

**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**

	<b><u>Page</u></b>
<b>I. <i>Liability On-Line: Copyright and Tort Risks of Providing Content, or Who's In Charge Here?</i>.....</b>	<b>1</b>
A. <i>The Applicability of Multiple Laws</i> .....	1
B. <i>Jurisdictional Questions</i> .....	2
C. <i>Determining Applicable Law</i> .....	12
D. <i>Copyright Infringement</i> .....	17
E. <i>Defamation</i> .....	22
F. <i>Trademark Infringement</i> .....	24
G. <i>Regulation of Spam</i> .....	29
H. <i>Spyware</i> .....	33
I. <i>Trespass</i> .....	34
J. <i>Privacy</i> .....	35
<b>II. <i>Patent Protection of Software and Business Methods</i>.....</b>	<b>60</b>
<b>III. <i>Mass Market Software Issues</i> .....</b>	<b>62</b>
A. <i>Loss of Trade Secrets by Mass Distribution</i> .....	62
B. <i>Enforceability of Shrinkwrap and Clickwrap Licenses</i> .....	62
C. <i>Use of Licenses Instead of Sales</i> .....	66
<b>IV. <i>Copyright Misuse and Trade Secret Preemption</i> .....</b>	<b>66</b>
A. <i>Copyright Misuse</i> .....	66
B. <i>Preemption of Trade Secret Claims</i> .....	67
<b>V. <i>Computer Software Copyright Issues</i> .....</b>	<b>67</b>
A. <i>Literal elements: Code</i> .....	68
B. <i>Non-literal elements "User Interface" and "Look and Feel"</i> .....	68
<b>VI. <i>Reverse Engineering and Compatibility</i> .....</b>	<b>76</b>

A.	<i>SEGA v. Accolade</i> .....	77
B.	<i>Atari Games Corp. v. Nintendo of America, Inc.</i> .....	77
C.	<i>In Sony Computer Entertainment, Inc. v. Connectix Corp.</i> , .....	78
D.	<i>In Brooktree Corp. v. Advanced Micro Devices</i> , .....	78
E.	<i>DSC Communications Corp. v. DGI Technologies, Inc.</i> , .....	78
F.	<i>Lotus Development Corp. v. Borland Int'l, Inc.</i> .....	78

**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.<sup>1</sup>
- ◆ 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.<sup>2</sup>
- ◆ 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 Helpert Syracuse & Hirschtritt LLP.  
© Andre R. Jaglom 1993, 1994, 1995, 1996, 1997, 1998, 2000, 2002, 2003, 2005, 2006, 2007.  
All Rights Reserved

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

<sup>2</sup> L. Rose & J.P. Feldman, *Practical Suggestions for International Advertising and Promotions on the 'Net'*, CYBERSPACE LAW, 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?<sup>3</sup>
- ◆ 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.<sup>4</sup> 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.<sup>5</sup> 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 specific jurisdiction with respect to matters arising out of the website itself) or continuously and

---

<sup>3</sup> 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).

<sup>4</sup> *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.

<sup>5</sup> A. Harmon, “Music Industry in Global Fight on Web Copies,” N.Y. TIMES (Oct. 7, 2002).

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*,<sup>6</sup> *Mink v AAAA Development LLC*,<sup>7</sup> *Cybersell Inc. v. Cybersell Inc.*<sup>8</sup> and *Bensusan Restaurant Corp. v. King and the Blue Note*,<sup>9</sup> among others.<sup>10</sup> 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.*<sup>11</sup> 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.*<sup>12</sup> held that establishing a website accessible to all states constitutes purposeful establishment of minimum contacts with all states.<sup>13</sup> *National Football League v. Miller*,<sup>14</sup> 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.

---

<sup>6</sup> 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”).

<sup>7</sup> 190 F.3d 333 (5th Cir. 1999).

<sup>8</sup> 130 F.3d 414 (9th Cir. 1997).

<sup>9</sup> 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.

<sup>10</sup> 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*, 28 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).

<sup>11</sup> 937 F. Supp. 161 (D. Conn. 1996).

<sup>12</sup> 53 F. Supp. 2d 1000 (N.D. Ill. 1999).

<sup>13</sup> 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).

<sup>14</sup> 54 U.S.P.Q. 2d 1574 (S.D.N.Y. 2000).

Similarly, consider *United States v. Thomas*,<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup>

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.<sup>18</sup>

---

<sup>15</sup> 74 F.3d 701 (6th Cir. 1996).

<sup>16</sup> 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.

<sup>17</sup> *Id.* at 709-11.

<sup>18</sup> 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

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*<sup>19</sup> that it was subject to its jurisdiction in a trademark infringement suit, since the infringement arose from the registration business.<sup>20</sup> 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.*<sup>21</sup> The Court distinguished *GTE New Media Services Inc. v. BellSouth Corp.*,<sup>22</sup> 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.B. 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.<sup>23</sup>

A growing number of cases have followed *Zippo Manufacturing Co. v. Zippo Dot Com Inc.*,<sup>24</sup> 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.<sup>25</sup>

---

Missouri); *Heroes Inc. 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).

<sup>19</sup> 289 F.3d 865 (6<sup>th</sup> Cir. 2002).

<sup>20</sup> See also *Neogen Corp. v. Neo Gen Screening, Inc.*, 282 F. 3d 883 (6<sup>th</sup> 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*).

<sup>21</sup> 293 F.3d 506 (D.C. Cir. 2002).

<sup>22</sup> 199 F.3d 1342 (D.C. Cir. 2000).

<sup>23</sup> *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.).

<sup>24</sup> 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 (4<sup>th</sup> 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).

<sup>25</sup> *Chicago Archeitectural Foundation v. Domain Magic, LLC*, 2007 WL 3046124 (N.D.Ill. 2007).

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.*,<sup>26</sup> 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.<sup>27</sup> Alternatively, the jurisdictional question in *Systems Designs Inc. v. New CustomWare Co.*<sup>28</sup> 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.<sup>29</sup>

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<sup>30</sup>.

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 sites with Nazi and neo-Nazi material, which are illegal in Germany.<sup>31</sup> After conviction, he was

---

<sup>26</sup> 139 F. Supp. 2d 696 (D. Md. 2001).

<sup>27</sup> See, e.g., *ISI Brands Inc. v. KCC Int’l Inc.*, 458 F. Supp. 2d 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 (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).

<sup>28</sup> 248 F. Supp. 2d 1093 (D. Utah 2003).

<sup>29</sup> *McBee v. Delica Co.*, 417 F.3d 107 (1<sup>st</sup> Cir. 2005), reported in 70 PAT.,TM & Copyr.J. (BNA) 439 (Aug. 12, 2005) available at <http://pub.bna.com/ptcj/042733Aug2.pdf>.

<sup>30</sup> 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).

<sup>31</sup> *Germany Charges Compuserve Manager*, N.Y. TIMES, Apr. 10, 1997, at D19.

given a two year suspended prison sentence and fined.<sup>32</sup> The guilty verdict was finally overturned in November 1999, based on a new multimedia law enacted after the conviction.<sup>33</sup> 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.<sup>34</sup> 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.<sup>35</sup> And, more recently, the French Supreme Court held that a website that did not target the French public did not infringe French trademarks.<sup>36</sup>

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<sup>37</sup> prohibiting the display or sale of racist material.<sup>38</sup> The presiding judge ordered Yahoo! to block French users from viewing Nazi memorabilia;<sup>39</sup> 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.<sup>40</sup> The Yahoo! ruling was upheld on appeal<sup>41</sup> 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.<sup>42</sup> 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.<sup>43</sup>)

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

---

<sup>32</sup> *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).

<sup>33</sup> *German Court Overturns Pornography Ruling Against Compuserve*, N.Y. TIMES, Nov. 18, 1999, at C4.

<sup>34</sup> *Saint-Tropez Commune v. SA Eurovirtuel*, reported in 53 INTA Bulletin No. 3, Feb. 1, 1998, at 2.

<sup>35</sup> *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.

<sup>36</sup> *Hugo Boss v. Reemtsma Cigarettenfabrik* (French Sup. Ct. Jan. 11, 2005), reported in WORLD INTERNET L REP. (BNA) (Sept. 2005) at p. 9.

<sup>37</sup> Section R645-1 of the French Criminal Code.

<sup>38</sup> *Association Union des Etudiants Juifs de France et al. v. Yahoo! Inc.*, reported in WORLD INTERNET L REP. (BNA) (7/00).

<sup>39</sup> *Judge leaves screening of racist material to French ISPs*, Oct. 31, 2001, available at [www.ananova.com/news/story/sm\\_437656.html](http://www.ananova.com/news/story/sm_437656.html).

<sup>40</sup> *ISPs Not Obligated to Block Access to Hate Portal: Action Internationale pour la Justice, La Licra et al. v. Association Franchise 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.

<sup>41</sup> John Tagliabue, "French Uphold Ruling Against Yahoo on Nazi Sites," N.Y. TIMES, Nov. 21, 2000, at C8.

<sup>42</sup> T. Richardson, "Europe Elbows Internet Content Blocking"; THE REGISTER (11/4/2002); <http://www.theregister.co.uk/content/6/24808.html>.

<sup>43</sup> J. Evers, "German Railway Operator to Sue Google over Sabotage Links," COMPUTERWORLD (4/16/2002).

rehearing *en banc*.<sup>44</sup> (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.<sup>45</sup>) Some commentators believe the French court's attempt to restrict Nazi memorabilia on Yahoo! may be a harbinger of the Internet of the future 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.<sup>46</sup> 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.<sup>47</sup> (The statute was held unconstitutional in September 2004).<sup>48</sup> 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.<sup>49</sup> 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.<sup>50</sup> 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.<sup>51</sup>

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

---

<sup>44</sup> *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).

<sup>45</sup> *Louis Féraud Int'l S.a.r.l. v. Viewfinder, Inc. d/b/a Firstview.com*, 2005 WL 2420525L (S.D.N.Y. 2005).

<sup>46</sup> Lisa Guernsey, "Welcome to the Web. Passport, Please?," N.Y. TIMES, Mar. 15, 2001, at G1.

<sup>47</sup> PA crimes code, 18 Pa.Cons.Stat. § 7330, Internet Child Pornography. *See Application of Fisher*, No. Misc. 689 Jul 02 (Ct. Common Pleas, Montgomery Co. Sept. 17, 2002) (order requiring Internet service provider to remove or disable access to child pornography) available at: <http://www.stepto.com/publications/219e.pdf>.

<sup>48</sup> *Center for Democracy and Technology v. Pappert*, 337 F.Supp.2d 606 (E.D.Pa. 2004).

<sup>49</sup> *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](http://www.usatoday.com/tech/news/techpolicy/2004-01-07-censor-law-appeal_x.htm).

<sup>50</sup> *See* Internet Law News (BNA) (Sept. 30, 2002).

<sup>51</sup> *See* D. McCullagh, "Google Excluding Controversial Sites," c|net news.com (Oct. 23, 2002) at <http://news.com.com/2100-1023-963132.html>.

case by citing the fact that Italian Internet users needed Italy-based service to view offending pages.<sup>52</sup>

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.<sup>53</sup> 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.<sup>54</sup> 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.<sup>55</sup>

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.<sup>56</sup> 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."

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

---

<sup>52</sup> *Controlling Access to Foreign websites: In re Dulberg*, WORLD INTERNET L. REP. (BNA), Feb. 2001, at 14.

<sup>53</sup> *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).

<sup>54</sup> *King v. Lewis* [2004] EWHC 168 (QB) (06 February 2004), available at <http://bailii.org/ew/cases/ewke/qb/2004/168.html>.

<sup>55</sup> *Bonnier Media Ltd. v. Smith*, available at [www.scotcourts.gov.uk/opinions/DRU2606.html](http://www.scotcourts.gov.uk/opinions/DRU2606.html). See also "Frenchman Sentenced in Senegal for Internet Libel," YAHOO NEWS (Jan. 7, 2004), <http://uk.news.yahoo.com/040107/323/eijv5.html>.

<sup>56</sup> *Bangoura v. Washington Post* (Ontario Sup. Ct. Justice January 27, 2004), available at [www.canlii.org/on/cas/onsc/2004/2004onsc10181.html](http://www.canlii.org/on/cas/onsc/2004/2004onsc10181.html), reported in WORLD INTERNET L. REP. (BNA) (Feb. 2004) at 14, *rev'd* (Ontario Court of Appeal Sept. 16, 2005) reported in Toronto Star (Sept. 16, 2005), [http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article\\_Type1&call\\_pageid=971358637177&c=Article&cid=1126907414358&DPL=IvsNDS%2f7ChAX&tacodologin=yes](http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&call_pageid=971358637177&c=Article&cid=1126907414358&DPL=IvsNDS%2f7ChAX&tacodologin=yes).

was aimed at a Connecticut audience and not at Virginia, and so there was no jurisdiction over the newspapers in Virginia.<sup>57</sup> 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.<sup>58</sup> 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.”<sup>59</sup>

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.<sup>60</sup> 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.<sup>61</sup>

#### *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.”<sup>62</sup> 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 maintenance of a toll-free telephone number and a mailing list that included Minnesota residents.<sup>63</sup>

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

---

<sup>57</sup> *Young v. New Haven Advocate*, 315 F.3d 256 (4th Cir. 2002), *cert. denied* 123 S. Ct. 2092 (May 19, 2003).

<sup>58</sup> *Revell v. Lidov*, 371 F.3d 467 (5th Cir. 2002).

<sup>59</sup> *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.stepto.com/assets/attachments/3276.pdf>

<sup>60</sup> *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>.

<sup>61</sup> *McVea v. Crisp*, 2007 WL 4205648 (W.D. Tex. 2007), *available at* <http://www.stepto.com/assets/attachments/3275.pdf>.

<sup>62</sup> J. Sterngold, *A One-Armed Bandit Makes a House Call*, N.Y. TIMES, Oct. 28, 1996, at D1, col. 2.

<sup>63</sup> *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).

jurisdiction and choice of law.<sup>64</sup> 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.<sup>65</sup> 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.<sup>66</sup>

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.<sup>67</sup> 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.<sup>68</sup>

In Germany, however, the availability of a German language version of the [www.goldenjackpot.com](http://www.goldenjackpot.com) website was deemed sufficient to establish “that the Internet casino in issue has directly targeted the German market.”<sup>69</sup>

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.<sup>70</sup> An appeals panel largely reversed, applying an exception where nations show that 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.<sup>71</sup> A WTO Compliance panel ruled in February 2007 that the U.S. had failed to comply with the prior

---

<sup>64</sup> *14 Charged by U.S. In First Such Case On Internet Betting*, N.Y. TIMES, Mar. 5, 1998, at A1, col. 8.

<sup>65</sup> *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).

<sup>66</sup> *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)).

<sup>67</sup> *Ladbrokes v. De Lotto*, WORLD INTERNET L. REP. (BNA) Oct. 2003, at 21.

<sup>68</sup> C. Rohsler, *Internet Gambling – Worldwide Themes and Dissonances*, WORLD INTERNET L. REP. (BNA) at 6 (Aug. 2003).

<sup>69</sup> *Id.* (reporting Ct. App. Hamburg, Judgment of Nov. 4, 1999).

<sup>70</sup> 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>.

<sup>71</sup> F.Butterfield, “U.S. Limits on Internet Gambling Are Backed,” N.Y. Times (April 8, 2005), p. C14 col.1.

ruling, opening the door to trade sanctions,<sup>72</sup> and in December Antigua was permitted to violate copyrights on U.S. content up to a value of \$21 million.<sup>73</sup>

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 participants to enforce each others' commercial laws even if such laws prohibit actions that are legal under local laws.<sup>74</sup>

There are many critics in the United States who fear that U.S. citizens will lose many of their rights if all websites are forced 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.<sup>75</sup> 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.

