602]

Under revised regulations issued in August 2002,[603] the requirement of consent for treatment and reimbursement was eliminated, replaced by mere notice by the covered entity of its disclosure policies. The Bush administration argued that the consent requirement could delay treatment. Although consent is still nominally required for marketing activities, the new regulations distinguish recommending treatment from marketing, a loophole exploited by pharmaceutical companies paying pharmacies to send mailings advocating the use of alternative

---

597 *Id*, *reported in* Hoffman, "Wide Range of Businesses Must Implement 'Red Flags' Programs" (Lexology, May 18, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=f16f3cac-726e-4e12-b307-864d86352ed6.

598 S.E.C. Reg. S-P

599 *Reported in* Steptoe & Johnson, *E-Commerce Law Week* (March 22, 2008); 73 Fed. Reg. 13692 (Mar. 13, 2008), *available at* http://www.sec.gov/rules/proposed/2008/34-57427.pdf.

600 Pub.L.No.104-191, 110 Stat. 1936 (1996).

601 A health care clearinghouse is "a public or private entity that processes or facilitates the processing of nonstandard run data elements of health information into standard data elements." 42 U.S. § 1320(d)(2).

602 One unintended consequence has been to impede medical research, as researchers can no longer review medical records to identify those who might benefit from a clinical trial, but rather must rely on patients' own physicians to initiate such contacts. M.D. Baum & L. Rossi, "Privacy Rule Builds Biomedical Research Bottleneck, U. Pittsburgh Medical Center (Sept. 13, 2004), http://www.eurekalert.org/pub_releases/2004-09/uopm-prb091304.php.

603 45 C.F.R. Parts 160 and 164. This may include banks that process health care payments. *See* "United States – Banks Processing Payments to Health Providers," WORLD DATA PROTECTION REP. (BNA) 20 (Jan. 2002)

proprietary drugs to patients that the pharmacy records indicate use competing products, without the knowledge or consent of the patients.[604]

In addition, HIPAA security standards, effective April 21, 2005, require health care organizations to ensure the confidentiality, security, integrity and availability of electronic health information and protect it against unauthorized disclosure or use.[605] Notwithstanding the delayed effective date, these security regulations are likely to become the de facto standard for compliance with the HIPAA privacy regulations.[606] The regulations require administrative, physical and technical safeguards and the kind of ongoing risk assessment, policy development and implementation, and ongoing revision required by the GLB Safeguards Rule and the FTC security requirements described above.[607] In addition, the security rules imposed a duty to document any "security incident," such as an impermissible disclosure, to sanction employees who violate HIPAA policies, and to mitigate adverse effects of the incident, which may include notice to affected individuals.[608]

Under President Obama's 2009 stimulus package, the American Recovery and Reinvestment Act ("ARRA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), any entity covered by HIPAA that suffers a breach of health information is required to notify all affected individuals no later than 60 days after the discovery of such a breach.[609] If the breach involved 500 or more individuals, the entity is required to immediately notify the Secretary of the Department of Health and Human Services ("HHS"). Where the breach affects fewer than 500 individuals, it must be appropriately logged and submitted to the Secretary annually. Furthermore, the government's enforcement powers have been expanded to include compliance audits and the more robust pursuit of privacy and security complaints and investigations.[610] Penalties for not complying with HITECH could subject a covered entity to as much as $50,000 per violation, with a $1.5 million cap.[611] For entities not

---

[604] A. Zimmerman & D. Armstrong, "How Drug Makers Use Pharmacies To Push Pricey Pills," WALL STREET J., p.A1 (May 1, 2002).

[605] 45 CFR Parts 160, 162 and 164 (2003).

[606] B. Brevin, "New HIPAA Security Rules Could Open Door to Litigation." COMPUTERWORLD, (February 20, 2003) http://www.computerworld.com/printthis/2003/0,4814,78684,00.html.

[607] *See* S. Weil, "HIPAA Security Rule: What It Is & How to Comply With It," Security Focus (March 1, 2004).

[608] 45 C.F.R. Part 164; J.E. Arent, "United States: Risks and Responsibilities under HIPAA Following an Impermissible Disclosure," WORLD DATA PROTECTION REP. (BNA) (April 2004) at 25.

[609] *See* Pub. L. 111-5. *See also* E-COMMERCE LAW WEEK (Feb. 28, 2009), *available at* www.steptoe.com/E-CommerceLawWeek; Press Release, *FTC Issues Final Breach Notification Rule for Electronic Health Information*, Federal Trade Commission (August 17, 2009), *available at* http://www.ftc.gov/opa/2009/08/hbn.shtm. Pursuant to HITECH, the notice must include a description of what happened, the date of the breach, the date of discovery of the breach, the types of unsecured protected health information, steps the individual should take, steps the entity took or is taking to investigate and/or mitigate, and contact procedures for individuals with more questions. *See* "FTC issues Final Rule on Notifying Consumers About Breaches of Electronic Health Records," *reported in* Lexology (September 3, 2009), *available at* http://www.lexology.com/library/detail.aspx?g=07aeb5d8-ccab-48db-88bf-0e08e192d35e.

[610] HITECH also strengthens individuals' right of access to their electronic health records, and places limits on the use and disclosure of protected health information for marketing purposes. Any Covered Entity must provide an individual with access to such electronic information in form and format requested by the individual upon 30 days' notice (unless the information is located off-site). *See* Hanna, Rangel, Setliff and Ward "HIPAA Security and Privacy Rules Modified for HITECH Act Provisions," *reported in* Lexology (August 2, 2010); s*ee also "HIPAA HITECH Regulations Proposed" reported in* Lexology (July 29, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=1a7cddb7-169e-4b7d-83df-a078ade02ed9.

[611] Mulhollan, "HIPAA Has Teeth – Part II" *reported in* Lexology (June 10, 2010), *available at*

covered by HIPAA, such as vendors, ARRA provides that any entity that suffers a breach of any size must notify the FTC, which will then notify the HHS Secretary.[612]

Employee health plans are generally subject to the privacy restrictions, although there are exceptions for fully insured plans and self-administered plans with fewer than fifty participants. Where an employer is not a covered entity, but its health plan is, it is important to create appropriate firewalls to keep the health plan's information from the employer.

Subsequent developments show that HIPAA and its accompanying regulations are not toothless tigers. HHS has conducted several data security operations, seeking to enforce the HIPAA standards discussed above. In 2007, HHS conducted a "security audit" at Piedmont Hospital in Atlanta.[613] And on July 15, 2008, HHS entered into a settlement with Providence Health & Services resulting from Providence's "potential violations" of HIPAA's requirements to safeguard electronic patient data. The settlement – which requires the payment of $100,000 and the adoption of a corrective action plan – resulted from the loss of laptops and discs containing unencrypted medical records of more than 386,000 patients.[614] The following year, CVS Caremark settled FTC charges based on its failure to implement reasonable and appropriate procedures for securing customer and employee information, and also agreed to pay $2.25 million for HIPAA violations.[615] In February 2011, HHS also fined Cignet Health of Maryland $4.35 million for HIPAA violations, most of which was attributable to the company's failure to cooperate with HHS's investigation.[616]

In 2012, the Department of Health and Human Services' Office of Civil Rights ("OCR") released its HIPAA privacy and security audit protocols.[617] These new protocols "provide more

---

http://www.lexology.com/library/detail.aspx?g=e26e6e08-2968-48e4-9eed-2144f51f4dd4. In addition to fines, individuals are subject to criminal penalties. A former UCLA Health System employee, apparently disgruntled over an impending firing, was sentenced to four months in federal prison after pleading guilty in January 2010 to illegally snooping into patient records, mainly those belonging to celebrities. http://www.scmagazineus.com/health-worker-is-first-hipaa-privacy-violator-to-get-jail-time/article/168894.

612 Similar to ARRA, a California law went into effect on January 1, 2009, requiring health care organizations in California to report breaches of patient data. In the first five months that the law was in effect, there were over 800 breaches reported. *See New Law Floods California With Medical Data Breach Reports*, Wired (July 9, 2009), *available at* http://www.wired.com/threatlevel/2009/07/health-breaches.

613 *See Feds Finally Put Teeth into HIPAA Enforcement*, Computerworld (Sept. 8, 2008), *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=325376.

614 Corrective action plan, *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/. Most recently, Concentra Health Services and QCA Health Plan Inc. paid close to $2 million combined in fines to resolve an HSS enforcement action resulting from their failure to adequately secure electronic protected health information of customers located on stolen, unencrypted company owned-laptop computers. Corrective action plan, *available at* http://www.hhs.gov/news/press/2014pres/04/20140422b.html.

615 *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations*, FTC Press Release (February 18, 2009), *available at* http://www.ftc.gov/opa/2009/02/cvs.shtm.