### C. *Determining Applicable Law*

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 law of the jurisdiction where the server is located.<sup>76</sup> 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.

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

---

<sup>72</sup> "WTO Panel Upholds Ruling on U.S. Internet Gambling Laws," WORLD COMMUNICATIONS REG. REP. (BNA) at 15 (April 2007).

<sup>73</sup> "In Trade Ruling, Antigua Wins a Right to Piracy," N.Y. TIMES (Dec. 22, 2007), [www.nytimes.com/2007/12/22/business/22gambling.html](http://www.nytimes.com/2007/12/22/business/22gambling.html).

<sup>74</sup> Lisa M. Bowman, *Global treaty could transform Web*, CNET NEWS.COM (June 22, 2001) located at <http://news.cnet.com/news/0-1005-200-6345725.html>.

<sup>75</sup> 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>.

<sup>76</sup> 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.

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.<sup>77</sup>

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.<sup>78</sup>

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 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.<sup>79</sup>

The Electronic Commerce Directive, a regulatory framework for e-commerce, was put forth by the European Union in 2000.<sup>80</sup> The E-Commerce Directive employs a "country of 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.<sup>81</sup>

The country of origin principle, however, does not apply to consumer transaction contracts.<sup>82</sup> Consumers remain protected by the laws of their own nation,<sup>83</sup> such as Germany's requirement that consumers be notified of their right to revoke online transactions.<sup>84</sup> 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

---

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

<sup>78</sup> 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).

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

<sup>80</sup> 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://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l\\_178/l\\_17820000717en00010016.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.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://europa.eu.int/eur-lex/pri/en/dpi/rpt/doc/2003/com2003\\_0702en01.doc](http://europa.eu.int/eur-lex/pri/en/dpi/rpt/doc/2003/com2003_0702en01.doc).

<sup>81</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 (the "E-Commerce Directive"), available at [http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l\\_178/l\\_17820000717en00010016.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf), Recital (22), Annex.

<sup>82</sup> *Id.*, Recitals (29), (53), (55), (56), (65), Art. 1, §3, Annex.

<sup>83</sup> *Id.*, Recital (55).

<sup>84</sup> See M.Hilber, "Round-Up of Recent E-Commerce Decisions in Germany," WORLD COMM. REG. REP. (BNA) (Sept. 2006).

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.”<sup>85</sup> 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.<sup>86</sup>

The European Union has been active in attempting to resolve cross-border electronic commerce issues. The E.U. Commission has issued a draft regulation, to govern jurisdictional issues surrounding cross-border consumer e-transactions.<sup>87</sup> This proposed regulation, termed Rome II, will 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 Rome II 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.<sup>88</sup>

Moreover, a company that sells over the Internet increasingly must consider not only the jurisdictional issues discussed above, but also 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 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.<sup>89</sup>

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.<sup>90</sup>

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

---

<sup>85</sup> Council Regulation No. 44/2001 on Jurisdiction and the Recognition and Enforcement of Judgements in Civil and Commercial Matters, art. 15(c).

<sup>86</sup> 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).

<sup>87</sup> See [http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003\\_0427en01.pdf](http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0427en01.pdf); see also [http://europa.eu.int/comm/justice\\_home/fsj/civil/applicable\\_law/wai/fsj\\_civil\\_applicable\\_law\\_en.htm](http://europa.eu.int/comm/justice_home/fsj/civil/applicable_law/wai/fsj_civil_applicable_law_en.htm).

<sup>88</sup> *Proposed European e-commerce law would stifle business*, July 25, 2001, located at [http://www.iccwbo.org/home/news\\_archives/2001/e\\_commerce\\_law.asp](http://www.iccwbo.org/home/news_archives/2001/e_commerce_law.asp).

<sup>89</sup> D. Marino and D. Fontana, *The EU Draft Directive on Electronic Commerce*, WORLD INTERNET L. REP. (BNA) (3/00), at 26.

<sup>90</sup> Laurent Szuskin and Myria Saarinen, *Enactment of the Decree Relating to E-Signatures*, WORLD INTERNET L. REP. (BNA) (June 2001), at 7.

of the hardware and software required to access the electronic records.<sup>91</sup> In addition, 38 states have adopted, and four more have pending legislation to adopt, the Uniform Electronic Transactions Act (“UETA”)<sup>92</sup>, 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.<sup>93</sup> 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.<sup>94</sup>

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.<sup>95</sup> 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.<sup>96</sup>

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 the developing trend in the United States that a state’s jurisdiction over a particular website is conferred through actual transactions in the state.<sup>97</sup>

---

<sup>91</sup> Stephanie Tsacoumis and Victoria P. Rostow, *E-SIGN Your Life Away: Digital Signatures in the New Economy*, 4 WALLSTREETLAWYER.COM, at 20.

<sup>92</sup> UETA was approved by the National Conference of Commissioners on Uniform State Laws at its annual meeting in July 1999.

<sup>93</sup> For current statistics on the adoption of the UETA, see <http://www.nccusl.org/nccusl/pubndrafts.asp>.

<sup>94</sup> *Most UETA Bills Introduced in 2001 Pass*, WORLD INTERNET L. REP. (BNA) (Sept. 2001), at 17.

<sup>95</sup> 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.

<sup>96</sup> <http://www.un.org/apps/news/story.asp?NewsID=16685&Cr=general&Cr1=assembly>.

<sup>97</sup> 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); contra, *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).

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.<sup>98</sup> Similar issues arise as the SEC considers how to regulate offerings of securities by foreign websites.<sup>99</sup> 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.<sup>100</sup> Australia and Japan have similar rules and have published guidelines offerors can follow, including a jurisdictional disclaimer, to avoid violating their securities laws.<sup>101</sup>

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 to be a “general solicitation” in violation of Rule 507.<sup>102</sup>

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.<sup>103</sup> This approach has since been adopted in seven states, including Indiana,<sup>104</sup> Maryland<sup>105</sup> and New York.<sup>106</sup> 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

---

<sup>98</sup> 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.

<sup>99</sup> 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>.

<sup>100</sup> 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.

<sup>101</sup> *Id.* See also, *FSA Introduces Guidelines on Foreign Firms’ Internet Ads*, World Internet L. REP. (BNA) (Feb. 2001), at 6.

<sup>102</sup> 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); 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).

<sup>103</sup> NASAA Statement of Policy Regarding Offers of Franchises on the Internet, *available at* [http://www.nasaa.org/nasaa/scripts/fu\\_display\\_list.asp?pfid=72](http://www.nasaa.org/nasaa/scripts/fu_display_list.asp?pfid=72).

<sup>104</sup> Order No. 97-0378AO, BUS. FRANCHISE GUIDE (CCH) ¶ 5140.011 (Dec. 24, 1997).

<sup>105</sup> Code of Md. Regs., Div. of Securities § 02.02.08.18.

<sup>106</sup> 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.

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<sup>107</sup> 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.<sup>108</sup> New York has implemented the NASAA policy statement.<sup>109</sup>

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.<sup>110</sup>

#### 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.*,<sup>111</sup> 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

---

<sup>107</sup> 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 L.J.N.’S FRANCHISING BUS. NEWS & L. ALERT 11 (Aug. 2001), at 6.

<sup>108</sup> See NASAA Statement of Policy Regarding Franchise Advertising on the Internet, *available at* [http://www.nasaa.org/nasaa/scripts/fu\\_display\\_list.asp?pfid=72](http://www.nasaa.org/nasaa/scripts/fu_display_list.asp?pfid=72). 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.

<sup>109</sup> 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.

<sup>110</sup> Statutory Instrument 2000 No. 2334, *available at* [www.legislation.hmso.gov.uk/si/si2000/20002334.htm](http://www.legislation.hmso.gov.uk/si/si2000/20002334.htm); “New Rules Governing Sales to Consumers over the Internet” *located at* [www.elexica.com/items/data/d9c607dc9.htm](http://www.elexica.com/items/data/d9c607dc9.htm). New York implemented the NASAA policy statement.

<sup>111</sup> 907 F. Supp. 1361 (N.D. Cal. 1995).

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.<sup>112</sup> 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 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.<sup>113</sup> 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.<sup>114</sup>

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.<sup>115</sup>

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?<sup>116</sup> Admittedly, the provision of a link is less active than the storage and transmission of infringing material and

---

<sup>112</sup> *Id.* at 1369-72.

<sup>113</sup> 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](http://www.thestandard.com/article/display/0,1151,22941,00.html).

<sup>114</sup> *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 Enters., 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).

<sup>115</sup> *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/E-CommerceLawWeek>.

<sup>116</sup> 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.

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 least in the absence of knowledge by the defendant of the infringing photographs.<sup>117</sup> 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](http://chillingeffects.org), and informs users when a search would yield a removed link, pointing them instead to [chillingeffects.org](http://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.<sup>118</sup>

#### *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.<sup>119</sup>

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.<sup>120</sup> More recently, the Central District of California held that Google did not infringe an adult website's copyright when it provided frames and in-line links to full-size images on the adult website, 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 Google.<sup>121</sup> 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, the website was unlikely to overcome Google's fair use defense, because of the transformative nature of Google's use.<sup>122</sup>

---

<sup>117</sup> *Bernstein v. JC Penney Inc.*, 50 U.S.P.Q.2d (BNA) 1063 (C.D. Cal. 1998).

<sup>118</sup> See D. Gallagher, "New Economy," N.Y. Times, Apr. 22, 2002.

<sup>119</sup> *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).

<sup>120</sup> *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003), withdrawing prior opinion reported at 280 F. 3d 934 (9th Cir. 2002).

<sup>121</sup> *Perfect 10 Inc. v. Google Inc.*, 416 F.Supp.2d 828 (C.D.Cal. 2006).

<sup>122</sup> *Perfect 10 Inc. v Amazon.com Inc.*, 2007 WL 4225819 (9<sup>th</sup> 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.

German Courts have 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<sup>123</sup>

Pop-up advertisements that appear in a different window over a competitor's website generally have been held noninfringing.<sup>124</sup>

"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.<sup>125</sup>

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.<sup>126</sup> 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.<sup>127</sup> In Germany, the Federal Supreme Court found deep links to press articles violated no rights and did not constitute unfair competition.<sup>128</sup>

---

<sup>123</sup> Compare Decision of Regional Court of Hamburg, reported in WORLD INTERNET L. REP. (July 1004), with Decision of District Court of Erfurt (Case No. A2:3 O 1180/05), reported in WORLD COMM. REG. REP. (April 2007) at 20. The Erfurt decision is available in German at [www.suchmaschinen-und-recht.de/urteile/Landgericht-Erfurt-20070315.html](http://www.suchmaschinen-und-recht.de/urteile/Landgericht-Erfurt-20070315.html). The 2003 Hamburg decision is available in German at [www.suchmaschinen-und-recht.de/urteile/Landgericht-Hamburg-20030905.html](http://www.suchmaschinen-und-recht.de/urteile/Landgericht-Hamburg-20030905.html). 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).

<sup>124</sup> *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).

<sup>125</sup> *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).

<sup>126</sup> *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](http://www.wired.com/news/politics/0,1283,54083,00.html); [www.wired.com/news/print/0,1294,54083,00.html](http://www.wired.com/news/print/0,1294,54083,00.html) (reporting on a similar decision by Munich's Upper Court in Germany).

<sup>127</sup> 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).

<sup>128</sup> *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](http://www.theregister.co.uk/content/6/31838.html).

The Digital Millennium Copyright Act,<sup>129</sup> 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.<sup>130</sup> 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.<sup>131</sup>

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 counter notices 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.<sup>132</sup> The principal responsibility for policing infringement, however, rests with the copyright owner. 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.<sup>133</sup>

In 2001, eBay Inc. won a precedent setting decision in federal court under the Digital Millennium Copyright Act. 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 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 Digital Millennium Copyright Act.<sup>134</sup>

---

<sup>129</sup> H.R. 2281; Pub. L. No. 105-304), 17 U.S.C. § 512.

<sup>130</sup> H.R. 2281, Pub. L. No. 105-304 § 202(j).

<sup>131</sup> *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 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).

<sup>132</sup> *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004).

<sup>133</sup> *Perfect 10 Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), cert. denied 128 S. Ct. 709 (2007)

<sup>134</sup> *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*

### E. Defamation

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.*,<sup>135</sup> 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."<sup>136</sup>

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.<sup>137</sup> 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.<sup>138</sup>

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.<sup>139</sup> 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.*,<sup>140</sup> recently strengthened the protection for ISP's under Section 203 of the Communications Decency Act. Defendant

---

*Liability as it Begins Policing Content*, THE RECORDER (Mar. 13, 2001). Perhaps eBay's victory in September will encourage other websites to start policing themselves as well.

<sup>135</sup> 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710, 23 Media L. Rep. 1794 (Sup. Ct. Nassau Co. 1995).

<sup>136</sup> 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).

<sup>137</sup> *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).

<sup>138</sup> *Id.*

<sup>139</sup> *Barrett v. Clark*, 2001 WL 881259 (Cal. Sup. July 25, 2001) (unpublished opinion).

<sup>140</sup> 339 F.3d 1119 (9th Cir. Aug. 13, 2003).

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 203 of the Communication Decency Act because it did not "play a significant role in creating, developing or transforming the relevant information."<sup>141</sup>

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."<sup>142</sup> 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.<sup>143</sup>

American and European courts seem to be of the same mind on this issue. Specifically, both French and British courts have ruled recently that ISPs are not liable for postings on their websites, provided that, once they are notified of offending statements, they take all reasonable steps to remove the statement.<sup>144</sup> The Electronic Commerce Directive<sup>145</sup> limits the liability of ISPs for unlawful material on their websites,<sup>146</sup> 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.<sup>147</sup>

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

---

<sup>141</sup> *Id.*, at 1125.

<sup>142</sup> *Grace v. Ebay Inc.*, 120 Cal. App. 4th 984 (Cal. App. 2d 2004).

<sup>143</sup> *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).

<sup>144</sup> *See Multiman 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.

<sup>145</sup> 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://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l\\_178/l\\_17820000717en00010016.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf), Recital (22), Annex.

<sup>146</sup> "European Parliament Swiftly Passes Electronic Commerce Directive" E-COMMERCE L. WKLY. (NLP IP Co.) (5/1/00) at 544.

<sup>147</sup> 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.

find jurisdiction and apply the law of jurisdictions where the alleged defamation is accessible than are U.S. courts.<sup>148</sup>

#### 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,<sup>149</sup> or in a “metatag” that is invisible to human viewers but detected by search engines,<sup>150</sup> it generally will be enjoined.

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.<sup>151</sup> 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.*,<sup>152</sup> 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. That appears to be the general view outside the Second Circuit, as numerous courts have now followed this approach.<sup>153</sup> (Courts have differed, however, with respect to when the use of competitive trademarks might constitute nominative fair use.<sup>154</sup>)

---

<sup>148</sup> See discussion in Section I.B., *supra*.

<sup>149</sup> 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).

<sup>150</sup> 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).

<sup>151</sup> *Playboy Enterprises, Inc. v. Netscape Comm’ns Corp.* 345 F.3d 1020 (9th Cir. 2004).

<sup>152</sup> 278 F. Supp. 2d 1193 (W.D. Wash. 2003). See also *SNA, Inc. v. Array*, 51 F. Supp. 2d 554 (E.D. Pa. 1999).