616 Elbon, "Covered Entities and Associates Must Take Heed of Recent HIPAA Privacy Sanctions," Bradley Arant Boult Cummings LLP (Mar. 10, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=1346490c-822f-4ed7-b005-6d36fc5bc60e.

617 Dianne J. Bourque and Stephanie D. Willis, *HIPAA Audit Protocols Now Public; Plus, Preliminary Insights from OCR*, (Jun. 28, 2012), reported in Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=129fbc07-6701-420a-b92f-eb9205dbb562. (noting that the audit protocols were intended to cover the three main areas of HIPAA privacy and security enforcement including: (1) the Privacy Rule; (2) the Security Rule; and (3) the Breach Notification Rule.).

clarity on auditors' standards for performing HIPAA compliance audits of covered entities and business associates."[618]

These HIPAA enforcement developments underscore the growing importance of maintaining proper safeguards to protect electronic patient data.

d. Workplace Privacy

In the United States, employees' privacy rights have been severely curtailed through the virtually unregulated and unrestricted use of various electronic monitoring and surveillance systems utilized by employers. Millions of U.S. workers are subject to continuous surveillance of their e-mail and Internet use while at work.[619]

As a general rule, employees do not have an expectation of privacy from their employer in their e-mail or office systems, particularly where the employer has an announced policy of monitoring e-mail.[620] Employees may lose an objectively reasonable expectation of privacy in the contents of even their own personal computers that are used with and connected to an employer's network,[621] although some courts have held that employees have some reasonable expectation of privacy in their workplace, at least with regard to personal email accounts.[622] An American Management Association Survey in 2003 found that most U.S. companies monitor employee e-

---

[618] Kimberly J. Gold, *Utilizing the HIPAA Audit Protocols as a ComplianceTtool*, Compliance Today, December 2010, at 50, *available at* http://www.hcca-info.org/Resources/NEWSRoom/ComplianceToday.aspx (subscription required).

[619] *See*, Carl S. Kaplan, *Reconsidering the Privacy of Office Computers*, N.Y. TIMES ON-LINE, (July 27, 2001), located at http://www.nytimes.com/2001/07/27/technology/27CYBERLAW.html.

[620] *See, e.g., U.S. v. Bailey*, 272 F. Supp. 2d 822 (D. Neb. 2003); *Garrity v. John Hancock Mut. Life Ins. Co.*, No. 00-12143-RWZ (D. Mass. May 7, 2002); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996); *McLaren v. Microsoft Corp.*, No. 05-97-00824-cv (Tex. Ct. App. 1999); *Restuccia v. Burk Technology, Inc.*, No. 95-2125 (Mass. Supr. Ct. 1996); *City of Ontario v. Quon*, 130 S.Ct. 2619 (where the Supreme Court unanimously held that a public employer's search of an employee's text messages on employer-issued communications device was reasonable and did not violate the employee's constitutional rights under the Fourth Amendment since the search was justified and not excessively intrusive); *but see, Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 321-22 (2010) (employee had reasonable expectation of privacy in messages exchanged between employee and her attorneys where, among other things: (i) the employer's policy did not specifically address employees' use of personal e-mail accounts; (ii) the employee "plainly took steps to protect the privacy of those e-mails and shield them from her employer," viz., used a personal, password-protected e-mail account instead of her company e-mail address; and (iii) "[t]hey are conversations between a lawyer and client about confidential legal matters, which are historically cloaked in privacy").

[621] *See, e.g., United States v. King*, 509 F.3d 1338 (holding that a worker convicted of possession of child pornography had no objectively reasonable expectation of privacy when the worker connected his personal laptop to a network which allowed network users to access files in the laptop).

[622] *See Pure Power Boot Camp Inc. v. Warrior Fitness Boot Camp, LLC*, 2010 WL 5222128 (S.D.N.Y. Dec. 22, 2010) (holding that the employer's reliance upon its privacy policy was not enough to defend its accessing of an employee's personal Hotmail e-mail account in the workplace); *but compare with New York v. Klapper*, 28 Misc.3d 225 (N.Y. Co. Criminal Court, April 28, 2010) (dismissing criminal charges against employer who used a keystroke monitor to record the personal emails of an employee), *reported in* E-Commerce Law Week, *available at* *http://www.steptoe.com/publications-6846.html*.

mail to some degree and enforce company e-mail policies with discipline, with 22% of companies having terminated employees for e-mail policy violations.[623]

The announced policy is important, however, to avoid falling under the Electronic Communications Privacy Act of 1986[624] – the federal wiretap law – which bars third party interception of electronic communications. The Act contains an exception for an employer's right to monitor employees, provided it is done in the ordinary course of business or with the employee's express or implied consent. It thus is important for employers who wish to monitor e-mail to provide notice of a policy that negates any expectation of privacy by employees in their e-mail. Monitoring of stored communications, such as email messages stored on an employee's computer or a company's e-mail server, may be treated more leniently, and an employer who is the "provider" of the email system may be permitted to access the messages stored on the system, even in the absence of consent.[625]

This reasoning caused an uproar, however, when The First Circuit initially held that an email service provider did not violate the wiretap law when it monitored users' incoming mail without their consent. The service provider was a bookseller that offered email service to customers, and configured the system to forward all incoming email from Amazon.com, a competitor, to the bookseller's mailbox as well as to the customer. Because the forwarding was performed on a stored message rather than by an "interception" of the e-mails in transit, the First Circuit panel held it was lawful.[626] After rehearing *en banc*, however, the entire First Circuit reversed, finding that "[t]he statute contains no explicit indication that Congress intended to exclude communications in transient storage. . . from the scope of the Wiretap Act" and that the purpose of the statutory language "was to enlarge privacy protections for stored data under the Wiretap Act, not to exclude e-mail messages stored during transmission from those strong protections."[627] The distinction between stored communications and those that are intercepted is still observed by some courts, however. In 2007, a federal district court found that e-mails accessed while in storage were not covered by the Wiretap Act.[628] In 2009, another federal district court found that previously opened web-based e-mails stored by an internet service provider that were less than 181 days old were not considered to be in "electronic storage," as defined by the Wiretap Act.[629] Instead, because such e-mails were opened and were not held for the purposes of backup protection, they were considered to be "held or maintained … solely for the purpose of providing storage or computer processing services to [the] subscriber or customer," pursuant to the Stored Wire and Electronic Communications and Transactional

---

623 AMA Research, "2003 E-mail Rules, Policies and Practices Survey," (2003), http://www.amanet.org/research/pdfs/Email_Policies_Practices.pdf.

624 18 U.S.C §§ 2510 *et seq*.

625 *See Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3d Cir. 2003); *Bohach v. City of Reno*, 932 F.Supp. 1232, 1236 (D. Nev. 1996); C.H.Kennedy & T. Kanan, "Surveillance of Workplace Communications: U.S. Employer Rights," WORLD INTERNET L. REP (BNA) (March 2004) at 20; "Internet Privacy is a Fallacy" *available at* http://www.steptoe.com/publications-6846.html.

626 *U.S. v. Councilman*, 373 F.3d.197 (1st Cir. 2004); *see* "Privacy Groups and Government Appeal E-mail Tapping Case," Outlaw.com (Sept. 6, 2004), http://www.out-law.com; "Online Privacy Eviscerated by First Circuit Decision," Electronic Freedom Foundation, http://www.eff.org/news/archives/2004_06.php#001658.

627 *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005); *see also United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir., 2010).*

628 *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443 (C. D. Cal. 2007).

629 *U.S. v. Weaver*, 636 F. Supp. 2d 769 (C. D. Ill. 2009).

Records Access Act (the "Stored Communications Act" or the "SCA").[630] Accordingly, under the Stored Communications Act, such e-mails could be obtained from the internet service provider by using a trial subpoena, as opposed to a warrant as would be required for e-mails in "electronic storage."[631]

An announced policy or employee handbook is also important to protect company information from departing employees suspected of disloyal acts.[632] While many employers typically conduct electronic and data investigations on departing employees, employers should exercise caution as these investigations often uncover personal information, like passwords used by the employee for personal e-mail accounts, which could possibly give rise to claims under the Stored Communications Act. Some courts have held that improperly using these passwords to open and monitor the employee's personal e-mail or social media accounts may give rise to a claim for unauthorized access under the Stored Communications Act.[633] However, it should be noted that employers can also make claims under the Stored Communications Act, which can serve as a complement to, or substitute for, the Computer Fraud and Abuse Act, and which does not require the plaintiff to prove a statutory threshold of damages.[634]

State laws may provide differing rights and obligations, and need to be reviewed as well. For instance, 2012 and 2013 have witnessed the passage of a flurry of state laws restricting employers from requesting an employee's or applicant's social media account log-in information.[635] Many of these new state laws ban employers from requiring applicants or employees to disclosure their passwords or usernames, add the employer (or a supervisor) as a "contact," change privacy settings, permit employer "shoulder-surfing," or otherwise provide access to social media accounts. On the other hand, the state "password protection laws" typically include several exceptions, including accessing accounts opened by the employee at the employer's request or accounts set up for the employee by the employer; accessing employer-provided devices or electronic communications systems; viewing publically-available information; and/or engaging in limited investigations of suspected violations of employer policies or the law.