<sup>153</sup> E.g., *Australian Gold, Inc. v. Hatfield*, 436 F. 3d 1228 (10<sup>th</sup> Cir. 2006); *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).

<sup>154</sup> *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)

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. When the keyword is a competitor’s trademark, infringement claims have ensued. In the U.S., Google has prevailed in some such cases and lost in others. The courts have divided over whether such use of the competitor’s trademark is a “use in commerce” and so actionable under the Lanham Act, where the consumer never sees the trademark in an ad or on any goods or displays. Courts in the Second Circuit have rejected such claims, holding that there was no use in commerce, following the Second Circuit’s *I-800-Contacts* decision in the pop-up ad context.<sup>155</sup> In contrast, other courts have found such keyword advertising to constitute a use in commerce, and 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 to proceed with respect to sponsors’ links that contained the word “Geico” in the text of the advertisement itself.<sup>156</sup> Other cases have taken a similar approach.<sup>157</sup>

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.<sup>158</sup> This French case poses serious problems for keyword advertising, as the trademark in question, “bourse de 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

---

(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).

<sup>155</sup> E.g., *Rescuecom Corp. v. Google Inc.*, 456 F.Supp.2d 393 (N.D.N.Y. 2006), available at <http://pub.bna.com/ptcj/5041055Sept28.pdf>; *Merck & Co. v. Mediplan Health Consulting Inc.*, No. 05civ.3650, 425 F. Supp. 2d 402, reaffirmed on reconsideration, 431 F. Supp. 2d 425 (S.D.N.Y. 2006).

<sup>156</sup> *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>.

<sup>157</sup> E.g., *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); *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); *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).

<sup>158</sup> *Société Luteciel v. Google France*, No. 03/00051 (Trib. de Gr. Inst. Nanterre Oct. 13, 2003), reported in 66 PATENT, TRADEMARK & COPYRIGHT J. 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](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).

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.

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.<sup>159</sup> Canadian courts have reached similar conclusions, finding the use of metatags identical to domain names or trademarks of others to constitute actionable “passing off.”<sup>160</sup>

A German court enjoined a similar arrangement where trademarks of Estée Lauder, such as “Clinique,” when used as search terms in the Excite Search engine, would cause an ad for Fragrance Counter, an Internet seller of perfumes and cosmetics, to appear,<sup>161</sup> and a French court enjoined the use of metatags embodying a French company’s registered corporate name on the website of a direct competitor.<sup>162</sup> The British High Court of Justice reached a similar conclusion.<sup>163</sup>

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.<sup>164</sup> 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,<sup>165</sup> but such conduct was held not to constitute infringement by the Second Circuit in *1-800-Contacts Inc. v. WhenU.com Inc.*, following two similar district court decisions,<sup>166</sup> 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.

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.<sup>167</sup> The policy provides for arbitration of disputes before WIPO or additional

---

<sup>159</sup> *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).

<sup>160</sup> *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’n v. O.P.E.I.U. Local 378*, 10 C.P.R. 4th 423 (B.C. Sup. Ct. 2001), reported in Bushtein, *supra*.

<sup>161</sup> *In re Estée Lauder Cosmetics Ltd.* (Dist. Ct. Hamburg February 16, 2000).

<sup>162</sup> *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>.

<sup>163</sup> *Reed Executive PLC v. Reed Business Information Ltd.*, High Ct. Justice (May 20, 2002), reported in WORLD INTERNET L. REP (BNA) 22 (July 2002).

<sup>164</sup> B. Tedeschi, “Publishers of Websites File Suit to Stop Pop-Up Ads,” N.Y. TIMES (June 28, 2002).

<sup>165</sup> *Staples, Inc. v. Office Depot, Inc.*, 01 Civ. 9128 (DAB) (S.D.N.Y.) (complaint).

<sup>166</sup> 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).

<sup>167</sup> The policy is available at <http://www.icann.org/udrp/udrp.htm>.

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.<sup>168</sup>

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 fair use of the domain name all serve to demonstrate a legitimate interest in the domain name. 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.<sup>169</sup>

Congress addressed the same problem of bad faith domain name registrations with the enactment of the Anticybersquatting Consumer Protection Act (the "ACPA").<sup>170</sup> This statute amends Section 43 of the Lanham Act,<sup>171</sup> 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<sup>172</sup> 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."<sup>173</sup> Under the new law, a court may order the

---

<sup>168</sup> *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).

<sup>169</sup> *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 "philipsucks.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).

<sup>170</sup> Enacted Title III of the Intellectual Property and Communications Omnibus Reform Act of 1999, Pub. L. No. 106-113 (1999).

<sup>171</sup> 15 U.S.C. 1125.

<sup>172</sup> 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).

<sup>173</sup> 15 U.S.C. § 1125(d)(1)(A).

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.<sup>174</sup> 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.<sup>175</sup>

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 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.<sup>176</sup> 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.<sup>177</sup> 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.<sup>178</sup> One district court has found the failure to perform a trademark search before registering a domain name suggests bad faith.<sup>179</sup>

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.<sup>180</sup> The court ordered the transfer of the domain name to the plaintiff.<sup>181</sup> And 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.<sup>182</sup>

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

---

<sup>174</sup> 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).

<sup>175</sup> 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>.

<sup>176</sup> *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).

<sup>177</sup> 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).

<sup>178</sup> 15 U.S.C. § 1125(d)(1)(B)(ii).

<sup>179</sup> *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).

<sup>180</sup> *Broadbridge Media LLC v. Hypercd.com*, 106 F.Supp.2d 505 (S.D.N.Y. 2000).

<sup>181</sup> *Id.*

<sup>182</sup> *Harrods Ltd. v. Sixty Internet Domain Names*, 302 F.3d 214 (4<sup>th</sup> Cir. 2002).

California recently issued a compromise of sorts with regard to confusingly similar names, requiring the owner of [www.nissan.com](http://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.<sup>183</sup>

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.<sup>184</sup>

### 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.<sup>185</sup> This Act requires unsolicited commercial e-mail messages to be labeled (though not by a standard method)<sup>186</sup> and to include opt-out instructions, as well as the sender's physical address. 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.<sup>187</sup>

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

---

<sup>183</sup> *Nissan Motor Co., Ltd. et al. v. Nissan Computer Corp.*, 89 F. Supp. 2d 1154 (C.D. Ca. 2000).

<sup>184</sup> *Verein der Mitwohonzentralen v. Die Mitwohonzentrale 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).

<sup>185</sup> 15 U.S.C §§ 7701-7713 (2003). An FTC summary of the Act's requirements is available at <http://www.ftc.gov/bap/online/pubs/buspubs/canspam.htm>. The FTC has issued regulations determining what constitutes commercial e-mail subject to the CAMSpam Act. 16 CFR Part 316.

<sup>186</sup> 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 labelling would not materially help to reduce or block spam. See <http://www.ftc.gov/opa/2005/06/advl.com>

<sup>187</sup> 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>.

destruction of property.<sup>188</sup> Enforcement efforts under the Act began promptly, as internet service providers sued major senders of spam,<sup>189</sup> the FTC began criminal actions,<sup>190</sup> and state enforcement efforts were initiated.<sup>191</sup> 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 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.<sup>192</sup>

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.<sup>193</sup> (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.<sup>194</sup> 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.<sup>195</sup> New York convicted the notorious "Buffalo spammer" on forgery, identity theft and other charges.<sup>196</sup>

As of CAN-SPAM's enactment, at least 35 states had enacted laws regulating spam.<sup>197</sup> 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.<sup>198</sup>

---

<sup>188</sup> P. Festan, "Stiff Spam Penalties Urged," CNETnews.com, <http://news.com.com/2100-1028-5191651.htm> (April 14, 2004).

<sup>189</sup> S. Hansell, "Internet Providers Sue Hundreds Over Unsolicited E-Mail, N.Y. Times, Mar. 10, 2004, <http://www.nytimes.com/2004/03/10/technology/10CMD-SPAM.html>.

<sup>190</sup> "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.

<sup>191</sup> "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).

<sup>192</sup> *Gordon v. Virtumundo*, 2007 WL 2253296 (W.D. Wash. 2007).

<sup>193</sup> 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). 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/2005/1/12/technology/12porn.htm>.

<sup>194</sup> "Attorney General Lockyer wins First-Ever Lawsuit Against Spammer," Cal. Atty. Gen'l Press Release (Oct. 24, 2003), <http://caag.state.ca.us/newsalerts/2003/03-130.htm>.

<sup>195</sup> "North Carolina Man Sentenced to 9 Years for Spam," Tech News on ZD Net, <http://news.zdnet.com/2100-1009-22-5438340.html> (Nov. 3, 2004).

<sup>196</sup> "Man Convicted in Spam Case," N.Y. TIMES (Apr. 2, 2004), p. C4.

<sup>197</sup> 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.

<sup>198</sup> E.g. Tex. Stat., tit. 4, §46.003.

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 possibility, or to fail promptly to stop sending unsolicited commercial e-mail after being requested to do so.<sup>199</sup> 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.<sup>200</sup>

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<sup>201</sup> 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.<sup>202</sup> The 2004 Maryland Spam Deterrence Act imposes criminal penalties, with fines of up to \$25,000, asset forfeiture and prison terms of up to ten years.<sup>203</sup>

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.<sup>204</sup> 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 AOL, and that therefore the Virginia statute had been violated.<sup>205</sup> (Similar actions had also been brought successfully under the federal Computer Fraud and Abuse Act (the "CFAA"),<sup>206</sup>) and SMS text messages sent to cell phones have been found to be subject to the

---

<sup>199</sup> Del. Code Ann., tit. 11, §§937, 938.

<sup>200</sup> Va. Code §18.2-152.3:1.

<sup>201</sup> See <http://www.cbsnews.com/stories/2002/10/09/national/main524957.shtml>.

<sup>202</sup> See <http://www.siliconvalley.com/mld/siliconvalley/news/local/2861505.html>.

<sup>203</sup> Maryland SB604, signed into law May 26, 2004.

<sup>204</sup> Va. Code § 18.2-152.3(3), -152.12

<sup>205</sup> *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 D. (E.D. Va. 1998).

<sup>206</sup> 18 U.S.C. §1030. See, e.g. *Hottmail 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

Telephone Consumer Protection Act, just like unsolicited faxes.<sup>207</sup> And just two days after CAN-SPAM was signed into law, the New York Attorney General announced suits against spammers under state fraud laws.<sup>208</sup>

With the exception of Europe, most other nations are less far along the road to regulation of spam. In North America, Canada, while it has strong privacy protections,<sup>209</sup> has moved more slowly in the area of spam, where the government has expressed the view that legislation is unnecessary.<sup>210</sup> 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,<sup>211</sup> and strengthened the law in 2005 to cover spam directed to business email accounts, prohibiting false sender information and increasing penalties.<sup>212</sup> 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.<sup>213</sup> Australia adopted anti-spam legislation in December 2003 that requires recipient consent, identification of the sender, and an opt-out mechanism.<sup>214</sup> 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.<sup>215</sup> It also requires

---

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). 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).

<sup>207</sup> *Joffe v. Acacia Mortgage Corp.*, 121 P.3d 831(Ariz. Ct. App. 2005), available at <http://www.cofadl.state.az.us/opinionfiles/cv/cv020701.pdf>.

<sup>208</sup> 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>.

<sup>209</sup> For information on Canadian privacy legislation and regulations and related information, see the website of the Privacy Commissioner of Canada, [http://www.privcom.gc.ca/legislation/index\\_e.asp](http://www.privcom.gc.ca/legislation/index_e.asp).

<sup>210</sup> M. Geist, “Time to Hit Delete Key on Weak Spam Policy,” THE GLOBE AND MAIL p. B15 (May 30, 2002), <http://www.theglobeandmail.com/servlet/ArticleNews/printarticle/gam/20020530/TWGEIS2> (article by University of Ottawa Law School professor).

<sup>211</sup> *See* “New Japanese Anti-Spam Rules,” WORLD INTERNET L. REP. (BNA) (Mar. 2002); “Law on Unsolicited E-mail Takes Effect,” Japan Today (Sept. 3, 2001), <http://www.japantoday.com/gidx/news221054.html>.

<sup>212</sup> “Japan Strengthens Anti-Spam Law,” WORLD INTERNET L. REP. (BNA) (July 2005)

<sup>213</sup> 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, [http://www.noie.gov.au/publications/NOIE/spam/final\\_report/SPAMreport.pdf](http://www.noie.gov.au/publications/NOIE/spam/final_report/SPAMreport.pdf) (noting source of South Korean information was a media release and questioning re liability of translation).

<sup>214</sup> The Spam Act 2003, *reported in* Bayside Bulletin (Apr. 16, 2004), <http://redland.yourguide.au>. Further information available at [www.aca.gov.au](http://www.aca.gov.au).

<sup>215</sup> 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://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett). *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

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. (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.<sup>216</sup>

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,<sup>217</sup> 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 sender's identity.<sup>218</sup> 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.<sup>219</sup>

Finally, the United Nations has begun efforts to control spam, suggesting uniform anti-spam legislation that would facilitate cross-border enforcement cooperation.<sup>220</sup>

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.<sup>221</sup>

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.<sup>222</sup> In December 2006, Sony BMG settled with forty states and the District of

---

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 [www.spamlaws.com/docs/2000-31-ec.pdf](http://www.spamlaws.com/docs/2000-31-ec.pdf).

<sup>216</sup> M. Breersma, "EU Legislation - No Market For Spam," eWeek (Aug. 26, 2004), [www.eweek.com/print\\_article/0,1761,a=134119,00.asp](http://www.eweek.com/print_article/0,1761,a=134119,00.asp).

<sup>217</sup> For listings of the status of anti-spam laws in European nations, with links to the text and translations of enacted and pending legislation, see <http://www.euro.cauce.org/en/countries/index.html>. See also <http://www.spamlaws.com/eu.html>.

<sup>218</sup> District Court of Zurich (Decision of 6th December 2002, ZR 102, 2003, no. 39).

<sup>219</sup> See <http://www.euro.cauce.org/en/countries/index.html>.

<sup>220</sup> "UN Aims to Bring Spam Under Control Within Two Years," <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/9090561.htm>.

<sup>221</sup> 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>.

<sup>222</sup> "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*

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.<sup>223</sup> 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.<sup>224</sup>

### 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.<sup>225</sup> 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.<sup>226</sup> 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 survives today, in other words, largely as a little brother of conversion.”<sup>227</sup>

The transmission of electronic signals through a computer network has been held to be sufficiently physical contact to constitute trespass to property.<sup>228</sup> 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.<sup>229</sup> 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.<sup>230</sup>

---

*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).

<sup>223</sup> “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).

<sup>224</sup> *Matter of Sony BMG Music Entertainment*, FTC File No. 062-3019, available at <http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf>.

<sup>225</sup> *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

<sup>226</sup> *Oyster Software, Inc. v. Forms Software, Inc.*, 2001 U.S. Dist. LEXIS 22520 (N.D. Cal. 2001).

<sup>227</sup> *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).

<sup>228</sup> *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).

<sup>229</sup> *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 WL 1887522, No. 99 CV7654, \*4 (C.D. Cal. Aug. 10, 2000).

<sup>230</sup> *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).

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.<sup>231</sup>

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.<sup>232</sup> 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.<sup>233</sup>

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 contents of the e-mail, "an injury entirely separate from, and not directly affecting, the possession or value of personal property."<sup>234</sup> 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.<sup>235</sup>

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*,<sup>236</sup> 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.<sup>237</sup>

## J. Privacy

As the use of the Internet 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

---

<sup>231</sup> *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).

<sup>232</sup> *Intel Corp. v. Hamidi*, 1 Cal Rptr. 3d 32, 30 Cal. 4th 1342, 71 P.3d 296 (Cal.Sup.Ct. 2003).

<sup>233</sup> *Id.* at 36.

<sup>234</sup> *Id.* at 37.

<sup>235</sup> *Id.* at 44.

<sup>236</sup> 384 F.Supp.2d 1219 (N.D. Ill. 2005).

<sup>237</sup> *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>.

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.

### 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 relatively unregulated in the United States. Except in a few specific areas, discussed below, the U.S. has adopted a laissez-faire approach to the issue. Use of such data is far more restricted in Europe.<sup>238</sup> The European Community's 1998 Directive on "Transborder Flows of Personal Data"<sup>239</sup> prohibits companies from transmitting data to countries that do not adequately protect it.<sup>240</sup>

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 formal 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.<sup>241</sup> Indeed, EC enacted a new 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.<sup>242</sup> Spyware, web bugs and similar devices, that can store hidden information or trace user activities, are permitted only for legitimate purposes with the user's knowledge.<sup>243</sup> (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,<sup>244</sup> the Canadian Privacy Commission found that an airline's denial of access to users

---

<sup>238</sup> 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/pdf/files/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>.

<sup>239</sup> The Directive is available at [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett) and [http://www.privacy.org/pi/intl\\_orgs/ec/eudp.html](http://www.privacy.org/pi/intl_orgs/ec/eudp.html).

<sup>240</sup> 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).

<sup>241</sup> 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).

<sup>242</sup> 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://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett). 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.

<sup>243</sup> *Id.*

<sup>244</sup> *Id.*

who refused cookies was a violation of the Canadian Protection of Personal Information and Electronic Documents Act.<sup>245</sup> This Canadian law became applicable on January 1, 2004 to all companies – including U.S. companies – that collect, use or disclose personal information about Canadian citizens in the course of commercial activities.)

The EU Directive affects 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<sup>246</sup> 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;<sup>247</sup>
- (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;
- (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

---

<sup>245</sup> 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.privcom.gc.ca/cf-dc\\_030416\\_7\\_e.asp](http://www.privcom.gc.ca/cf-dc_030416_7_e.asp), reported in “Canada: Airline Violated Privacy Law Using Computer Cookies,” WORLD INTERNET L. REP. (BNA) at p.27 (July, 2003).

<sup>246</sup> For more information on the Safe Harbor Agreement see the Commerce Department’s website at [www.export.gov/safeharbor](http://www.export.gov/safeharbor)

<sup>247</sup> 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.

(g) *Enforcement*: A mechanism for enforcing compliance with these principles.<sup>248</sup>

A comprehensive checklist is available on the Department of Commerce's Safe Harbor website, [www.export.gov/safeharbor/index.html](http://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.<sup>249</sup> (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.)

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.<sup>250</sup>

United States companies should consider bringing themselves within the safe harbor if they collect personal data from individuals in the EC. This means certifying to the Department of Commerce their adherence to the safe harbor principles and implementing privacy policies that comply with those principles.<sup>251</sup>

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.<sup>252</sup> The report suggests 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.<sup>253</sup> Major companies are beginning to use the format.<sup>254</sup>

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

---

<sup>248</sup> See [www.ita.doc.gov/td/ecom/shprinciplesfinal.htm](http://www.ita.doc.gov/td/ecom/shprinciplesfinal.htm).

<sup>249</sup> See J. Clausing, *Europe and U.S. Reach Data Privacy Pact*, N.Y. TIMES, Mar. 15, 2000.

<sup>250</sup> 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); *Newby v. Amazon.com* (N.D.Cal.) (filed Jan. 7, 2000), reported at <http://news.cnet.com/news/0-1007-200-1517791.html>.

<sup>251</sup> As of January 18, 2005, there were 647 companies on the Department of Commerce's certified list, see <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>.

<sup>252</sup> 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).

<sup>253</sup> "Opinion on More Harmonised Information Provisions," Article 29 Data Protection Working Party, 11987/04/EN, WP100 (Nov. 25, 2004);

[http://europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs/2004/wp100\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp100_en.pdf); see M. Campanelli, "EU Issues Guidance on Privacy Notices," DMNEWS (Jan. 5, 2005), [http://www.dmnews.com/cgi-bin/artprevbot.cgi?article\\_id=31430](http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=31430).

<sup>254</sup> J. Vijayan, "Companies Simply Data Privacy Notices," COMPUTERWORLD (Jan. 10, 2005), <http://computerworld.com/managementtopics/management/story/0,10801,98812,00.html?SKC=management-98812>.

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.<sup>255</sup> Note that companies that outsource data processing to third parties remain responsible for breaches of privacy occurring at the third parties' hands.<sup>256</sup> Another option is the development of "binding corporate rules" for internal governance within the organization. Such binding rules must be legally enforceable and subject to audit, and subject to approval by data protection authorities.<sup>257</sup>

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 Directive.<sup>258</sup>

The EC's investigation, initiated in May 2002, into whether Microsoft's Passport Internet authorization system violates EU rules<sup>259</sup> 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.<sup>260</sup>

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.<sup>261</sup> Hewlett-Packard agreed to remedy the problem.

---

<sup>255</sup> See <http://europa.eu.int/eur-lex/LexUriServ/site/en/oi/2004/81385/138520041229en00740084.0df>; <http://europa.eu.int/comm/privacy>; 4 WORLD DATA PROTECTION REP. (No. 3) of 1 (March 2004); see also "standard contractual clauses for the transfer of personal data to third countries – Frequently asked questions," MEMO/05/3 (Jan. 7, 2005), <http://europa.eu.int/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=1&language=EN&guiLanguage=en>.

<sup>256</sup> 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/print.html](http://www.theregister.co.uk/2006/07/12/outsourced_data_protection/print.html).

<sup>257</sup> 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), available at [http://newsweaver.co.uk/bnainternational/e\\_article000457103.cfm?x=b5H6IVW,b2sjsql8L](http://newsweaver.co.uk/bnainternational/e_article000457103.cfm?x=b5H6IVW,b2sjsql8L). 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>.

<sup>258</sup> *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>.

<sup>259</sup> "Microsoft Faces European Commission Inquiry on Privacy Concerns," N.Y. TIMES, May 28, 2002, at p. C4; "Microsoft's European Passport Troubles," <http://www.ciol.com/content/news/trends/102061301.asp>.

<sup>260</sup> "European Union Microsoft 'Passport' – Commission Will Not Impose Sanctions," WORLD INTERNET L. REP (BNA) at 30 (Feb. 2003).

<sup>261</sup> Hunton & Williams, Privacy and E-Commerce Alert (March 14, 2003).

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.<sup>262</sup>

More recently, 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.<sup>263</sup> 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."<sup>264</sup> The French data protection agency, the Commission Nationale d' Information et des Libertés ("CNIL") found that anonymous hotlines would "reinforce the risk of slanderous denunciations" and "was disproportionate to the objectives sought."<sup>265</sup> In addition, a French court ordered the French subsidiary of a U.S. company to discontinue a whistleblower hotline, on similar grounds.<sup>266</sup>

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.<sup>267</sup> 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, 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<sup>268</sup>, 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

---

<sup>262</sup> "Privacy: French Agency Decries Bad-Credit Blacklist, Citing Sharing of Data Beyond Affected Sector," BANKING DAILY (BNA) (December 17, 2003). Statement of Commission Nationale de l'Informatique et Libertés, available in French at [http://www.cnil.fr/frame.htm?thematic/listesnoires/accueil\\_listes.htm](http://www.cnil.fr/frame.htm?thematic/listesnoires/accueil_listes.htm).

<sup>263</sup> Sarbanes Oxley Act of 2002 §301; SEC Rule 10A-3(b)(3).

<sup>264</sup> Arbeitsgericht Wuppertal, Court order dated June 15, 2005, 5 BV 20/05; *English translation available at* <http://www.theworldlawgroup.com/newsletter/details.asp?ID=745557282005>.

<sup>265</sup> CNIL Decision 2005-110 of May 26, 2005 (Exide Technologies): *English translation available at* <http://www.theworldlawgroup.com/newsletter/details.asp?ID=1246367122005> and <http://www.theworldlawgroup.com/newsletter/details.asp?ID=1943487122005>.

<sup>266</sup> 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](http://www.legalis.net/jurisprudence-decision.php3?ID_article=1497).

<sup>267</sup> CNIL, "Guideline document adopted by CNIL on 10 November 2005 for the implementation of whistleblowing systems....," available at <http://www.cnil.fr/fileadmin/documents/uk/CNIL-recommandations-whistleblowing-VA.pdf>.

<sup>268</sup> 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](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf).

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
- 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.

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.<sup>269</sup> Many major U.S. companies are adapting global privacy standards based on the E.U. model. Proctor & Gamble, Dupont and General Electric are examples.<sup>270</sup> Indeed, a number of corporations, such as P&G and AXA Financial Services, take the approach of complying with the strictest applicable privacy requirements.<sup>271</sup>

## 2. U.S. Online Privacy Regulation

### a. Federal Trade Commission Regulation

Events in recent years suggest that the American laissez-faire approach to consumers' privacy has begun to change, albeit slowly. The Federal Trade Commission has become the 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" (hereafter, the "1998 Privacy Report").<sup>272</sup> That report asserts as 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."<sup>273</sup>

A similar FTC report to Congress in 2000 emphasized the same four key elements known as the Fair Information Practice Principles.<sup>274</sup>

### b. More Recent FTC 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%.<sup>275</sup> Among the issues on the FTC's pro-privacy agenda are enforcing the privacy promises posted on websites,<sup>276</sup> investigating complaints of U.S. companies failing to

---

<sup>269</sup> 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>.

<sup>270</sup> *Id.*

<sup>271</sup> See L. Conley, "Refusing to Gamble on Privacy," Fast Company, No. 84 (June 2004), [http://www.fastcompany.com/magazine/84/essay\\_hughes.html](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>.

<sup>272</sup> See [www.ftc.gov/reports/privacy3/priv-23a.pdf](http://www.ftc.gov/reports/privacy3/priv-23a.pdf).

<sup>273</sup> 1998 Privacy Report, at Executive Summary (emphasis in original).

<sup>274</sup> See [www.ftc.gov/reports/privacy2000/privacy2000.pdf](http://www.ftc.gov/reports/privacy2000/privacy2000.pdf); [www.ftc.gov/reports/privacy2000/pitofskystmtonlineprivacy.html](http://www.ftc.gov/reports/privacy2000/pitofskystmtonlineprivacy.html).

<sup>275</sup> *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>.

<sup>276</sup> 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,

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,<sup>277</sup> and its settlement of charges against two companies that collected personal data from high school students and sold them to commercial marketers despite promises not to do so.<sup>278</sup>

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.<sup>279</sup>

In early 2002, the FTC settled an action against Eli Lilly and Co. for alleged inadvertent violation of its privacy policy.<sup>280</sup> 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.<sup>281</sup> 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.<sup>282</sup> A similar case was settled in 2004 by Tower

---

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.

<sup>277</sup> See WORLD DATA PROTECTION REPORT (BNA) (January 2002) at 17.

<sup>278</sup> 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).

<sup>279</sup> Gateway Learning Corp., FTC File No. 042-3047, Trade Cas. (CCH) ¶15,617 (2004).

<sup>280</sup> In re Eli Lilly and Co., FTC No. 0123214 (Jan. 18, 2002) reported in WORLD DATA PROTECTION REP. (BNA) at 12.

<sup>281</sup> 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.

<sup>282</sup> 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>.

Records and Petco Animal Supplies, with a similar security program required by the FTC.<sup>283</sup> 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.<sup>284</sup> 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 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 and biennial independent audits over a twenty-year period.<sup>285</sup>

The FTC in these cases 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.<sup>286</sup> Similar approaches appear in the information security guidelines adopted as Recommendations by the Organization for Economic Cooperation and Development Council on July 25, 2002<sup>287</sup> and the FTC’s final rule establishing information security standards for customer information under the Gramm-Leach-Bliley Act,<sup>288</sup> 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.<sup>289</sup> 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.<sup>290</sup>

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

---

<sup>283</sup> “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).

<sup>284</sup> 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>.

<sup>285</sup> 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 Title Agency, Inc., Nations Holding Company and Christopher M. Likens*, File No. 052 3117.

<sup>286</sup> *Id.* at 194.

<sup>287</sup> See [www.oecd.org/document/42/0,2340,en\\_2649\\_201185\\_15582250\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html).

<sup>288</sup> See [www.ftc.gov/opa/2002/05/safeguardrule.htm](http://www.ftc.gov/opa/2002/05/safeguardrule.htm).

<sup>289</sup> 16 C.F.R. Part 682 (2005).

<sup>290</sup> “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>.

not be permitted to disclose customer data, at least without notice and an opportunity to opt out.<sup>291</sup>

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,<sup>292</sup> 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.<sup>293</sup>

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.<sup>294</sup>

Finally, recognizing that security will never be perfect, plans to respond when breaches occur are essential. 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,<sup>295</sup> and another survey found that 84% of 642 large North American organizations suffered a security incident in the previous year.<sup>296</sup> 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 taken, such as offering free credit monitoring service.

### 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,

---

<sup>291</sup> 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).

<sup>292</sup> See J. Schwartz, "Surveillance 101—Privacy vs. Security on Campus," N.Y. TIMES, Week in Review (Aug. 4, 2002).

<sup>293</sup> 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>.

<sup>294</sup> See T.J. Smedinghoff, "Trends in the Law of Information Security," WORLD INTERNET L. REP. (BNA) (August 2004) at 13.

<sup>295</sup> D.Kaplan, "Three of four financial institutions suffered external breach in past year," SC Magazine (June 14, 2006), <http://www.scmagazine.com/uk/news/index.cfm?fuseaction=XCK.News.Article&nNewsId=564512>.

<sup>296</sup> "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>.

whether on an opt-out or opt-in basis.<sup>297</sup> 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.<sup>298</sup> Alaska, California, Connecticut, Illinois and Vermont have also adopted financial privacy legislation,<sup>299</sup> although the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act),<sup>300</sup> 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. 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,<sup>301</sup> 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, a California gives identity theft victims the right to place a security alert on their credit report to prevent further fraudulent activity.<sup>302</sup> The FACT Act contains a comparable provision<sup>303</sup> 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.<sup>304</sup>

California was the first state to address the security of customer information in a law that became effective July 1, 2003.<sup>305</sup> 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.<sup>306</sup> Similar breach notification bills have been

---

<sup>297</sup> Minn. Laws 2002, ch.395; for text see [www.spamlaws.com/state/mn.html](http://www.spamlaws.com/state/mn.html).

<sup>298</sup> 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.

<sup>299</sup> 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/Regs&Bulls/bnkregs/REG\\_B2001\\_01.pdf](http://www.bishca.state.vt.us/Regs&Bulls/bnkregs/REG_B2001_01.pdf). 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>.

<sup>300</sup> Pub. L. 108-159.

<sup>301</sup> 16 C.F.R. § 602.1.

<sup>302</sup> Cal. Civil Code § 1785.15.

<sup>303</sup> FACT Act of 2003, Pub. L. 108-159, § 112.

<sup>304</sup> 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).

<sup>305</sup> California Civil Code §1798.82.