---

630 18 U.S.C. § 2701, *et seq.*

631 *U.S. v. Weaver*, 636 F.Supp. 2d 769 (C. D. Ill. 2009).

632 *See U.S. v. John*, 597 F.3d 263, 269, 272 (5th Cir. 2010) (holding that a former employee had violated the Computer Fraud and Abuse Act and exceeded authorized access to company information based on employer's official policy, which was reiterated in training programs that employee had attended, and that prohibited misuse of the company's internal computer systems and confidential customer information); *but see Accenture, LLP, v. Sidhu*, 2010 WL 4691944 (narrowly construing the Computer Fraud and Abuse Act and holding that when an employer makes a computer available to an employee, that employee is authorized to access that computer for any reason, even if his access violates company policy).

633 *See Pietrylo v. Hillstone Rest. Group*, No. 06-5754, 2009 U.S. Dist. LEXIS 88702 (D.N.J., Sept. 25, 2009).

634 *See Devine v. Kapasi*, 729 F.Supp.2d 1024 (N.D.Ill., 2010) (holding that private companies with facilities through which an electronic communication service is provided can sue under the SCA when such facility is breached); *but see Freedom Banc Mortgage Services, Inc. v. O'Harra*, 2012 WL 3862209 (S.D. Ohio 2012) (actions of former employee who remotely accessed company systems did not violate the SCA, but did violate the Computer Fraud and Abuse Act, because the employer's computer network did not constitute an electronic communications "facility" within the meaning of the SCA.).

635 *See* Arkansas (H.R. 1901, 89th Gen. Assem., Reg. Sess. (2013)), California (A.B. 1844, 2012 Assemb.), Illinois (H.B. 3782, 97th Gen. Assemb. (2012)), Maryland (Md. Code Ann., Lab. & Empl. § 3-712 (2012)), Michigan (2012 Mich. Pub. Acts 478), New Mexico (N.M. Laws 2013, S.B. 371), Nevada (A.B. 181, 2013 Assemb.), Utah (2013 Utah Laws, H.B. 100). Similar proposed legislation is pending in several other states.

In other countries, the rules may vary, although the European Commission plans to propose a draft Directive on Privacy in the Workplace by 2005,[636] and employees are protected by the European 1998 Directive and national data protection law. There are decisions affirming employers' right to monitor employee e-mail on company computers in some cases, while others have restricted such employer monitoring.[637] In Great Britain, the Employment Practices Data Protection Code, which covers opening e-mail and voice mail, monitoring Internet usage and video recording, requires intrusive monitoring to be justified, and mandates notice to employees in almost all cases.[638] And prosecutors in South Korea brought criminal charges against the manager of a company for illegally accessing e-mail of an employee suspected of leaking internal corporate information.[639] France, on the other hand, has recently been expanding the scope of employers' rights, finding that an employer was entitled to open an employee's files without the employee's presence or consent.[640] In addition, France's highest court, the Cour de Cassation, determined in 2011 that it was permissible for a company to terminate an employee based upon an e-mail exchange with a co-worker that referred to a supervisor in offensive terms.[641]

Finally, employee e-mails and instant messages in the workplace are potentially subject to inspection upon the commencement of a criminal investigation against an employee. Recently two former Bear Sterns hedge fund managers were indicted for securities fraud based upon work e-mails sent that indicated they knew investments were troubled while simultaneously telling investors that market conditions were stable.[642] Similar stories abound of Wall Street professionals caught in a web of their own work e-mails.[643]

---

[636] "Working Document on the Surveillance of Electronic Communication in the Workplace," Article 29 – Data Protection Working Party (May 29, 2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf.

[637] *See* M. Wugmeister, "E.U. Data Protection Requirements: An Overview for Employers, "WORLD DATA PROTECTION REP. (April 2004) at 7; E. Temperton & A.M. Norburg, "Workplace Monitoring in Europe," WORLD DATA PROTECTION REP. (Jan. 2004) at 1; "Employees Rebel Against Monitoring of Online Activities," http://www.internationallawoffice.com/newsletters/detail.aspx?g=ac10eaab-d572-4fe8-a9ce-119cbef702cb (Sept. 12, 2002) (reporting Regional Labor Court decision upholding dismissal of employee who used company e-mail to send pornography); "Employers Get Green Light to Monitor Employee E-mails," http://www.internationallawoffice.com/Newsletters/Detail.aspx?g=51a9129a-b3b0-429d-a615-2762233d1e9d&redir=1 (reporting Tribunal of Milan ruling that employer may monitor e-mails received by employee in company mailbox); I. Gavanon & A. Bowlant, "France – Employee Internet Usage: When Is Monitoring by Employers Allowed?," WORLD INTERNET L. REP (BNA) 30 (June 2002).

[638] "Respect Workers' Privacy, Employers Told," GUARDIAN UNLIMITED (June 11, 2003), http://money.guardian.co.uk/work/story/0,1456,975109,00.html.

[639] *See* "South Korea_First Criminal Case on Corporate Surveillance of Employees' E-Mail," WORLD INTERNET L. REP. (BNA) 11 (June 2002).

[640] *Reported in* Steptoe & Johnson, E-Commerce Law Week (Jan. 30, 2010); *See also "French Supreme Court Upholds Right of Company to Access an Employee's Emails" available at* http://www.bakermckenzie.com.

[641] "French High Court Upholds Company's Review of Employees' Email," Steptoe & Johnson, E-Commerce Law Week (Issue 650, April 2, 2011), *available at* http://www.steptoe.com/publications-7507.html.

[642] *U.S. v. Cioffi and Tannin*, No. 2007-R01328 (E.D.N.Y. 2008). A copy of the indictment *available at* http://online.wsj.com/public/resources/documents/bearindictment.pdf.

[643] *See Wall Street's Messaging Mistakes*, NEW YORK TIMES (June 19, 2008), *available at* http://dealbook.nytimes.com/2008/06/19/wall-streets-messaging-mishaps/.

4. Balancing Privacy and Security

U.S. government security concerns have obviously increased dramatically since the events of September 11, 2001. The balance of security concerns and individual rights, including privacy rights, has been a topic of discussion and dispute.

In one example, European privacy regulations came into direct conflict with U.S. security concerns in connection with U.S. requirements for the collection and transmission of various passenger data for flights destined for the U.S. The disclosure in 2003 that Jet Blue airlines had transmitted passenger data to a defense contractor brought the issue to a head. U.S.-EU negotiations led to the issuance of a December 16, 2003 Communication from the European Commission setting forth a "Global EU Approach" to the issue,[644] and ultimately to a formal US-EU Passenger Name Record Agreement being signed on May 28, 2004, providing for the collection of passenger data for flights between the U.S. and Europe.[645] This led, however, to protests from some in Europe that the accommodation was a political decision in violation of EU law,[646] and the European Parliament objected to the agreement and successfully challenged it in the European Court of Justice, which annulled the agreement in May 2006, as without legal basis, returning the issue to square one. [647] Finally, a new agreement was signed on July 23, 2007, by which the U.S. provided assurances as to the use of passenger data, and the EU agreed that the U.S. has provided an adequate level of protection for the data, so that airlines could lawfully provide the information.[648] Even within the EU, this issue has been debated. EU plans to require companies to retain telephone and email records to assist in anti-terrorism investigations have been criticized by privacy regulators.[649]

In 2006, a report of Belgium's privacy protection commission found that the transfer by the SWIFT bank money transfer consortium, based in Belgium, of transaction information to the Central Intelligence Agency, the U.S. Treasury and other U.S. agencies, violated European data protection regulations and was a "gross miscalculation." The report (which stemmed from the

---

644 "Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach," Communication from the Commission to the Council and the Parliament (Dec. 16, 2003), http://ec.europa.eu/justice/policies/privacy/docs/adequacy/apis-communication/apis_en.pdf. *See Also* F. Bolkestein, Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market regarding EU/US talks on transfers of airline passengers' personal data (Dec. 16, 2003), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/03/396&format=HTML&aged=1&language=EN&guiLanguage=en.

645 "DHS and EU Sign Agreement to Allow Collection of Passenger Data," Department of Homeland Security (May 28, 2004), http://www.dhs.gov/xnews/releases/press_release_0420.shtm.

646 R. Singel, "EU Travel Privacy Battle Heats Up," WIRED NEWS (Dec. 22, 2003), http://www.wired.com/news/politics/0,1283,61680,00.html; "MEPs Divided Over Commission Deal on Airline Passenger Data," EuroParl News Report (Dec. 17, 2003), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+PRESS+NR-20031217-1+0+DOC+XML+V0//EN.