<sup>306</sup> 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," N.Y. TIMES, February 24, 2005, <http://www.nytimes.com/reuters/politics/politics-tech-choicepoint.html>.

passed in most states.<sup>307</sup> The private bar has gotten into the act, with at least one negligence action filed against a health care firm for negligence in failing to safeguard healthcare records.<sup>308</sup>

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.<sup>309</sup>

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.<sup>310</sup> And the California Online Privacy Act of 2003 (A.B. 68) requires online businesses that collect personally identifiable information from California residents to post a privacy policy and inform customers about what data will be collected and how it will be used, with a private right of action provided for.<sup>311</sup>

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.<sup>312</sup> In 2002, California adopted legislation, effective July 1, 2003, requiring firms that conduct business in California to disclose promptly any breaches of security

---

<sup>307</sup> Such laws have been enacted in Arizona, Arkansas, Alaska, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington, Wisconsin, Wyoming and Washington D.C. *See* E-COMMERCE LAW WEEK (April 23, 2005, May 5, 2005, June 11, 2005, June 23, 2005, July 2, 2005, December 31, 2005, April 1, 2006, May 6, 2006, June 15, 2006, January 6, 2007, June 2, 2007 and July 7, 2007), available at [www.stepto.com](http://www.stepto.com). 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/ecom/doc/library/proposals/dir\\_citizens\\_rights\\_en.pdf](http://ec.europa.eu/information_society/policy/ecom/doc/library/proposals/dir_citizens_rights_en.pdf). Other countries such as Canada and New Zealand, have issued voluntary breach notification guidelines. WORLD DATA PROT.REP. (BNA) (Sept., 2007)

<sup>308</sup> *See* E-COMMERCE LAW WEEK (Feb. 12, 2006), available at [www.stepto.com/E-CommerceLawWeek](http://www.stepto.com/E-CommerceLawWeek) (reporting on class action complaint by former patient against Providence Health System in Oregon Circuit Court, Multnomah County).

<sup>309</sup> 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](http://news.com.com/2100-1030_3-6039645.html).

<sup>310</sup> 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)).

<sup>311</sup> J. Vijayan, "First Online Privacy Law Looms in California," COMPUTERWORLD (June 28, 2004), <http://www.computerworld.com/printthis/2004/0,4814,94128,00.html>.

<sup>312</sup> "DoubleClick Settles Privacy Inquiry," N.Y. TIMES (Aug. 27, 2002) at C3.

affecting personal data of a California resident to that resident.<sup>313</sup> The new law provides for private actions for damages, and injunctive relief.

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."<sup>314</sup> 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.<sup>315</sup> 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 emails, 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.<sup>316</sup>

A major security breach of TJX Companies, Inc., the owner of retail chains such as T.J. Maxx and Marshall's, in which hackers stole over 40 million credit card numbers, that were inadequately encrypted, led to a multistate investigation by state attorneys general as well as private class action suits.<sup>317</sup>

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.<sup>318</sup>

### 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"),<sup>319</sup> 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.

---

<sup>313</sup> Ch. 915, Statutes of 2002; Cal. Civ. Code §§ 1798.29, 1798.82-.84.

<sup>314</sup> 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>.

<sup>315</sup> L. Rosencrance, "Barnesandnoble.com Hit with Fine for Online Security Breach," COMPUTERWORLD (April 30, 2004), <http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,92804,00.f=x62>.

<sup>316</sup> Press Release, "Investigation Reveals Massive Privacy Breach," Office of New York State Attorney General Eliot Spitzer (March 13, 2006), available at [http://www.oag.state.ny.us/press/2006/mar/mar13a\\_06.html](http://www.oag.state.ny.us/press/2006/mar/mar13a_06.html).

<sup>317</sup> See 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\\_P M&nid=8](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010884&source=NLT_P M&nid=8).

<sup>318</sup> "Student Survey Firms Settle Charges FTC of Selling Data to Marketers," 84 ANTITRUST & TRADE REG. REP. (BNA) 80 (January 31, 2003).

<sup>319</sup> 15 U.S.C. §§ 6501 *et seq.*

The FTC regulations,<sup>320</sup> 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.<sup>321</sup>

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<sup>322</sup> 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 May 1999, before issuance of the regulations, the FTC settled charges against Liberty Financial Companies, Inc. alleging that the company solicited information from children and teenagers on the representation that the information would be totally anonymous, when in fact it was maintained in a database in identifiable form.<sup>323</sup> The settlement prohibited Liberty Financial from making misrepresentations about its collection of personal information from children under 18, and from collecting personal information from children under 18 if it knows the child does not have parental consent to provide it. The settlement further requires prominent notice regarding the collection and use of information, a procedure for obtaining verifiable parental consent and deletion of all information previously collected from children.

In its first enforcement action under COPPA, the FTC imposed fines totaling \$100,000.<sup>324</sup> 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.<sup>325</sup> 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

---

<sup>320</sup> 16 CFR Part 312 (1999); TRADE REG. REP. (CCH) No. 575 Part 2 (April 28, 1999).

<sup>321</sup> *3 Web Operators Settle COPPA Charges For Unauthorized Collection of Personal Data*, 80 ANTITRUST & TRADE REG. REP. 2004 (BNA) (Apr. 20, 2001), at 357.

<sup>322</sup> 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.

<sup>323</sup> *Liberty Financial Companies, Inc.* TRADE CAS. (CCH) ¶ 24,598 (1999).

<sup>324</sup> 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).

<sup>325</sup> *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>.

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.<sup>326</sup>

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 than was necessary for participation in the “club” and that its privacy policy did not comply with COPPA’s requirements. The settlement required a \$35,000 civil penalty and the deletion of all personal information improperly collected for the past two years.<sup>327</sup>

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.<sup>328</sup> 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.<sup>329</sup>

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.”<sup>330</sup> 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

---

<sup>326</sup> *Manufacturer of Popular Girls’ Toys Settles FTC Charges of Violating COPPA*, 81 ANTITRUST & TRADE REG. REP. 2027 (BNA) (Oct. 5, 2001).

<sup>327</sup> 82 ANTITRUST & TRADE REG. REP. (BNA) 365 (April 26, 2002); *eSchool News online*, <http://www.eschoolnews.com/news/showStory.cfm?ArticleID=3744&ref=wo>.

<sup>328</sup> “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>.

<sup>329</sup> “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/bonziung.htm>.

<sup>330</sup> *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).

to COPPA, with the FTC finding that the vocabulary and language on the site appeared to be directed to adults.<sup>331</sup>

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.<sup>332</sup> 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.<sup>333</sup>

## **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 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.<sup>334</sup>

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

---

<sup>331</sup> 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.html](http://news.com.com/2100-1038_3-5470145.html).

<sup>332</sup> 82 ANTITRUST & TRADE REG. REP. (BNA) 365 (April 26, 2002).

<sup>333</sup> See, e.g., *Privo, Inc.*, TRADE CAS. (CCH) ¶ 15,637 (2004).

<sup>334</sup> *N.Y. State Bar Association v. FTC*, 2004 WL 964173, 2004 TRADE CAS. (CCH) ¶ 74,383 (D.D.C. 2004).

regulated by another federal regulatory body.<sup>335</sup> 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.<sup>336</sup> (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 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”).<sup>337</sup> 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

---

<sup>335</sup> 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.

<sup>336</sup> Available at <http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/attachment.pdf>.

<sup>337</sup> 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/online/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.

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”).<sup>338</sup> 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.<sup>339</sup>

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.<sup>340</sup> Pursuant to the Safeguards Rule, a financial institution must 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.<sup>341</sup> 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.<sup>342</sup> This transition rule gave financial institutions two years to require their service providers, by contract, to implement an ISP.<sup>343</sup> 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

---

<sup>338</sup> See 16 C.F.R. 314.3(a).

<sup>339</sup> See 16 C.F.R. 314.4(a)-(e).

<sup>340</sup> See 16 C.F.R. 314.4(d)(2).

<sup>341</sup> 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.

<sup>342</sup> 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.

<sup>343</sup> See 16 C.F.R. 314.5(b). See also FTC Commentary to 16 C.F.R. 314.

monitor an ISP and on how to oversee a third-party service provider in the near future.<sup>344</sup> The FTC has brought charges under the Safeguards Rule for failure to have reasonable protection for customers' sensitive information.<sup>345</sup>

Several financial regulatory agencies have proposed regulations to govern financial institution responses to breaches of customer information security.<sup>346</sup> 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.

### c. Medical Records – HIPAA

Privacy of individually identifiable health information is regulated by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)<sup>347</sup> and regulations promulgated under HIPAA. HIPAA regulates “covered entities, which include health care providers, health plans and “health care clearinghouses”<sup>348</sup> 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.<sup>349</sup>

Under revised regulations issued in August 2002,<sup>350</sup> 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 proprietary drugs to patients that the pharmacy records indicate use competing products, without the knowledge or consent of the patients.<sup>351</sup>

In addition, HIPAA security standards, effective April 21, 2005, require health care organizations to ensure the confidentiality, security, integrity and availability of electronic health

---

<sup>344</sup> Federal Trade Comm'n, “Financial Institutions and Customer Data: Complying with the Safeguards Rule” (September 2002), available at <http://www.ftc.gov/bcp/online/pubs/bspubs/safeguards.pdf>.

<sup>345</sup> See *Sunbelt Leading Services, Inc.*, TRADE CAS. (CCH) ¶ 15,678 (2004).

<sup>346</sup> 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).

<sup>347</sup> Pub.L.No.104-191, 110 Stat. 1936 (1996).

<sup>348</sup> 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).

<sup>349</sup> 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](http://www.eurekalert.org/pub_releases/2004-09/uopm-prb091304.php).

<sup>350</sup> 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)

<sup>351</sup> A. Zimmerman & D. Armstrong, “How Drug Makers Use Pharmacies To Push Pricey Pills,” WALL STREET J., p.A1 (May 1, 2002).

information and protect it against unauthorized disclosure or use.<sup>352</sup> Notwithstanding the delayed effective date, these security regulations are likely to become the de facto standard for compliance with the HIPAA privacy regulations.<sup>353</sup> 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.<sup>354</sup> In addition, the security rules impose 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.<sup>355</sup>

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.

#### **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. Up to 14 million U.S. workers are subject to continuous surveillance of their e-mail and Internet use while at work.<sup>356</sup>

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.<sup>357</sup> An American Management Association Survey in 2003 found that most U.S. companies monitor employee e-mail to some degree and enforce company e-mail policies with discipline, with 22% of companies having terminated employees for e-mail policy violations.<sup>358</sup>

The announced policy is important, however, to avoid falling under the Electronic Communications Privacy Act of 1986<sup>359</sup> – 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

---

<sup>352</sup> 45 CFR Parts 160, 162 and 164 (2003), available at <http://www.cms.hhs.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf>.

<sup>353</sup> 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>.

<sup>354</sup> See S. Weil, “HIPAA Security Rule: What It Is & How to Comply With It,” Security Focus (March 1, 2004), <http://www.securityfocus.com/infocus/1764>.

<sup>355</sup> 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.

<sup>356</sup> 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>.

<sup>357</sup> 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); *McLaren v. Microsoft Corp.*, No. 05-97-00824-cv (Tex. Ct. App. 1999); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996); *Restuccia v. Burk Technology, Inc.*, No. 95-2125 (Mass. Supr. Ct. 1996).

<sup>358</sup> AMA Research, “2003 E-mail Rules, Policies and Practices Survey,” (2003), [http://www.amanet.org/research/pdfs/Email\\_Policies\\_Practices.pdf](http://www.amanet.org/research/pdfs/Email_Policies_Practices.pdf).

<sup>359</sup> 18 U.S.C §§ 2510 *et seq.*

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.<sup>360</sup>

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 emails in transit, the First Circuit panel held it was lawful.<sup>361</sup> 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."<sup>362</sup> 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 emails accessed in while in storage were not covered by the wiretap act.<sup>363</sup>

State laws may provide differing rights and obligations, and need to be reviewed as well.

In other countries, the rules may vary, although the European Commission plans to propose a draft Directive on Privacy in the Workplace by 2005,<sup>364</sup> 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.<sup>365</sup> 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

---

<sup>360</sup> 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.

<sup>361</sup> *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](http://www.eff.org/news/archives/2004_06.php#001658).

<sup>362</sup> *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005).

<sup>363</sup> *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443 (C. D. Cal. 2007).

<sup>364</sup> "Working Document on the Surveillance of Electronic Communication in the Workplace," Article 29 – Data Protection Working Party (May 29, 2002), available at [http://europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs/2002/wp55\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_en.pdf).

<sup>365</sup> 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/Ld.cfm?i=1010327&Newsletters\\_Ref=5528](http://www.Internationallawoffice.com/Ld.cfm?i=1010327&Newsletters_Ref=5528) (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/Ld.cfm?i=1010327&Newsletters\\_Ref=523](http://www.internationallawoffice.com/Ld.cfm?i=1010327&Newsletters_Ref=523) (reporting Tribunal of Milan ruling that employer may monitor e-mails received by employee in company mailbox); [http://www.worldbusinesslawreport.com/index.cfm?selectedpub=1.8&action=dsp\\_item&id=712](http://www.worldbusinesslawreport.com/index.cfm?selectedpub=1.8&action=dsp_item&id=712); I. Gavanon & A. Bowlant, "France – Employee Internet Usage: When Is Monitoring by Employers Allowed?," WORLD INTERNET L. REP (BNA) 30 (June 2002).

in almost all cases.<sup>366</sup> 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.<sup>367</sup>

#### 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,<sup>368</sup> 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.<sup>369</sup> This led, however, to protests from some in Europe that the accommodation was a political decision in violation of EU law,<sup>370</sup> 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.<sup>371</sup> 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.<sup>372</sup> Even within the EU, this issue has been debated. EU plans

---

<sup>366</sup> “Respect Workers’ Privacy, Employers Told,” *GUARDIAN UNLIMITED* (June 11, 2003), <http://money.guardian.co.uk/work/story/0,1456,975109,00.html>.

<sup>367</sup> See “South Korea First Criminal Case on Corporate Surveillance of Employees’ E-Mail,” *WORLD INTERNET L. REP.* (BNA) 11 (June 2002).

<sup>368</sup> “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://europa.eu.int/comm/internal\\_market/privacy/docs/adequacy/apis-communication/apis\\_en.pdf](http://europa.eu.int/comm/internal_market/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.int/rapid/start/cgi/guesten.ksh?p\\_action.gettxt=gt&doc=SPEECH/03/613|0|AGED&lg=EN](http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=SPEECH/03/613|0|AGED&lg=EN)

<sup>369</sup> “DHS and EU Sign Agreement to Allow Collection of Passenger Data,” Department of Homeland Security (May 28, 2004), <http://www.dhs.gov/dhspublic/display?content=3650>.

<sup>370</sup> 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://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+PRESS+NR-20031217-1+0+DOC+XML+V0//EN&LEVEL=2&NAV=S>.

<sup>371</sup> See “EU court annuls data deal with US,” *BBC News* (May 30, 2006), <http://news.bbc.co.uk/2/hi/europe/5028918.stm>; L. Pasveer, “Court outlaws EU-U.S. passenger data transfer,” *C|net news.com* (May 30, 2006) [http://news.com.com/2100-1029\\_3-6077893.html](http://news.com.com/2100-1029_3-6077893.html); S. Leatham, “EU-USA Agreement Challenged by European Parliament,” *ElectricNews.net* (June 30, 2004), <http://www.electricnews.net/news.html?code=95415064>; G. Meade, “MEPs Block US Counter-Terrorism Deal,” *scotsman.com* (April 21, 2004), <http://news.scotsman.com/latest.cfm?id=2811081>.