647 *See* "EU court annuls data deal with US," BBC News (May 30, 2006), http://news.bbc.co.uk/2/hi/europe/5028918.stm; L.Pasveeer, "Court outlaws EU-U.S. passenger data transfer," C|net news.com (May 30, 2006) http://news.com.com/2100-1029_3-6077893.html; G.Meade, "MEPs Block US Counter-Terrorism Deal," scotsman.com (April 21, 2004), http://news.scotsman.com.

648 Agreement between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) (July 23, 26, 2008), *available at* http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf.

649 "Privacy Chief Warns EU on Terror Laws," http://www.out-law.com/page-8139.

European Parliament's July 5, 2006, resolution condemning the U.S. covert surveillance[650]) found that, while sharing some data on financial transfers was essential in the fight against terrorism, adequate safeguards were required that would ensure that European privacy rules would be observed. In particular, the use of the data should have been limited to terrorism investigations, with a time limit on the retention of the information. SWIFT's defense that, with offices in the U.S., it was bound by U.S. law and required to turn over the data in response to validly issued administrative subpoenas, was rejected because SWIFT was also subject to Belgian law. [651] The report concluded that SWIFT had violated the EU's 1995 Data Protection Directive[652] The EU Article 29 Working Party came to the same conclusion,[653] and in June of 2007, issued to institutions using SWIFT a compliance deadline of September 1, 2007.[654] The U.S. Treasury Department subsequently provided commitments to the EC with respect to its use of the personal information, including agreements to provide certain independent safeguards governing the use of the data.[655] Eventually, SWIFT announced it would stop processing European banking transactions in the U.S.[656] and has opened a new operating center in Switzerland to maintain and process intra-EU messages not subject to 'Trans-Atlantic' data harvesting concerns.[657] In April 2010, the US and EU reached a political agreement on a mandate for the processing and transfer of financial messaging data for purposes of SWIFT. The agreement, which was approved in June 2010, provides strict safeguards regarding the transfer of data and establishes a system equivalent to the US Terrorist Finance Tracking program (TFTP).[658]

These issues have arisen in the context of domestic privacy regulation as well. The Electronic Privacy Information Center complained to the Federal Trade Commission requesting an investigation of the JetBlue disclosure[659] and several U.S. government investigations reissued.[660] Other airlines made similar disclosures, and a class action was brought against Northwest Airlines for violating its posted privacy policy. A court decision dismissed the case on the ground that the plaintiffs did not claim to have read the privacy policy – a decision that

---

650 *See SWIFT: Passing Customer Personal Data to the U.S. Treasury*, WORLD DATA PROTECTION REPORT (BNA) 13 (Jan. 2008).

651 D. Bilefsky, "Data Transfer Broke Rules, Report Says," N.Y.TIMES (Sept. 28, 2006), http://www.nytimes.com/2006/09/28/world/europe/28cnd-swift.html.

652 Directive 95/46/EC of October 24, 1995. The Directive prohibits the unauthorized access to individual's personal data with consent.

653 Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT), Article 29 Data Protection, Working Party, 01935/06/EN WP128 (Nov. 22, 2006), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf.

654 *See SWIFT, supra*.

655 *SWIFT, supra.*

656 *SWIFT to stop processing EU banking data in the US*, THE REGISTER (Oct. 15, 2007), *available at* http://www.theregister.co.uk/2007/10/15/swift_processing_halt/print.html.

657 *SWIFT, supra;* "EU Approves Data-Sharing SWIFT Agreement with US Authorities," http://www.dw-world.de/dw/article/0,,4952263,00.html; "SWIFT: New EU-US Agreement will be Renegotiated Next Year," http://www.europarl.europa.eu/sides/getDoc.do?language=en&type=IM-PRESS&reference=20090915IPR60697.

658 *Id*.

659 Electronic Privacy Information Center Complaint and Request for Injunction, Investigation and for Other Relief, *Matter of JetBlue Airways Corp., available at* http://epic.org/privacy/airtravel/jetblue/ftccomplaint.html; *See also* "JetBlue Retains Deloitte & Touche To Assist The Airline In Its Analysis Of Its Privacy Policy," JetBlue Press Release (Sep. 22, 2003), *available at* http://www.highbeam.com/doc/1G1-108017873.html.

660 T. Katzer, "Senators Probe Airliner Passenger Security Breaches," Information Week (April 14, 2004), http://www.informationweek.com/news/18901493?queryText=%22Senator%20Probe%22.

has brought criticism from privacy advocates.[661] The incident illustrates the need for companies to abide by their own privacy policies, unlike companies that have handed to the government entire databases in violation of their own privacy policies in an effort to assist with terrorist investigations.[662]

The tension between privacy and security manifest themselves in other contexts as well. Indeed, the Department of Homeland Security has appointed a Chief Privacy Officer, Nuala O'Connor Kelly, to address these issues. Her speech on the second anniversary of 9/11 directly addressed the need to respect privacy as the Department addresses security.[663] Nonetheless, conflicts have arisen, a few examples of which follow.

The USA PATRIOT Act,[664] enacted in the wake of September 11, provides expanded powers to the government that have raised privacy concerns. The Act, for example, provides authority for the government to obtain library records,[665] provoking a heated response from the American Library Association in the form of a resolution relating to the Act and its analysis of "The USA Patriot Act in the Library."[666] Unsurprisingly, the Department of Justice's view of the Act is rather different, as expressed in an article available on its website.[667]

The USA PATRIOT Act also requires, in Title III, that U.S. financial institutions undertake measures to combat money laundering and terrorist financing. Section 326 of the Act went into effect in October 2003 and requires banks, broker-dealers, mutual funds, futures commission merchants, and introducing brokers to obtain certain identifying information from their customers.[668] At a minimum, these financial institutions are required to obtain the name,

---

661 *Northwest Airlines Privacy Litigation*, 2004 WL 1278459 (D. Minn. 2004); *see* P. Festa "Judge Tosses Online Privacy Case," ENetNews.com (June 16, 2004), http://news.com.com/2100-1023-5234971.html.

662 Companies typically require a warrant or court order before relinquishing the contents of electronic files to the government. Companies may soon look to rewrite their privacy policies to include provisions that would enable them to make records available to the government in the event of a national emergency. Stefanie Olsen, "Companies rethink Net privacy after attacks," CNET.COM (Oct. 2, 2001), http://news.com.com/2100-1023-273767.html. *See also* J. Canham, "Security on the Internet – At the Cost of Privacy?," WORLD INTERNET L. REP. (BNA) (Nov. 2001), at 34.

663 Remarks of Nuala O'Connor Kelly, Chief Privacy Officer, Before the 25th International Conference of Data Protection and Privacy Commissioners (Sep. 11, 2003), *available at* http://www.dhs.gov/xnews/speeches/speech_0144.shtm.

664 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

665 *Id.* at § 215 amending the Foreign Intelligence Surveillance Act, tit. V, § 501(a)(1).

666 American Library Ass'n, "Resolution on the USA Patriot Act and Related Measures that Infringe on the Rights of Library Users" (Jan. 29, 2003), *available at* http://www.ala.org/Template.cfm?Section=IF_Resolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11891; American Library Ass'n, "The USA Patriot Act in the Library" (), *available at* http://www.ala.org/Template.cfm?Section=Intellectual_Freedom_Issues&Template=/ContentManagement/ContentDisplay.cfm&ContentID=5195. *See also* American Library Ass'n, "Privacy: An Interpretation of the Library Bill of Rights" (June 19, 2002), *available at* http://staging.ala.org/Template.cfm?Section=Interpretations&Template=/ContentManagement/ContentDisplay.cfm&ContentID=8613.

667 U.S. Dep't of Justice, "The USA PATRIOT Act: Preserving Life and Liberty" DOJ's "Preserving Life and Liberty," *available at* http://www.lifeandliberty.gov (page modified Dec. 11, 2003).

668 *See* Financial Crimes Enforcement Network; Treasury; Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Office of Thrift Supervision, Treasury; National Credit Union Administration; "Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks"; joint final rules. 68 Fed. Reg. 25090-25113 (May 9, 2003); Financial Crimes Enforcement Network; Treasury; Securities and Exchange Commission;

address, date of birth, and social security number (if a U.S. person) or passport number or alien identification number (if a non-U.S. person). These types of collected information fall under the category of nonpublic personal information, the privacy of which is protected under the Gramm-Leach-Bliley Act[669], and, as such, these financial institutions are required to safeguard this collected information. However, the USA PATRIOT Act regulations are silent with respect to safeguarding the collected identifying information. The government has not explicitly reminded financial institutions and their customers that the collected information is subject to the protections of Gramm-Leach-Bliley; it is important to bear in mind that any disclosure of such nonpublic personal information to third-parties, including law enforcement authorities, must be in accordance with the provisions of Gramm-Leach-Bliley.[670]

K. *Internet Access for Persons with Disabilities*

Another issue faced by website operators is whether an internet site must comply with the requirements of federal and state laws protecting persons with disabilities. For example, "[t]o ensure that the disabled have full and equal enjoyment of the goods and services of places of public accommodation, the Americans with Disabilities Act ("ADA") requires 'reasonable modification' of 'policies, practices, and procedures,' the provision of auxiliary aids to ensure effective communication with the disabled, and the removal of architectural and communications barriers."[671]

In *National Federation of the Blind v. Target Corporation*,[672] an organization dedicated to assisting blind and disabled persons brought a class action suit against Target under the ADA stemming from the alleged inaccessibility of Target.com to blind individuals. Specifically, the plaintiffs maintained that Target could have designed a website accessible to the blind with simple and inexpensive technology by imbedding invisible code beneath graphics. This code enables a blind individual to use a screen reader which vocalizes the text and describes webpage content. The defendants moved to dismiss on the basis that Target.com is not a physical space or a place of public accommodation within the meaning of the ADA. The court denied the defendants' reasoning and made clear that the ADA protects individuals with disabilities seeking to use a website in conjunction with a physical store:

> [C]onsistent with the plain language of the statute, no court has held that … a plaintiff has a cognizable claim only if the challenged service prevents physical access to a pubic accommodation. Further, it is clear that the purpose of the statute is broader than mere physical access-seeking to bar actions or omissions which

"Customer Identification Programs for Broker-Dealers"; joint final rule. 68 Fed. Reg. 25113-25131 (May 9, 2003); Financial Crimes Enforcement Network; Treasury; Securities and Exchange Commission; "Customer Identification Programs for Mutual Funds"; joint final rules. 68 Fed. Reg. 25131-25149 (May 9, 2003); Financial Crimes Enforcement Network; Treasury; Commodity Futures Trading Commission; "Customer Identification Programs for Futures Commission Merchants and Introducing Brokers"; joint final rules. 68 Fed. Reg. 25149-25162 (May 9, 2003).

669 Pub. L. 106-102 (2000).

670 *See* Section 502 of the Gramm-Leach-Bliley Act.

671 *National Federation of the Blind v. Target Corp.*, 452 F. Supp. 2d 946, 951 (N.D. Cal. 2006) (citing 42 U.S.C. § 12182(b)(2)(A)(ii-iv).

672 *Id.*

> impair a disabled person's "full enjoyment" of services or goods of a covered accommodation.[673]

The court denied the defendants' motion to dismiss, reasoning that "the challenged service here is heavily integrated with the brick and mortar stores and operates in many ways as a gateway to the store."[674] In August 2008, the parties finalized a settlement of the case. The settlement includes Target's payment of $6,000,000 divided among the class members plus attorneys' fees and costs. The settlement also stipulates that Target provide website service fully accessible to blind people, among other things.[675]

The *Target* case may cause disability rights groups around the world to carefully monitor the website accessibility of companies doing business on the web.[676]

A pair of conflicting 2012 federal court decisions shows that the law is still developing on this issue. In *Cullen v. Netflix, Inc.*, the Northern District of California held that a website is "not a place of public accommodation" and that "the ADA does not apply to access to [the website's] streaming library."[677] However, just weeks earlier, the District of Massachusetts held in *National Ass'n of the Deaf v. Netflix, Inc.* that the "Watch Instantly" streaming page of Netflix's website constitutes a place of "public accommodation," because it "falls within at least one, if not more, of the enumerated ADA categories."[678] The findings in *Cullen* and *National Ass'n of the Deaf* suggest that it will only be a matter of time before the appellate courts − and perhaps the Supreme Court − have their say on whether the ADA is applicable to website accessibility.

In 2010, President Obama signed the Twenty-First Century Communications and Video Accessibility Act of 2010 into law, which extends the disability access requirements of the Communications Act of 1934 to IP-enabled communications such as text-messaging, video conferencing, video delivery, and VoIP services.[679] Other provisions of the Act require that mobile phone manufacturers make their Internet browsers accessible to the visually impaired, that television shows or movies delivered over the Internet be closed captioned or contain audio descriptions, and that VoIP services be compatible with hearing aids.

---

673 *Id.* at 953-54 (quoting 42 U.S.C. § 12182(a)).

674 *Id.* at 955; *compare with Access Now v. Southwest Airlines*, 227 F.Supp.2d 1312 (S.D. Fla. 2002) (holding that an airline's website, www.southwest.com, was not a place of public accommodation because there was no nexus between denial of goods and services offered via the airline's website, and denial of goods and services offered at a comparable brick-and-mortar store location).

675 Press release of the Disability Rights Advocates and settlement details, *available at* http://www.dralegal.org/cases/private_business/nfb_v_target.php.

676 *See, e.g., The Technology Law Newswire Service*, Eversheds (Oct. 2, 2008) (noting that the U.S. *Target* case may prompt disability rights group in the U.K. to take action under the British Disability Discrimination Act of 1995).

677 880 F.Supp.2d 1017 (N.D. Cal. 2012).

678 869 F.Supp.2d 196 (D. Mass. 2012).

679 "New Law Extends Disability Access Requirements to IP-Enabled Communications" (Steptoe's E-Commerce Law Week, 21 Oct. 2010), *available at* http://www.steptoe.com/publications-7227.html.

II. *Mass Market Software Issues*

A. *Loss of Trade Secrets by Mass Distribution*

A decision that should be of particular concern to software publishers is *Stac Electronics v. Microsoft Corp.*,[680] which awarded damages for misappropriation of trade secrets in Microsoft's MS-DOS 6.0 software, but refused injunctive relief, holding that the trade secrets had been lost by the distribution of millions of copies of the software to customers, who could have reverse-engineered it and discovered the trade secrets. If followed, this decision seems to spell the end of trade secret protection for all software widely distributed, even in object code form, without enforceable contractual provisions against reverse-engineering.[681] The *Stac* court did not appear to consider whether such reverse-engineering would have violated Microsoft's copyright rights.

[680] CV-93-413-ER (C.D. Cal. 5/13/94 and 6/8/94), *reported in* 48 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 165 (1994), *app. voluntarily dismissed*, 38 F.3d 1222 (Fed. Cir. 1994).

[681] While not specifically targeting trade secrets, some companies have been relying on the Computer Fraud and Abuse Act to prosecute and criminalize the theft of trade secrets. http://www.law.com/jsp/article.jsp?id=1202458635753&rss=newswire.

B. *Enforceability of Shrinkwrap and Clickwrap Licenses*

Software publishers almost universally follow a practice of licensing software to users by means of license agreements printed on the outside of a retail package or on an inner envelope containing program disks, or displayed on the user's screen with acceptance required before the software will proceed.[682] Such so-called "shrinkwrap licenses" received a significant boost from the Seventh Circuit in *ProCD, Inc. v. Zeidenberg.*[683] Until the *ProCD* decision, the few courts considering the question had ruled against the enforceability of shrinkwrap licenses, at least in the circumstances of the specific cases.

Thus in *Vault v. Quaid Software Ltd.*,[684] the Fifth Circuit held that shrinkwrap licenses were unenforceable, notwithstanding a state statute validating them. The statute, held the court, was preempted by federal copyright law, and a license term prohibiting reverse engineering was unenforceable as conflicting with the rights the court viewed as granted by copyright law.

A few years later, the Third Circuit invalidated a shrinkwrap license in *Step-Saver Data Systems, Inc. v. Wyse Technology*,[685] in the context of sales by a software company to a software retailer. In *Step-Saver*, the retailer's telephone orders were accepted with no mention of additional terms, but arrived with a shrinkwrap license disclaiming warranties and limiting remedies. The Court held the license terms were not part of the purchase agreement, declined to enforce a disclaimer "made available only after the contract is formed,"[686] and held that the fact that the proposed terms were made known to the buyer as a result of previous sales did not alter the failure to agree to them before the later purchase contracts were formed.[687]

In a well-reasoned economic analysis, the Seventh Circuit, in an opinion by Judge Easterbrook, arrived at the opposite conclusion, holding that "[s]hrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general (for example if they violate a rule of positive law, or if they are unconscionable."[688]

Judge Easterbrook found the shrinkwrap license to be a method of enabling the supplier of a national business address list database to enforce price discrimination, charging a low price to the general public for personal use, while charging a higher price to commercial users. This benefits both personal users, who have access to a product otherwise unaffordable, and commercial users, who would otherwise have to pay more because the supplier could not obtain any contribution from the consumer market. The defendant in *ProCD* bought a consumer version of the database and, in violation of the shrinkwrap license, made the database available on the Internet to anyone willing to pay its price, which was for less than the ProCD price to commercial users.