<sup>372</sup> 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), [http://www.eur-lex.europa.eu/LexUriServ/site/en/oj/l\\_204/l\\_20420070804en00180025.pdf](http://www.eur-lex.europa.eu/LexUriServ/site/en/oj/l_204/l_20420070804en00180025.pdf).

to require companies to retain telephone and email records to assist in anti-terrorism investigations have been criticized by privacy regulators.<sup>373</sup>

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 and other U.S. agencies, violated European data protection regulations and was a "gross miscalculation." The report 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.<sup>374</sup> The EU Article 29 Working Party came to the same conclusion.<sup>375</sup> SWIFT subsequently announced it would stop processing European banking transactions in the U.S.<sup>376</sup>

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<sup>377</sup> and several U.S. government investigations reissued.<sup>378</sup> 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 has brought criticism from privacy advocates.<sup>379</sup> 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.<sup>380</sup>

---

<sup>373</sup> "EU data protection chief warns against anti-terrorism plans," SiliconValley.com (Sept. 26, 2005), <http://www.siliconvalley.com/mls/siliconvalley/business/technology/12746814.htm>.

<sup>374</sup> 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>.

<sup>375</sup> 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](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf).

<sup>376</sup> "SWIFT to stop processing EU banking data in the US," THE REGISTER (Oct. 15, 2007), [http://www.theregister.co.uk/2007/10/15/swift\\_processing\\_halt/print.html](http://www.theregister.co.uk/2007/10/15/swift_processing_halt/print.html).

<sup>377</sup> Electronic Privacy Information Center Complaint and Request for Injunction, Investigation and for Other Relief, *Matter of JetBlue Airways Corp.*, available at <http://www.epic.org/privacy/airtravel/profiling/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://jetblue.com/learnmore/pressDetail.asp?newsId=202>.

<sup>378</sup> T. Katzer, "Senator Probe Airliner Passenger Security Breaches," Information Week (April 14, 2004), <http://www.informationweek.com/story/showArticle.jhtml?ArticleID=18901493>.

<sup>379</sup> *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>.

<sup>380</sup> 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.

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.<sup>381</sup> Nonetheless, conflicts have arisen, a few examples of which follow.

A recent lawsuit alleges misuse of the National Crime Information Center database by the U.S. Department of Justice and the FBI in the enforcement of immigration laws.<sup>382</sup>

The USA PATRIOT Act,<sup>383</sup> 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,<sup>384</sup> 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."<sup>385</sup> Unsurprisingly, the Department of Justice's view of the Act is rather different, as expressed in an article available on its website.<sup>386</sup>

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.<sup>387</sup> At a minimum, these financial institutions are required to obtain the name,

---

<sup>381</sup> 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/dhspublic/interapp/speech/speech\\_0144.xml](http://www.dhs.gov/dhspublic/interapp/speech/speech_0144.xml).

<sup>382</sup> *National Council of La Raza v. Ashcroft*, No. CV03-6324 (E.D.N.Y.) (complaint filed Dec. 17, 2003), *available at* <http://www.adc.org/uploads/media/dojsuit.pdf>; *see also* National Council of La Raza, "Administration Misuses Criminal Database, Unlawfully Targets Immigrants," Press Release (Dec. 17, 2003) *available at* [http://nclr.policy.net/proactive/newsroom/release.vtml?id=24120&PROACTIVE\\_ID=cecfcfac7cfcbebc9c5cecfcfcc5cececcc9cbceccdbcdcdc5cf](http://nclr.policy.net/proactive/newsroom/release.vtml?id=24120&PROACTIVE_ID=cecfcfac7cfcbebc9c5cecfcfcc5cececcc9cbceccdbcdcdc5cf).

<sup>383</sup> 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).

<sup>384</sup> *Id.* at § 215 amending the Foreign Intelligence Surveillance Act, tit. V, § 501(a)(1).

<sup>385</sup> 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](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](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>.

<sup>386</sup> 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).

<sup>387</sup> *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; "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

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<sup>388</sup>, 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.<sup>389</sup>

## II. *Patent Protection of Software and Business Methods*

Patent protection of software and business methods are becoming increasingly important topics for businesses. The past four years have seen an explosion of patent registrations containing the word “software”: up from 125 applications in 1996 to 40,000 in 1999.<sup>390</sup> Similarly, the number of patent applications dealing with computer implemented business methods doubled in only one year, from 1,300 in FY98 to 2,600 in FY99.<sup>391</sup>

Because of the number of business method patents being presented at the PTO, the evaluation process is being reviewed in order to improve it, allowing patents only for “true innovations.”<sup>392</sup> Legislation has also been introduced to improve the functioning of the PTO in response to this increase.<sup>393</sup> Proposed changes include (1) creating a rebuttable presumption that a business method invention consisting of a non-novel computer implementation of a pre-existing invention is obvious, and thus not patentable,<sup>394</sup> (2) requiring early publication of all business method patent applications, (3) establishing an administrative opposition process for challenging business method patents, and (4) lowering the burden of proof for business method patents.<sup>395</sup>

The explosion in business method patents was due largely to the landmark 1998 decision of the United States Court of Appeals for the Federal Circuit holding that software was broadly patentable in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*<sup>396</sup> The Court held that software running on a general purpose computer, that produces a “useful, concrete and tangible result,” is protectible, assuming it meets other statutory requirements, without the need to focus on whether it is a “process, machine, manufacture or composition of matter,” and even if

---

Identification Programs for Futures Commission Merchants and Introducing Brokers”]; joint final rules. 68 Fed. Reg. 25149-25162 (May 9, 2003).

<sup>388</sup> Pub. L. 106-102 (2000).

<sup>389</sup> See Section 502 of the Gramm-Leach-Bliley Act.

<sup>390</sup> James D. Zirin. “Patents in Cyberspace: Where Do You Draw the Line?” WORLD INTERNET L. REP. (BNA) (7/00).

<sup>391</sup> *PTO Notice of Roundtable Forum to Discuss Issues for Business Method Patents*; PATENT, TRADEMARK & COPYRIGHT J. (June 30, 2000), p. 199.

<sup>392</sup> *Id.* See also Sabra Chartrand, *Federal Agency Rethinks Internet Patents*, N.Y. TIMES, Mar. 30, 2000, at C-12.

<sup>393</sup> H.R. 1332 (Apr. 6, 2001), reported in 61 PATENT, TRADEMARK & COPYRIGHT J. 1519 (BNA), at 573 (Apr. 13, 2001).

<sup>394</sup> *Id.*

<sup>395</sup> *ABA Delegate Approve IP Resolutions On Business Methods, Madrid and Privilege*, 62 PATENT, TRADEMARK & COPYRIGHT J. 1536 (BNA) (Aug. 17, 2001), at 359.

<sup>396</sup> 149 F.3d 1368 (Fed. Cir. 1998).

the software merely presents and solves a mathematical algorithm. The court rejected the proposition – previously widely accepted – that software which merely embodied mathematical algorithms or represented business methods was not patentable subject-matter.

The software in *State Street Bank* involved “hub and spoke” mutual funds, and provided a method for allocating profits, losses and expenses to arrive at a share price for each fund. It has been suggested by some that under this decision, the inventors of such business methods as the credit card, airline reservation systems and frequent flyer programs could have patented them.

Several recent patents suggest the scope of patents that now are available:

- ◆ Priceline.com was issued a patent for its reverse-auction system of conditional offers to multiple sellers.<sup>397</sup>
- ◆ DoubleClick Inc. has received patents on basic methods of delivering advertising over the Internet.<sup>398</sup>
- ◆ Amazon.com obtained a patent on the ability to place an order online with a single mouse click once the item desired is displayed.<sup>399</sup>
- ◆ IBM obtained a patent, which it later renounced, on a “system and method for providing reservations for restroom use.”<sup>400</sup>

All but IBM have sued competitors to enforce their rights,<sup>401</sup> and Amazon.com obtained a temporary injunction barring its major competitor, Barnesandnoble.com, from providing single-click ordering on its site.<sup>402</sup>

Filings for such business methods patents appear to be burgeoning.<sup>403</sup> In light of this trend, it is important for businesses and their counsel to consider whether any business methods implemented through software, whether over the Internet or otherwise, might be subject to patent protection. Failure to do so risks not only the loss of a potential ability to exclude competitors or generate license income from them, but also runs the risk of being subject to infringement litigation by others who do obtain patents on a method and must then bear the burden and expense of establishing prior development.

Legislation has been introduced in Congress to place limitations on business methods patents. The “Business Methods Patents Improvement Act of 2000”<sup>404</sup> would have provided for publication of business methods patents by the Patent and Trademark Office within 18 months of

---

<sup>397</sup> U.S. Patent No. 5,794,207: Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers; U.S. Patent No. 5,897,620: Method and apparatus for the sale of airline-specified flight tickets (*available at* <http://www.patents.ibm.com>).

<sup>398</sup> U.S. Patent No. 5,933,811: System and method for delivering customized advertisements within interactive communication systems; U.S. Patent No. 5,937,392: Banner advertising display system and method with frequency of advertisement control (*available at* <http://www.patents.ibm.com>).

<sup>399</sup> U.S. Patent No. 5,960,411: Method and system for placing a purchase order via a communications network (*available at* <http://www.patents.ibm.com>).

<sup>400</sup> U.S. Patent No. 6,329,919: System and method of providing reservations for restroom use (*available at* <http://www.uspto.gov/paft/index.html>), reported in T. Wolverton, “IBM Flushes Restroom Patent, c|net news.com, <http://news.com/2100-1017-961803>.

<sup>401</sup> See 1 IP LAW WKLY. (AM. LAW. MEDIA) 623, 742 (1999).

<sup>402</sup> *Amazon.com v. Barnesandnoble.com Inc.*, 73 F. Supp. 2d 1228 (W.D. Wa. 1999).

<sup>403</sup> See J.R. Harris, “*The Silicon Rush: Staking Claims on the Internet Frontier*,” 4 CYBERSPACE LAW. (GLASSER) No. 2 at 11 (1999).

<sup>404</sup> H.R. 5364, 106th Cong. (2000).

filing, with an opportunity for third parties to oppose the granting of a patent. If a business methods patent is granted, it could be challenged in an administrative proceeding within nine months of issuance. In addition, the bill would have created a rebuttal presumption that a business method invention is obvious (and so not patentable) if the subject matter comes from combining or modifying prior art references and the only difference between those references and the claimed invention is computer implementation.

It is worth noting that the American approach permitting patents on business methods and software is far from universal. While the European Patent Office (“EPO”) favored allowing registration of software patents, the European Parliament overwhelmingly voted in July 2005 to veto a proposed directive that would have permitted software patents.<sup>405</sup> Australia accepts business process patents, but a report of the Australian Advisory Council on Intellectual Property has recommended in a 2004 report that the question be monitored closely.<sup>406</sup>

### III. *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.*,<sup>407</sup> 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. The *Stac* court did not appear to consider whether such reverse-engineering would have violated Microsoft’s copyright rights.

#### 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.<sup>408</sup> Such so-called “shrinkwrap licenses” received a significant boost from the Seventh Circuit in *ProCD, Inc. v. Zeidenberg*.<sup>409</sup> 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.*,<sup>410</sup> the Fifth Circuit held that shrinkwrap licenses were unenforceable, notwithstanding a state statute validating them. The statute, held the court,

---

<sup>405</sup> 70 PATENT, TRADEM & COPYR J. 331 (July 15, 2005).

<sup>406</sup> <http://www.acip.gov.au>.

<sup>407</sup> 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).

<sup>408</sup> 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).

<sup>409</sup> 86 F.3d 1447 (7th Cir. 1996).

<sup>410</sup> 847 F.2d 255 (5th Cir. 1988).

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*,<sup>411</sup> 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,"<sup>412</sup> 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.<sup>413</sup>

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)."<sup>414</sup>

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.

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.<sup>415</sup> 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.<sup>416</sup> 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

---

<sup>411</sup> 939 F.2d 91 (3d Cir. 1991).

<sup>412</sup> *Id.* at 104-105 n. 45.

<sup>413</sup> See also *Arizona Retail Systems, Inc. v. Software Link, Inc.*, 831 F. Supp. 759 (D. Ariz. 1993).

<sup>414</sup> *ProCD Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

<sup>415</sup> 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).

<sup>416</sup> Citing *Carnival Cruise Lines v. Shute*, 499 U.S. 595 (1991).

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.<sup>417</sup> 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.<sup>418</sup>

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 READ THE FOLLOWING AGREEMENT CLOSELY.”<sup>419</sup> 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.<sup>420</sup>

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.<sup>421</sup> And the Ninth Circuit has

---

<sup>417</sup> *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.”).

<sup>418</sup> 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 (9<sup>th</sup> 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>.

<sup>419</sup> *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. 268 (Jan. 25, 2002) available at <http://pub.bna.com/ptcj/0011489.pdf>.

<sup>420</sup> *Rudder v. Microsoft Corp.*, 2 C.P.R. 4(th) 474 (Ont. S.C.J. 1999).

<sup>421</sup> *Specht v. Netscape Communications Corp.*, 306 F. 3d 17 (2nd Cir. 2002). *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

held that a company cannot unilaterally change the terms of an agreement simply by posting changed terms online without notice to its customer.<sup>422</sup> 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 database repeatedly and therefore was effectively on notice of the terms of use, was bound by them.<sup>423</sup> The Central District of California reached a similar conclusion.<sup>424</sup> 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.<sup>425</sup> The Supreme Court of Canada upheld the enforceability of an arbitration change contained in an online agreement available on Dell's website via a hyperlink, finding such a link to be "reasonably accessible."<sup>426</sup>

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.<sup>427</sup>

The enforceability of clickwrap licenses remains subject to ordinary contract principles, such as unconscionability. Thus the Northern District of California refused to enforce an arbitration clause in a clickwrap agreement as unconscionable, describing the clause as an unenforceable, one-sided contract of adhesion.<sup>428</sup> Note that European consumer protection law may render unenforceable consumer contracts that are deemed to be unfair or imprecise. A

---

evidence showed defendants' knowledge thereof); *Net2Phone, Inc. v. Super. Ct. Los Angeles County*, No. B162210 (Cal.Ct.App.Dist. June 9, 2003), available at [www.courtinfo.ca.gov/opinions/documents/B162210.pdf](http://www.courtinfo.ca.gov/opinions/documents/B162210.pdf).

<sup>422</sup> *Douglas v. U.S. Dist. Ct. C.D. Cal. and TalkAmerica, Inc.*, 495 F.3d 1062 (9<sup>th</sup> Cir. 2007).

<sup>423</sup> *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>.

<sup>424</sup> *Ticketmaster L.L.C. v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (JWJx) (C.D. Cal. 2007).

<sup>425</sup> *Southwest Airlines Co. v. BoardFirst, L.L.C.*, Civ. Action No. 3:06-CV-0891-B (N.D. Tex. Sept. 12, 2007), available at <http://caseinfo/internet/southwest1.pdf>.

<sup>426</sup> *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>.

<sup>427</sup> 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://cyberpunks.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). See

<http://www.canlii.org/qc/juq/qccs/2003/2003qccs11838.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>.

<sup>428</sup> *Comb v. PayPal, Inc.*, 2002 WL 2002 171, 2002 U.S. Dist. LEXIS 16364 (N. D. Cal. 2002). The Court 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).