---

682 Not all courts recognize such licenses as licenses rather than sales. *Compare Softman Products Co. LLC v. Adobe Systems Inc.*, 171 F. Supp.2d 1075 (C.D. Cal. 2001) (Adobe software was sold, not licensed, to distributors; restrictions on resale not enforceable); *with Adobe Systems Inc. v. One Step Micro Inc.*, 84 F. Supp. 2d 1086 (N.D. Cal. 2000) (finding Adobe software was licensed, not sold).

683 86 F.3d 1447 (7th Cir. 1996).

684 847 F.2d 255 (5th Cir. 1988).

685 939 F.2d 91 (3d Cir. 1991).

686 *Id.* at 104-105 n. 45.

687 *See also Arizona Retail Systems, Inc. v. Software Link, Inc.*, 831 F. Supp. 759 (D. Ariz. 1993).

688 *ProCD Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996); *see also, McKee v. AT&T Corp.*, 191 P.3d 845 (Wash. 2008) (where consumer was not provided with a copy of AT&T's service agreement at the time he signed up for service, and only received the terms and conditions 10 days to two weeks after he subscribed for service, terms related to dispute resolution found unconscionable under Washington's Consumer Protection Act).

Treating the licenses as ordinary contracts governed by the U.C.C., the Seventh Circuit observed that "[n]otice on the outside, terms on the inside, and a right to return the software for a refund if the terms are unacceptable . . . may be a means of doing business valuable to buyers and sellers alike," as it allows the outside of the package to be used for information buyers might find more useful than fine print license terms.[689] The Seventh Circuit saw little difference between this approach and the sale of airline and cruise tickets containing elaborate terms not disclosed when a telephone purchase is made.[690] Concert tickets containing a legend prohibiting recording, consumer goods containing warranty terms, and drugs with detailed package inserts are similar.

The Seventh Circuit saw no reason to prohibit such alternative methods of contract formation and the transaction efficiencies they bring, and found such methods authorized by Section 2-204(1) of the U.C.C., which permits a contract for sale of goods to "be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract." ProCD proposed such "a contract that the buyer would accept by using the software after having an opportunity to read the license at leisure" and Zeidenberg did so, since the software displayed the license on the screen and required acceptance before proceeding.

The Seventh Circuit concluded: "Terms of use are no less a part of 'the product' than are the size of the database and the speed with which the software compiles listings. Competition among vendors, not judicial revision of a package's contents, is how consumers are protected in a market economy." It also concluded that such a private contractual arrangement limiting the use of the copyrighted works was not preempted by the copyright laws, any more than an agreement to return a rented videotape after two days or to refrain from using a law student's educational LEXIS account for commercial purposes would be preempted.

While the law remains unsettled, *ProCD* provides some comfort to those using shrinkwrap licenses.[691] The extent of that comfort will depend on whether other circuits, and ultimately the Supreme Court, decide to follow it, but the trend so far appears favorable.[692]

Similar questions arise regarding the enforceability of so-called "clickwrap" licenses that appear on a website prior to access to specified features or software. Courts have generally enforced such agreements at least where the agreement was prominent and the customer's assent clearly manifested. Thus, the D.C. Circuit upheld a clickwrap contract and its forum selection clause, where consumers were required to click an "Accept" button below the scroll box containing the agreement and the very top of the agreement contained a notice to "PLEASE

---

689 *See also, Hill v. Gateway 2000 Inc.*, 105 F.3d 1147 (7th Cir. 1997) (as long as purchasers have means of reviewing the terms – such as by asking in advance or by inspecting them after delivery but before use – the enforcement if such terms is not unfair).

690 Citing *Carnival Cruise Lines v. Shute*, 499 U.S. 595 (1991).

691 *But see Softman Products Co., LLC v. Adobe Systems Inc.*, C.D. Cal., No. CV 00-04161 DDP (Oct. 19, 2001) (In ruling that despite a shrinkwrap license on bundled software a software distributor is entitled to unbundle such software and sell components separately the Court declined to rule on the general validity of shrinkwrap licenses, although the opinion did state that "[r]eading a notice on a box is no equivalent to the degree of assent that occurs when the software is loaded onto the computer and the consumer is asked to agree to the terms of the license.").

692 The Federal Circuit followed *ProCD* in *Bowers v. Baystate Technologies, Inc.*, 320 F.3d 1317 (Fed. Cir. 2003). *See also Arizona Cartridge Remanufacturers Ass'n Inc. v. Lexmark Int'l Inc.*, 421 F. 3d 981 (9th Cir. 2005) (enforcing restrictions printed on outside of printer cartridge package) ; *Meridian Project Systems Inc. v. Hardin Construction Co.*, No. Civ. S-04-2728, 426 F. Supp.2d 1101, (E.D. Cal. 2006) (enforcing shrinkwrap license contained within box containing software media, following *ProCD*), *available at* http://pub.bna.com/ptcj/0402728Apr6.pdf.

READ THE FOLLOWING AGREEMENT CLOSELY."[693] A similar result was reached by a Canadian court in the case of an agreement where the user had to click "I agree" to proceed, and explicitly stated that the user would be bound to all the terms of the agreement even if the user did not read them.[694]

Results have been more mixed in the case of so-called "browsewrap" contracts where terms and conditions are posted on a website but no specific act of acceptance such as clicking an "I accept" button is required. The Second Circuit refused to enforce a clickwrap contract where the user was permitted to download software without having to manifest acceptance, and notice of the existence of contract did not appear on the first screen, where the download was available, but was only visible if the user scrolled down the page.[695] The Ninth Circuit has held that a company cannot unilaterally change the terms of an agreement simply by posting changed terms online without notice to its customer.[696] More recently, the Second Circuit in *Schnabel v. Trilegiant Corp.* held that an arbitration provision sent by e-mail to customers after they had enrolled in an online discount shopping program did not provide sufficient notice to these customers that they had agreed to arbitrate any dispute in accordance with the online program's "terms and conditions."[697] And the United States District Court for the Northern District of Texas ruled that a company's online terms of use agreement that reserved to the website operator the right to unilaterally modify the agreement was an unenforceable "illusory contract."[698] In another case, where terms of use for domain name registration data were displayed only after a query was made, however, the Second Circuit held that a competitor, which accessed the

---

693 *Forrest v. Verizon Communications, Inc.*, 805 A.2d 1007 (D.C. Ct. App. 2002); *In re RealNetworks, Inc. Privacy Litigation*, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. 2000); *Decker v. Circus Circus Hotel*, 49 F. Supp. 2d 743 (D.N.J. 1999); *Caspi v. Microsoft Network, LLC.*, 732 A. 2d 528, 323 N.J. Super. 118 (N.J. Super. App. Div. 1999); i.*LAN Systems, Inc. v. Net Scout Service Level Corp.*, No. 00-11489-WGY (D. Mass. Jan. 2, 2002), *reported at* 63 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 268 (Jan. 25, 2002) *available at* http://pub.bna.com/ptcj/0011489.pdf; *Scherillo v. Dun & Bradstreet, Inc.*, No. 09-cv-1557 (JFB)(ARL), 2010 WL 537805 (E.D.N.Y. 2010) (forum selection provision in clickwrap agreement enforceable where user clicked on "I agree" and "complete registration" boxes next to the terms and conditions; the fact that user had to "scroll" through text to get to forum selection clause does not affect analysis).

694 *Rudder v. Microsoft Corp.*, 2 C.P.R. 4(th) 474 (Ont. S.C.J. 1999).

695 *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002); *see also Hines v. Overstock.com*, 668 F. Supp. 2d 362, 367 (E.D.N.Y. 2009) (arbitration clause in browserwrap agreement accessible via link at bottom of page unenforceable where user "lacked notice of the Terms and Conditions because the website did not prompt her to review [it] and because the link [to it] was not prominently displayed …"); *In re Zappos.com, Inc.* 893 F.Supp.2d 1058 (D. Nev. 2012) (following *Hines*, arbitration clause held unenforceable where inconspicuous link was buried in the middle to bottom of each of the pages of retailer's website amongst similar-looking links); *but see Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 7, 2003) (enforcing terms and conditions where website included prominent notice on home page that use of interior pages was subject to terms and conditions, and evidence showed defendants' knowledge thereof); *Net2Phone, Inc. v. Super. Ct. Los Angeles County*, 109 Cal.App.4th 583 (Cal.Ct.App.Dist. 2003).