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.<sup>429</sup>

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.<sup>430</sup>

### 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,<sup>431</sup> 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 software acquired in violation of a license agreement,<sup>432</sup> while others have found such transactions to constitute sales notwithstanding agreements characterizing them as licenses.<sup>433</sup>

## IV. *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*,<sup>434</sup> 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.<sup>435</sup>

---

<sup>429</sup> *Union Fédérale des Consommateurs v. AOL France*, Court of First Instance of Nanterre (June 2004), available at [http://legalisnet/jurisprudence-decision.php3?id\\_article=1211](http://legalisnet/jurisprudence-decision.php3?id_article=1211) (in French); see discussion at [www.mofo.com/news/general.cfm?ID=1297&Type=5](http://www.mofo.com/news/general.cfm?ID=1297&Type=5).

<sup>430</sup> *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).

<sup>431</sup> 17 U.S.C. § 109(a).

<sup>432</sup> *Adobe Systems Inc. v. Stargate Software Inc.*, 216 F. Supp. 2d 1051 (N.D.C.A. 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).

<sup>433</sup> 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. Supp. 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).

<sup>434</sup> 911 F.2d 970 (4th Cir. 1990).

<sup>435</sup> 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).

Thereafter, the Fifth and Ninth Circuits adopted the copyright misuse defense in *Alcatel USA, Inc. v. DGI Technologies, Inc.*,<sup>436</sup> *DSC Communications Corp. v. DGI Technologies, Inc.*<sup>437</sup> and *Practice Management International Corp. v. American Medical Association*<sup>438</sup>.

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<sup>439</sup>.

*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*<sup>440</sup> was originally affirmed, but then reversed by the Second Circuit on rehearing, holding that the state 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.<sup>441</sup>

### V. *Computer Software Copyright Issues*

It is clear that software is copyrightable if it is original. The difficulty is in establishing the scope of copyright protection, since unlike the traditional kinds of works protected by copyright, software has a significant functional component. The challenge to the courts is to

---

<sup>436</sup> 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).

<sup>437</sup> 81 F.3d 597, 601-02 (5th Cir. 1996) (same).

<sup>438</sup> 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 Organizations Antitrust Litigation*, 964 F. Supp. 1469 (D. Kan. 1997); *Tamburg v. Calvin*, 1995 WL 121539 (N.D. Ill. 1995) (unpublished opinion).

<sup>439</sup> E.g., *Bellsouth Advertising & Publishing Corp. v. Donnelly Information Publishing, Inc.*, 933 F.2d 952 (11th Cir. 1991).

<sup>440</sup> 775 F. Supp. 544 (E.D.N.Y. 1991), *aff'd in part, vacated in part*, 982 F.2d 693 (2d Cir. 1992).

<sup>441</sup> 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).

limit protection to the expressive elements of the software, without protecting the utilization elements. The Supreme Court's failure to provide guidance on this question, in its equally divided affirmance without opinion in *Lotus Development Corp. v. Borland Int'l, Inc.*,<sup>442</sup> leaves an unsettled morass of conflicting Court of Appeals decisions. It is worth a brief historical excursion to see how we got to where we are, and review the differing views of the Circuits.

A. *Literal elements: Code.*

It is clear that the computer code itself is protectible. Congress amended the copyright law in 1980 to specifically include software. 17 U.S.C.A. § 101. Numerous Court of Appeals cases hold both source code and object code protectible, *see, e.g., Stern Electronics, Inc. v. Kaufman*, 669 F.2d 852, 855 n.3 (2d Cir. 1982 (source code)); *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1246-47 (3d Cir. 1983) (both); *Williams Electronics, Inc. v. Arctic International, Inc.*, 685 F.2d 870 (3d Cir. 1982) (object code), even where the code is embodied in a read-only memory (ROM) or other computer chip. *See, e.g., Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1249 (3d Cir. 1993); *Midway Mfg. Co. v. Strahon*, 564 F. Supp. 741, 749-52 (N.D. Ill. 1983); *Tandy Corp. v. Personal Micro Computers, Inc.*, 524 F. Supp. 171, 173 (N.D. Cal. 1981).

B. *Non-literal elements "User Interface" and "Look and Feel"*

The more difficult question is the extent to which the "look and feel" or "user interface" of a program are protected by copyright.

3. *Conventional View.* The conventional view, now largely abandoned, was that only the code itself is protected. Under that view, as long as one does not copy the code, one can clone the software. The subject matter of copyright had to be non-functional, so one could not protect the workings of the software, as opposed to the code.

4. *The Whelan View.* *Whelan v. Jaslow*<sup>443</sup> and *Broderbund Software Inc. v. Unison World*<sup>444</sup> held that copyright protects the "structure, sequence and organization" of software as well as the literal code. This view prevents the clean room "reverse-engineering" of software, in which a would-be cloner analyzes each step the software performs and has its programmers replicate it through different code. Since these decisions, the courts have been wrestling over the issue of what portions of software are copyrightable, and what portions are dictated by functionality and so not protectible. The issue is the extent to which how the program appears on the screen and how it works is part of copyright.

The *Whelan* view resulted from manufacturers' efforts to protect their programs' functionality, and holds that "look and feel" can be protected. Under this view the question becomes how the program controls the computer system in taking data, assembling and manipulating it and generating output in a useful form. The sequence of screens and how the users interact with the software become part of the copyrightable expression, rather than the unprotected idea.

The view is that programming is more than writing the code; rather, the creative process also involves developing the user interface, planning the program's organization and the sequence in which tasks are performed, and setting up the various file structures the software

---

<sup>442</sup> 516 U.S. 233, 116 S. Ct. 804 (1996).

<sup>443</sup> 797 F.2d 122 (3d Cir. 1986).

<sup>444</sup> 648 F. Supp. 1127 (N.D. Cal. 1986).

will use and create. Coding cannot begin until the detailed design is completed. The actual coding may be one of the smallest, least creative parts, as the *Whelan* court intimated.<sup>445</sup> A book or play can be infringed by copying plot elements without copying the literal text, said the *Whelan* court, so why not software?<sup>446</sup>

*Whelan* suggested that “The purpose or function of a utilitarian work would be the work’s idea, and everything that is not necessary to that purpose or idea would be part of the expression of the idea.” So long as there are varying means of achieving the purpose, the particular means chosen is protectible expression.<sup>447</sup> That seems too broad. It implies that a keyboard layout or “Q” for “quit” to exit the program are protectible. It also implies a regimen of “one idea per program” which seems too limited. It fails to address the problem of the merger doctrine that exists if there are only a limited number of rational ways to achieve a purpose — a few ways to express the idea — much like the concept of color preclusion in trade dress law. In such cases, copyright protection is not afforded, as it would provide a monopoly over the idea itself, rather than only the expression.<sup>448</sup> In addition the underlying purpose of *Whelan* — to protect the efforts of programmers — if divorced from considerations of the extent to which the fruits of those efforts are creative rather than functional, would appear at odds with the Supreme Court’s rejection of the “sweat of the brow” doctrine in *Feist Publications, Inc. v. Rural Telephone Service Co.*<sup>449</sup>

5. The *Altai* View. The leading case rejecting the *Whelan* view is *Computer Associates v. Altai*.<sup>450</sup> *Altai* rejected *Whelan* as providing overbroad protection. Instead, it establishes a three step process: Abstraction-Filtration-Comparison, designed to identify only the protectible elements, à la *Feist*. The first step is to break the program down into its constituent parts and, for each part, look at the various “levels of abstraction” from most particular to most general: code, parameter lists, flow charts, ultimate function or purpose. The next step, at each level of abstraction, is to filter out the unprotectible elements of the program: those which, under the merger doctrine, are inseparable from the underlying idea; those which are effectively “scenes a faire,” being dictated by efficiency or functionality or by external factors such as compatibility with hardware or with software it is to work with; and those in the public domain and so not original. The remainder is what is protectible, although care must be taken to determine whether the assemblage of elements may be protectible, just as a compilation of unprotectible facts is protectible if the selection and arrangement are original and minimally creative.<sup>451</sup> The final step is to compare that remainder to the allegedly infringing work to see if there is substantial similarity as to those elements, at each level.

In contrast to *Whelan*, in which everything other than the single underlying purpose is protected, *Altai* requires the elimination of all functional or otherwise unprotectible elements before determining what may be protected.

6. *Lotus v. Borland*. Most recently, in a dramatically different decision that calls into question the ability to protect the user interface of software under copyright, the First Circuit

---

<sup>445</sup> 797 F.2d at 1231.

<sup>446</sup> 797 F.2d at 1234.

<sup>447</sup> 797 F.2d at 1236.

<sup>448</sup> See *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1253 (3d Cir. 1983), cert. dismissed, 464 U.S. 1033 (1984).

<sup>449</sup> 111 S. Ct. 1282 (1991).

<sup>450</sup> 982 F. 2d 693 (2d Cir. 1992).

<sup>451</sup> *Feist Publications*, 111 S. Ct. at 1289.

reversed a district court decision in favor of Lotus Development Corp. against an alleged infringer. In an anticlimactic result, the decision was affirmed without opinion by an equally divided Supreme Court, providing no High Court precedent on the issue.<sup>452</sup> At issue was Borland's incorporation of the entire Lotus 1-2-3 menu structure as an alternative user interface in its Quattro and Quattro Pro spreadsheet programs. There was no dispute that the code, structure and appearance of the programs were different, apart from this use of the Lotus menu structure.

*The District Court Decision.* Before considering the First Circuit's decision, it is worth reviewing the district court opinion, which, together with related rulings, was, until the reversal, regularly cited favorably by other courts.<sup>453</sup>

*Lotus Development Corp. v. Borland Int'l, Inc.*<sup>454</sup> is interesting for its approach, which is somewhat more straightforward, if less rigorously analytical than *Altai*. Judge Keeton took a similar, but not identical, approach to *Altai*. He, too, examines the program from the most particular to the most general, not in terms of structure, but in terms of the formulation of the idea of the program, and finds the level at which idea stops and expression begins. Only then does he consider whether the expression of that idea is limited to elements essential to any expression of the idea. If not, so that there is protectible expression, he considers whether protectible expressive elements are a substantial part of the program.

Reviewing Judge Keeton's formulations of the idea behind the Lotus 1-2-3 program illustrates how this approach works:

“One may describe a number of conceptions of the 1-2-3 user interface. A non-exclusive list, commencing with the most abstract and moving toward the particular, includes:

1. Lotus 1-2-3 is an electronic spreadsheet.
2. It is a menu-driven electronic spreadsheet.
3. Its user interface involves a system of menus, each menu consisting of less than a dozen commands, arranged hierarchically, forming a tree in which the main menu is the root/trunk of the tree and submenus branch off from higher menus, each submenu being linked to a higher menu by operation of a command.
4. Its user interface involves a system of menus, each menu consisting of less than a dozen commands, arranged hierarchically, forming a tree in which the main menu is the root/trunk of the tree and submenus branch off from higher menus, each submenu being linked to a higher menu by operation of a command, so that all the specific spreadsheet operations available in Lotus 1-2-3 are accessible through the paths of the menu command hierarchy.

---

<sup>452</sup> *Lotus Development Corp. v. Borland Int'l, Inc.*, 49 F.3d 807 (1st Cir. 1995), *aff'd*, 516 U.S. 233, 116 S. Ct. 804 (1996).

<sup>453</sup> *See, e.g., Engineering Dynamics Inc. v. Structural Software Inc.*, 26 F.3d 1335 (5th Cir. 1994), *supplemented on pet. for rehearing*, 46 F.3d 408 (5th Cir. 1995); *Gates Rubber v. Bando American*, 9 F.3d 823 (10th Cir. 1993).

<sup>454</sup> 799 F. Supp. 203 (D. Mass. 1992), *rev'd*, 49 F.3d 807 (1st Cir.), *aff'd*, 516 U.S. 233, 116 S. Ct. 804 (1996).

5. Finally, one may conceive of the interface as that precise set of menu commands selected by Lotus, arranged hierarchically precisely as they appear in 1-2-3. Under this conception, the interface comprises the menu of commands ‘Worksheet,’ ‘Range,’ ‘Copy,’ ‘Move,’ ‘File,’ ‘Print,’ ‘Graph,’ ‘Data,’ ‘System,’ and ‘Quit,’ linked by operation of the command ‘Worksheet’ to the menu of commands ‘Global,’ ‘Insert,’ ‘Delete,’ ‘Column,’ ‘Erase,’ ‘Titles,’ ‘Windows,’ ‘Status,’ and ‘Page,’ etc. (The completion of this proposed statement of the ‘idea,’ listing all of the more than 400 commands for which ‘etc.’ stands, would require several dozen more lines of text.)<sup>455</sup>

Borland claimed the “idea” of 1-2-3 was at the final, fifth level, asserting that the idea was complete compatibility with earlier versions of the program and with macros written for such earlier versions. Judge Keeton rejected that extreme. He also rejected the other extreme, which *Whelan* supports, that the idea was simply “an electronic spreadsheet,” as too abstract. Rather, he concluded that the fourth choice set forth above was the appropriate definition of the “idea” of 1-2-3 interfaces. He concluded that the interface included non-essential expression because there were many ways to arrange the commands, even allowing for external factors, such as the frequency of use of each command. This conclusion was made easy by the fact that Borland’s software had a “native format” interface that was quite different from the Lotus interface available to users as an option. Some parts of the menu arrangements might have been required by external considerations such as frequency of use, and so not protected, but that was a jury question that affected only the scope of relief, not liability for infringement.

In sum, Judge Keeton held the Lotus 1-2-3 interface copyrightable, so long as there were sufficient alternative ways of accomplishing the same thing. Lotus could not protect the use of the “/” key to call up the menu screen, or “q” to quit, but a competitor could not copy the entire menu structure to create a clone.

Judge Keeton’s approach is less analytical than *Altai*, but it seems somewhat more accessible to judges, and, until the First Circuit’s reversal, appeared a harbinger of the direction other courts might go. Under that scenario, litigation would then turn on persuading the judge where the line between idea and expression falls — something no one has ever formulated clearly in the computer software context, or any other.

*The Court of Appeals Decision.* In reversing Judge Keeton, the First Circuit took a drastically different approach. Putting aside the difficult questions of identifying protectible expression, it instead addressed “the more fundamental question of whether a menu command hierarchy can be copyrighted at all.” 49 F.2d at 815. It then focused on the simplified — some might argue oversimplified — question of whether the menu structure constituted an unprotectible “method of operation” under § 102(b) of the Copyright Act. That section provides:

“In no case does copyright protection for a work of original authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the

---

<sup>455</sup> 799 F. Supp. at 216.

form in which it is described, explained, illustrated or embodied in such work.”<sup>456</sup>

Finding the 1-2-3 menu structure to provide “the means by which users control and operate” the software, the First Circuit held it to be an uncopyrightable “method of operation.”<sup>457</sup> It saw no difference between the menu structure and the buttons on a VCR.<sup>458</sup>

This approach takes a rather literal view of the words of § 102(b), treating it as a laundry list of “categories foreclosed from copyright protection,” even if the work in question consists of “original expression.”<sup>459</sup> The legislative history, however, shows that this section was not intended to enlarge or contract the scope of copyright protection, but merely “to restate . . . that the basic dichotomy between expression and idea remains unchanged.”<sup>460</sup> This suggests the need for an analysis to separate protectible expression from unprotectible idea or method of operation, which is essentially Judge Keeton’s approach, rather than the First Circuit’s view that a method of operation is *ipso facto* unprotectible, regardless of the original expression it may contain.

If the First Circuit is taken at its word — that a “method of operation” is “the means by which a person operates something, whether it be a car, a food processor, or a computer,”<sup>461</sup> and is unprotectible — then it is hard to see how any user interface could be protected. By definition, the user interface for a software program is the menu by which a person operates the software and, through it, the computer.