696 *Douglas v. U.S. Dist. Ct. C.D.Cal. and TalkAmerica, Inc.*, 495 F.3d 1062 (9th Cir. 2007); *see also Harris v. Blockbuster Inc.*, 622 F. Supp. 2d 396 (N.D. Tex. 2009) (arbitration provision in online TOU was illusory and unenforceable where Blockbuster reserved the right to modify the TOU at any time at its sole discretion); *but see Margae, Inc. v. Clear Link Techs., LLC*, No. 2:07-CV-916 TC (D. Utah 2008) (clickwrap agreement granting company the unilateral right to post an amended agreement upheld with respect to an arbitration clause where the user "had reason to continually visit the website that contained a link to the Amended Agreement").

697 697 F.3d 110 (2d Cir. 2012)

698 The Court also denied the website's motion to compel contractually required individual arbitration of the plaintiff's privacy claims. *Harris v. Blockbuster Inc., available at* https://ecf.txnd.uscourts.gov/cgi-bin/show_public_doc?2009cv0217-32.

database repeatedly and therefore was effectively on notice of the terms of use, was bound by them.[699] The Central and Northern Districts of California have reached similar conclusions.[700] And the Northern District of Texas held that Southwest Airlines' website terms of use were enforceable against a defendant after Southwest's cease and desist letter had put the defendant on notice of the terms.[701] The Supreme Court of Canada upheld the enforceability of an arbitration clause contained in an online agreement available on Dell's website via a hyperlink, finding such a link to be "reasonably accessible."[702]

The enforceability of clickwrap licenses also remains subject to ordinary contract principles, such as unconscionability.[703]

The Business Law Section of the American Bar Association has attempted to aid on-line merchants by setting forth fifteen strategies to guide the structure and implementation of on-line agreements. The strategies have been broken down into six conceptual categories: (1) opportunity to review terms; (2) display of terms; (3) rejection of terms and its consequences; (4) assent to terms; (5) opportunity to correct errors; and (6) record keeping to prove the consumer's assent.[704]

Moreover, clickwrap licenses necessarily rely on the authority of the "clicker" to agree. For instance, a United States District Court for the Southern District of Florida declined to enforce a defendant company's clickwrap End User License Agreement – which contained forum selection and arbitration clauses – where the plaintiff's employees "clicked-to-accept" the terms

---

699 *Register.com v. Verio, Inc.*, 356 F.3d 343 (2d Cir. 2004). *See also Jet Blue Airways Corp. Privacy Litigation*, 379 F. Supp.2d 299 (E.D.N.Y. 2005) (website privacy policy available by hyperlink is enforceable part of airline ticket); *Hubbert v. Dell Corp.*, 835 N.E.2d 113 (Ill. App. Ct. 2005), *available at* http://www.state.il.us/court/Opinions/AppellateCourt/2005/5thDistrict/August/html/5030643.htm.

700 *Ticketmaster L.L.C. v RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (JWJx) (C.D. Cal. 2007); *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-5780 JF (RS), 2009 WL 1299698 (N.D. Cal. 2009) (defendant's motion to dismiss copyright action denied where, among other things, defendant continued to violate the TOU by using automated "scrap[ing of] Facebook's website, despite technological security measures to block such access" and the parties' "fruitless" negotiations).

701 *Southwest Airlines Co. v. BoardFirst, L.L.C.*, Civ. Action No. 3:06-CV-0891-B, 2007 WL 4823761 (N.D. Tex. Sept. 12, 2007).

702 *Dell Computer Corp. v. Union des Consommateurs*, 2007 SCC 34 (Sup. Ct. Canada 2007), *available at* http://scc.lexum.umontreal.ca/en/2007/2007scc34.html.

703 *Comb v. PayPal, Inc.*, 218 F.Supp.2d 1165 (N.D. Cal. 2002) (arbitration clause in clickwrap agreement deemed unconscionable, unenforceable, and a one-sided contract of adhesion). The Court in *Comb* also expressed doubt as to whether the users had actually agreed to the contract. *See also Aral v. Earthlink, Inc.*, 36 Cal.Rptr.3d 229 (Cal. Ct. App. 2005) (arbitration clause in clickwrap agreement unenforceable contract of adhesion discouraging legitimate claims).

704 Christina L. Kunz, et al., *Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent*, 57 BUS. LAW. 401 (Nov. 2001) (produced by the Working Group on Electronic Contracting Practices of the Electronic Commerce Subcommittee of the Cyberspace Law Committee of the Business Law Section of the American Bar Association). Dell Canada's agreement described at "Dell's Software License Policy – Dude, You're Getting Screwed," http://www.cypherpunks.ca/dell.html, would not appear to qualify, although a Canadian court has held a website's terms of use enforceable even without a required "I agree" click, at least when there was evidence of knowledge of the terms of use. *Canadian Real Estate Ass'n v. Sutton (Quebec) Real Estate Services, Inc.*, Montreal, No. 500-05-074815-026 (Quebec Super. Ct., April 10, 2003), *available at* http://www.canlii.org/fr/qc/qccs/doc/2003/2003canlii22519/2003canlii22519.html. A contrary result was reached, however, with respect to disclaimers posted on Merrill Lynch's HSBC's NetTrades website, which were held unenforceable because they disclaimed liability even for gross negligence. *See Wei Zhu v. Merrill Lynch HSBC*, 2002 BCPC 0535, (B.C. Prov. Ct.), *available at* http://www.provincialcourt.bc.ca/judgments/pc/2002/05/p02%5F0535.htm.

of the defendant's EULA without actual or apparent authority.[705] In so holding, the court relied on the fact that the plaintiff had expressly informed the defendant that only three specific executives had authority to enter into agreements on the plaintiff's behalf.[706] On the other hand, a court held with little elaboration that a 19-year old website manager, who registered his company on a merchant website, had apparent authority to bind the company to the terms of a clickwrap agreement where "[n]o one has claimed that he was not of legal contracting age or of sound mind."[707]

Note that European consumer protection law may render unenforceable consumer contracts that are deemed to be unfair or imprecise. A French court invalidated over thirty provisions of AOL's French subscriber contract, including a provision that use of the website constituted acceptance of the contract.[708]

Finally, courts have differed as to whether a statement on a paper invoice referencing terms and conditions posted on a website is sufficient to make those terms binding on consumers. The conspicuousness of the reference appears to be key.[709] Needless to say, from the licensee standpoint, it is always a good idea to read the clickwrap license before "clicking" to agree, although in practice this seems more the exception than the rule.[710]

C. *Use of Licenses Instead of Sales*

Traditionally, because of the ease of copying, software publishers have licensed, rather than sold their software, so as to avoid the freedom of purchasers under the "first sale doctrine" of the Copyright Act,[711] to sell and otherwise dispose of lawfully made copies. Courts have varied in their treatment of this approach, with some courts holding that a license to use software was not a sale under the first sale doctrine, and thus did not provide the basis for the resale of

---

705 *Nat'l Auto Lenders, Inc. v. SysLOCATE, Inc.*, 686 F.Supp.2d 1318 (S.D. Fla. 2010).

706 *Id.* at *1, 3 (also noting that the plaintiff had "instructed its entire … staff to refrain from logging onto the [defendant's] website to prevent involuntary acceptance of the EULA").

707 *Appliance Zone, LLC v. Nextag, Inc.*, No. 4:09-cv-0089-SEB-WGH, 2009 WL 5200572 (S.D. Ind. 2009) (clickwrap agreement enforceable where "NexTag made the Agreement highly visible and easily accessible, and required as well an affirmative acceptance of the terms of the Agreement as a prerequisite to completing registration;" moreover, "the contract on Appliance Zone's own website appears to be substantively similar to the one on NexTag's website").

708 *Union Fédérale des Consommateurs v. AOL France,* Court of First Instance of Nanterre (June 2004), *summary available at* https://litigationessentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=1+N.Y.U.+J.+L.%26+Bus.+881&srctype=smi&srcid=3B15&key=19330f4fdbbced6ff72937947a1003e4.

709 *Compare Manasher v. NECC Telecom*, 2007 WL 2713845 (E.D. Mich. Sept. 18, 2007) (reference to online agreement in fifth box on second page of invoice inadequate to make agreement binding) *with Briceno v. Sprint Spectrum, L.P.*, 911 So. 2d 176 (Fla. App. 2005) (reference on first page of each invoice with boldface header advising of changes in terms and conditions previously provided is adequate to make changed terms enforceable).

710 On April 1, 2010, an online retailer UK video game company, Gameplay (GB), demonstrated the inherent problems in a clickwrap license through an April Fool's Day prank. The terms of the license stipulated that the purchasers would grant to GB a non-transferable, perpetual option "to claim, for now and forever more, your immortal soul." Moreover, the provision stated that such purchasers agreed to surrender their soul within 5 business days of written notification by GB "or one of its authorized minions" by notice to be delivered "through six foot high letters of fire," and further provided that GB had no liability for damages caused by such act. At the end of the provision, purchasers were told that they could click on a link to nullify the provision (and upon doing so were awarded a voucher of £5.00). Not surprisingly, just over 10% of people read the terms and conditions and received a voucher. "Immortal Souls and Standard Form Agreements: Reminders After April Fool's Prank," Lang Michener LLP (May 14, 2010).

711 17 U.S.C. § 109(a).

software acquired in violation of a license agreement,[712] while others have found such transactions to constitute sales notwithstanding agreements characterizing them as licenses.[713]

In one recent case, *Apple, Inc. v. Psystar Corp.*, the Ninth Circuit confirmed a three part test for distinguishing a license from a sale in the context of software: a license, as opposed to a sale, will exist where: (1) the copyright owner specifies that the user is granted a license, (2) the copyright owner restricts the user's ability to transfer the software, and (3) notable use restrictions are imposed. [714]

III. *Copyright Misuse and Trade Secret Preemption*

Since the 1990s a doctrine of copyright misuse has arisen in some courts, with significant input on the ability of a copyright holder to limit the activities of its licensees.

A. *Copyright Misuse*

Lasercomb America, Inc. v. Reynolds,[715] was the first significant case to apply the copyright misuse doctrine. There, the Fourth Circuit held that a license agreement for software prohibited the licensee from developing its own competing software, thus improperly extending copyright protection from the particular expression to the idea of such software. That misuse was held a bar to an action for infringement, even against a blatant copier who did not itself sign such a restrictive license agreement.[716]

Thereafter, the Fifth and Ninth Circuits adopted the copyright misuse defense in *Alcatel USA, Inc. v. DGI Technologies, Inc.*,[717] *DSC Communications Corp. v. DGI Technologies, Inc.*[718] and *Practice Management International Corp. v. American Medical Association*[719].

---

712 *Adobe Systems Inc. v. Stargate Software Inc.*, 216 F. Supp. 2d 1051 (N.D.C.A1. 2002); *Adobe Systems Inc. v. One Stop Micro Inc.*, 84 F. Supp. 2d 1086 (N.D. Cal. 2000); *Microsoft Corp. v. Harmony Computers & Electronics, Inc.*, 846 F. Supp. 208, 212-13 (E.D.N.Y. 1994); *Vernor v. Autodesk Inc.*, 2010 WL 3516435 (9th Cir. Sept. 10, 2010) (holding that a software user is a licensee rather than an owner of a software copy where the copyright owner (i) specifies that the user is granted a license, (ii) significantly restricts the user's ability to transfer the software and (iii) imposes notable use restrictions).

713 *E.g., Softman Products Co. LLC v. Adobe Systems Inc.* 171 F.Supp.2d 1075 (C.D. Cal. 2001); *Novell, Inc. v. CPU Distributing, Inc.*, 2000 U.S. Dist. LEXIS 9975 (S.D. Tex. 2000); *Applied Information Management, Inc. v. Icart*, 976 F. Sup. 149 (E.D. N.Y. 1997) (whether "license" was actually a sale was disputed questions of fact); *Novell, Inc. v. Network Trade Center, Inc.*, 25 F. Supp.2d 1218 (D. Utah 1997).

714 2011 U.S. App. LEXIS 19707 (9th Cir., Sept. 28, 2011) (holding Apple's software was licensed, not sold, to Psystar as a result of the terms of its software license agreement) as reported in Herman et. al, *Apple v. Psystar underscores the strength of software license agreements and the limits of the copyright misuse defense*, Lexology (Oct. 20, 2011).

715 911 F.2d 970 (4th Cir. 1990).

716 *See also PRC Realty Systems, Inc. v. Nat'l Ass'n of Realtors*, 972 F.2d 341 (4th Cir. 1992) *qad v. ALN*, 770 F. Supp. 1261 (N.D. Ill. 1991) (appeal of this issue dismissed, 974 F.2d 834) (holding that an effort to sue for infringement of the non-copyrightable portion of a program was copyright misuse, making the entire copyright unenforceable).

717 166 F.3d 772 (5th Cir. 1999) (agreement limiting use of operating system software to copyright owner's microprocessor cards was copyright misuse providing patent-like protection against development of competing hardware).

718 81 F.3d 597, 601-02 (5th Cir. 1996) (same).

719 121 F.3d 516 (9th Cir. 1997) (AMA's license of its medical procedure codes to a federal agency on condition the agency not use any competing code system was copyright misuse). *See also In re Independent Service*

The *Lasercomb* Court held it irrelevant that the restriction was reasonable under antitrust standards, finding the restrictive license to violate the public policy embodied in the copyright grant. In *Alcatel/USA* the Fifth Circuit rejected an antitrust claim, but nonetheless upheld the misuse defense. Nevertheless, some courts have stated that the defense is inapplicable in the absence of an antitrust violation[720].

Moreover, at least one court – relying on *Lasercomb* – has allowed a defendant to plead a copyright misuse *counterclaim*. Finding copyright misuse counterclaims analogous to patent misuse claims, the court in *Apple Inc. v. Psystar Corp.*[721] held that the defendant could amend its answer to assert a copyright misuse counterclaim. In so holding, the court rejected Apple's contention that copyright misuse may only be alleged as an affirmative defense:

> This [court] is unconvinced, however, that misuse may never be asserted as a counterclaim for declaratory relief. PsyStar may well have a legitimate interest in establishing misuse independent of Apple's claim against it, for example, to clarify the risks it confronts by marketing the products at issue in this case or others it may wish to develop. Moreover, if established, misuse would bar enforcement … not only as to defendants who are actually a party to the challenged license but also as to potential defendants not themselves injured by the misuse who may have similar interests.[722]

In an expansion of this principle, the U.S. District Court for the Central District of California held that Omega, S.A.'s "offensive" use of its copyright in the design on the backs of its watches to prevent unauthorized importation of those watches into the country constituted copyright misuse by seeking to extend the copyright to unprotectible useful articles".[723]

Lasercomb and its progeny suggest the need for great care in drafting contracts with restrictive covenants or noncompetition clauses, to separate those provisions from the license of the copyrighted work, and to link them instead to a license for trade secrets or some other permissible consideration.

B. *Preemption of Trade Secret Claims*

Even more troubling is that the district court in *Lasercomb* had held the plaintiff's trade secret claim to be preempted by copyright law (that holding was not appealed). Thus, if the *Lasercomb* district and appellate decisions are both good law, a copyright owner would be unable to use a restrictive covenant to protect its trade secrets, if subject matter of the trade secrets is also copyrighted. A similar preemption holding in *Computer Associates v. Altai* [724] was originally affirmed, but then reversed by the Second Circuit on rehearing, holding that the state

---

Organizations Antitrust Litigation, 964 F. Supp. 1469 (D. Kan. 1997); *Tamburg v. Calvin*, 1995 WL 121539 (N.D. Ill. 1995) (unpublished opinion).

720 *E.g., Bellsouth Advertising & Publishing Corp. v. Donnelly Information Publishing, Inc.*, 933 F.2d 952 (11th Cir. 1991).

721 No. C 08-03251 WHA, 2009 WL 303046 (N.D. Cal. 2009).

722 *Id.* at *2 (citing *Lasercomb*, 911 F.2d at 979). Ultimately, Psystar's copyright misuse counterclaim was dismissed where the court found that "Apple's [copyright and DMCA] claims are valid …." *Apple, Inc. v. Psystar Corp.*, No. C 08-03251 WHA, 2009 WL 3809798, *7 (N.D. Cal. 2009).

723 *Omega S.A., v. Costco Wholesale Corp.*, 2011 WL 8492716 (C.D. Cal. 2011).

724 775 F. Supp. 544 (E.D.N.Y. 1991), *aff'd in part, vacated in part*, 982 F.2d 693 (2d Cir. 1992).

trade secret claim is not preempted if the state law claim has additional elements that change the nature of the claim, such as the breach of a confidential relationship or fiduciary duty. This seems a better reasoned approach that should carry the day.[725]

[725] *See Data General Corp. v. Grumman Systems Support Corp.*, 36 F.3d 1147, 1164-65 (1st Cir. 1994); *Gates Rubber v. Bando American*, 9 F.3d 823, 847-48 (10th Cir. 1993); *Trades Corp. v. Guy F. Atkinson Co.*, 996 F.2d 655 (1993); *CMAX/Cleveland v. UCR*, 804 F. Supp. 337 (M.D. Ga. 1992). *See also Long v. Quality Computers and Applications, Inc.*, 860 F. Supp. 191, 196-97 (M.D. Pa. 1994) (trade secret claim against competitor was essentially the same as copyright claim and so preempted; trade secret claim against president of licensee for wrongful disclosure to competitor in violation of license has additional element and so is not preempted). *See also Alcatel USA, Inc. v. DGI Technologies, Inc.*, 166 F.3d 772, 784-88 (5th Cir. 1999) (affirming trade secret misappropriation verdict without discussing preemption, but overturning verdict of unfair competition by misappropriation as preempted by copyright law).