Indeed, some have argued that the protection under copyright of all elements of computer programs, and, indeed, of programs as a whole, are called into question by the First Circuit’s decision:

“A computer program, defined in the Copyright Act as ‘a set of instructions to be *used* directly or indirectly in a computer *in order to bring about a certain result*,’ is a means by which a person operates a computer. 17 U.S.C. § 101 (emphasis supplied [by amicus brief]). Virtually all elements of a program are means of operating some aspect of a computer. The First Circuit’s construction of Section 102(b) might well preclude protection for all such elements, even for the literal code of programs. . . . That result is clearly at odds with the statute, with the stated intent of Congress and with the weight of judicial authority in other circuits.”<sup>462</sup>

A narrower view of the First Circuit decision is espoused by Borland in opposing Lotus’ petition for certiorari:

“As the First Circuit made plain, this case is *not* about a computer program; it is about the menu words that are used as buttons and switches to operate the programs.”

---

<sup>456</sup> 17 U.S.C. § 102(b).

<sup>457</sup> 49 F.3d at 815.

<sup>458</sup> *Id.* at 817.

<sup>459</sup> *Id.* at 818.

<sup>460</sup> H.R. Rep. No. 1476, 94th Cong., 2d Sess. at 57, *reprinted in* 1976 U.S. Code Cong. & Admin. News at 5670.

<sup>461</sup> *Id.* at 815.

<sup>462</sup> Brief Amicus Curiae of Intellectual Property Owners in Support of Petitioner at 4, *Lotus Development Corp. v. Borland Int’l, Inc.*, No. 94-2003, 516 U.S. 233, 116 S. Ct. 804 (1996) [“*Lotus v. Borland* (Sup. Ct.)”]

Brief in Opposition to Petition for Certiorari [“Borland Opposition”], *Lotus v. Borland* (Sup. Ct.). Limited in this way, the First Circuit’s decision can be viewed as a policy argument in favor of permitting software developers to maintain compatibility with their predecessors. The First Circuit found it “absurd” that users of multiple programs would have to “learn how to perform the same operation in a different way for each program used,” or that 1-2-3 users who wrote macros employing the 1-2-3 menu hierarchy could not use their own work product in other programs.<sup>463</sup> Rather, it argued:

“ . . . in most contexts, there is no need to ‘build’ upon other people’s expression, for the ideas conveyed by that expression can be conveyed by someone else without copying the first author’s expression. In the context of methods of operation, however, ‘building’ requires the use of the precise method of operation already employed; otherwise ‘building’ would require dismantling, too. Original developers are not the only people entitled to build on the methods of operation they create; anyone can. Thus, Borland may build on the method of operation that Lotus designed and may use the Lotus menu command hierarchy in doing so.”<sup>464</sup>

The argument then can be put into competitive terms:

“ . . . while Lotus’ product initially became a success because it was technologically superior to its early competition, it later maintained its share because . . . the user’s investment in learning the method of operation of the Lotus product and the creation of macros ‘locked in’ those users who first selected Lotus over its early competition. Therefore, unless a new entrant with a superior product in the spreadsheet market could compete for the business of the vast majority of computer users who initially chose Lotus, competition would be limited solely to new spreadsheet users, a minor portion of the market.”<sup>465</sup>

The issue thus framed becomes one of balancing the constitutional policy to “promote the Progress of Science and the useful Arts, by securing for limited Times to Authors . . . the exclusive Right to their . . . writings,”<sup>466</sup> with the policy of fostering competition and permitting ready development of new software without sacrificing compatibility with prior programs urged by Borland and the First Circuit.

Arguably, however, the latter objective can be achieved by market principles. Software vendors who publicly grant permission to others to incorporate their user interfaces into other software, whether for free or for a reasonable royalty, may find readier acceptance of their products. Copyright owners who refuse to allow others to use their interface may find their products less accepted in the market by users who do not wish to have to learn multiple interfaces. Indeed, a significant factor in the success of the Microsoft Windows operating environment has been the fact that, with Microsoft’s blessing, most software written for that

---

<sup>463</sup> 49 F.3d at 817-18.

<sup>464</sup> *Id.* at 818.

<sup>465</sup> Borland Opposition at 10.

<sup>466</sup> U.S. CONST., art. I, § 8, cl. 8.

environment uses the same basic user interface, with the same menu structure for such common tasks as opening, saving and printing files.

With the failure of the Supreme Court, in its equally divided affirmance of *Lotus v. Borland*, to enunciate a clear rule to guide the courts and software developers with respect to the scope of copyright protection in software generally and user interfaces in particular, it remains to be seen in some future case whether the law will follow the trend of most courts other than the First Circuit to an “abstraction-filtration-comparison” type of analysis, impose the First Circuit’s “method of operation” inquiry as a first test, or take some other position entirely.

### 7. Other cases

(a) In *Mitel Inc. v. Iqtel Inc.*,<sup>467</sup> the Tenth Circuit rejected the First Circuit’s “method of operation” approach and used the *Altai* abstraction-filtration-comparison approach to deny protection to telephone call controller command codes (insufficiently original) and values (dictated by external factors such as hardware compatibility and industry practices and thus scènes à faire).

(b) In contrast, the Third Circuit held in *Dun & Bradstreet Software Services, Inc. v. Grace Consulting, Inc.*,<sup>468</sup> that interoperability with the infringed program was not an external factor justifying copying, and that interoperability must be viewed from the perspective of the infringed work, not of the infringing one.

(c) In *Engineering Dynamics Inc. v. Structural Software Inc.*,<sup>469</sup> the Fifth Circuit endorsed the *Altai* test as adopted in *Gates Rubber, infra*, and held input and output formats, taken as a whole, to be copyrightable in appropriate circumstances.

(d) In *Gates Rubber v. Bando American*,<sup>470</sup> the Tenth Circuit adopted the *Altai* test, but suggested first comparing for substantial similarity, and then filtering out unprotectible expression to see if what was protectible was copied. Comparing the entire work first may show a pattern of copying of unprotected elements that would be probative to show copying rather than independent creation.

(e) In *Autoskill, Inc. v. National Educational Support Systems, Inc.*,<sup>471</sup> the Tenth Circuit approved the district court’s use of the *Altai* test as a permissible method of analysis, although the description of the district court’s abstraction process seems closer to Judge Keeton’s approach than to that of the Second Circuit.

(f) The Ninth Circuit elaborated its analytical approach in *Apple Computer, Inc. v. Microsoft Corp.*<sup>472</sup> Like *Altai*, the Court required an “analytical dissection” of the allegedly infringing elements, to separate the protectible elements from the unprotectible.

---

<sup>467</sup> 124 F.3d 1366 (10th Cir. 1997), reported in 54 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 475 (1997).

<sup>468</sup> No. 00-2272 (3d Cir. Sept. 24, 2002) reported in 64 PATENT, TRADEMARK & COPYRIGHT J. 477 (Oct. 4, 2002).

<sup>469</sup> 26 F.3d 1335 (5th Cir. 1994), supplemented on pet. for rehearing, 46 F.3d 408 (5th Cir. 1995).

<sup>470</sup> 9 F.3d 823 (10th Cir. 1993).

<sup>471</sup> 994 F.2d 1476 (10th Cir. 1993).

<sup>472</sup> 35 F.3d 1435 (9th Cir. 1994), cert. denied, 513 U.S. 1184, 115 S. Ct. 1176 (1995).

In this case, the Ninth Circuit found virtually all the elements of Apple’s user interface to be unprotectible, as a result of having been licensed to Microsoft by Apple, or by applying the doctrines of merger (expression indistinguishable from the idea being expressed is unprotectible), scènes à faire (expression indispensable to, or at least standard in, the treatment of a given idea is unprotectible) and originality (only original components of a work are protectible).

While the Court noted that an original compilation of such unprotectible elements might still be protectible, it held that where virtually all the elements at issue were unprotectible, then the protection afforded to the overall compilation is “thin” and infringement will be found only if the infringing work is virtually identical. (Applying this test to the *Lotus v. Borland* situation, where the entire Lotus 1-2-3 menu tree was copied, arguably leads to a result contrary to that of the First Circuit, which held the 1-2-3 menu unprotectible.)<sup>473</sup>

(g) *ILOG Inc. v. Bell Logic LLC*,<sup>474</sup> held that added features developed as an add-on interface to the plaintiff’s software were improvements in methods of operation and so not copyrightable under *Lotus v. Borland*.

(h) *Productivity Software International, Inc. v. Healthcare Technologies, Inc.*<sup>475</sup> followed *Altai* and found no infringement because (i) no identified elements were protected by copyright and (ii) the arrangements of those elements, while entitled to narrow protection, were not substantially similar to the alleged infringing program.

(i) *MiTek Holdings Inc. v. Arce Engineering Inc.*<sup>476</sup> approved the *Altai* test, but held that the method the program follows to achieve its purpose, including the menus and submenu command tree structure, “is a process that is not entitled to copyright protection.” *Id.* at 1580.

(j) *CMAX/Cleveland v. UCR*.<sup>477</sup>

---

<sup>473</sup> See also *Softel Inc. v. Dragon Medical and Scientific Communications, Inc.*, 118 F.3d 955 (2d Cir. 1997) (compilation of unprotectible elements may be protectible, and works must be compared as a whole as well as in individual elements, *i.e.*, at different levels of abstraction); *Harbor Software, Inc. v. Applied Systems, Inc.*, 936 F. Supp. 167 (S.D.N.Y. 1996) (screen displays and reports protectible as compilations are not infringed if allegedly infringing work differs “by more than a trivial degree”).

<sup>474</sup> No. 01-10648-WGY (D. Mass. Jan. 9, 2002), reported in PATENT, TRADEMARK & COPYRIGHT J. (BNA) 266 (Jan. 25, 2002), available at <http://pub.bna.com/ptcj/0110648.pdf>.

<sup>475</sup> 93 Civ. 6949 (RPP), 1995 U.S. Dist. LEXIS 10381, 37 U.S.P.Q.2d (BNA) 1036, COPYRIGHT L. REP. (CCH) ¶ 27,440 (S.D.N.Y. 1995).

<sup>476</sup> 864 F. Supp. 1568 (S.D. Fla. 1994).

<sup>477</sup> 804 F. Supp. 337 (M.D. Ga. 1992) (following *Altai*).

## VI. *Reverse Engineering and Compatibility*

While modern copyright analysis eliminates the “clean-room” approach of reverse-engineering a complete work-alike, look-alike clone of a software package, reverse-engineering is still important, particularly to ensure compatibility with existing software and hardware. A question arises as to whether one can engage in reverse engineering software without necessarily infringing its copyright, for a necessary step to the process is loading the software into memory, which arguably creates an infringing copy; the copyright law allows copying only for archival purposes or as a necessary step in *running* — as opposed to analyzing — the program.

Several cases had held that making such an ephemeral intermediate copy in memory does indeed constitute infringement.<sup>478</sup> The Ninth Circuit has found such intermediate copies to be fair use, however, at least where the final product is non-infringing.<sup>479</sup> Again lurking in these cases is the question of how far the copyright monopoly should extend, or needs to extend, to provide the constitutionally intended incentive to development.

Section 302 of the Digital Millennium Copyright Act,<sup>480</sup> enacted in October 1998, reversed these decisions in the service and maintenance context, providing that the owner or lessee of a machine does not infringe a program by making or authorizing a copy of the program through activating the machine that lawfully contains an authorized copy, for purposes of maintenance or repair of the machine, so long as the new copy is not used for any other purpose and is immediately destroyed after the maintenance or repair is completed. The term “maintenance” has been construed to have a longer-term connotation, permitting the copy to be retained for so long as monitoring for problems continues.<sup>481</sup>

Of course, this statute does not apply to other copies of software made in memory, as for the purpose of reverse-engineering.

Reverse engineering of software may violate not only the exclusive right of the copyright holder to copy, but also its exclusive right to create derivative works. Relevant to the issue is the Semi-conductor Chip Protection Act, passed after the 1980 amendments to the Copyright Act that made clear that software was protected by copyright, which established a *sui generis* protection scheme for chips. That Act provided for a right to reverse engineer, and suggests that this explicit right was needed because existing fair use principles would not permit reverse-engineering.<sup>482</sup>

The question of whether the copies made of a work in the reverse-engineering process are actionable infringement has an analogy in *Walt Disney Co. v. Filmation*,<sup>483</sup> where intermediate

---

<sup>478</sup> See *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033, 114 S.Ct. 671 (1994) (loading operating system software into memory on startup of computer by third party maintenance provider in violation of license agreement was copyright infringement — fair use not discussed); *Advanced Computer Services of Michigan Inc. v. MAI Systems Corp.*, 845 F. Supp. 356 (E.D. Va. 1994) (loading software in memory creates a copy fixed in tangible medium and so infringes).

<sup>479</sup> See *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir.), *cert. denied*, 2000 U.S. LEXIS 5843, 148 L. Ed. 2d 118 (2000), discussed below.

<sup>480</sup> H.R. 2281, Pub. L. No. 105-304, 15 U.S.C. § 1201 *et seq.*

<sup>481</sup> *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, No. 04 1462 (Fed. Cir. August 24, 2005), reported in PAT. TRADEMARK & COPYR. J. (BNA) 500 (Sept. 2, 2005) available at <http://pub.bna.com/ptcj/041462Aug24.pdf>.

<sup>482</sup> See A.R. Miller, *Copyright Protection for Computer Programs, Databases and Computer-Generated Works: Is Anything New Since CONTU?*, 106 HARV. L. REV. 977, 1023-24 (1993).

<sup>483</sup> 628 F. Supp. 871 (C.D. Cal. 1986).

production materials copied from Disney’s “Pinocchio” were held to infringe, regardless of whether they were ultimately used to make an infringing film. If the intermediate step constitutes infringement, then the lack of substantial similarity in the final product is not necessarily dispositive of whether there is infringement. More recently, a federal court held that the scanning of a copyrighted photograph in preparation for graphically manipulating it into a new work constituted infringement, regardless of the similarity of the ultimate new work to the original.<sup>484</sup>

Several cases address this issue in the reverse-engineering context.

A. *SEGA v. Accolade*<sup>485</sup> held that the reverse engineering of a security system on video games to allow them to run on a SEGA Genesis system was fair use. The Ninth Circuit held the copying to be a necessary step in determining the security code, which was held to be a functional element of the software and not protected. The opinion contains some very questionable economic assumptions about the market: because a typical user buys more than one video game to play on his console, the Court said there is no adverse impact on the sale of SEGA games, so that fair use factor did not favor SEGA. This analysis gives rather short shrift to the fourth and critical fair use factor of adverse impact on the economic value of the infringed work. The Court concluded that, in such cases, where reverse-engineering is the only way to gain access to the ideas and functional elements — the unprotectible parts — of a copyrighted work, and where there is a legitimate reason for such access, such reverse-engineering is fair use. At a minimum, however, fair use should be limited to products which complement, rather than substitute for, the infringed work.

B. *Atari Games Corp. v. Nintendo of America, Inc.*<sup>486</sup> said that so long as a competitor does only what is necessary to understand the unprotected elements of a software program, it constitutes fair use. But the Federal Circuit found the Nintendo security lock at issue to be protected, unlike the SEGA lock held by the Ninth Circuit to be functional, and affirmed a preliminary injunction against Atari. The Ninth Circuit later amended its opinion in *SEGA* to reconcile the two decisions, saying that the Nintendo key was an original program to generate a data key to unlock the console, and there were many ways to generate such a key. In contrast, the SEGA code was simply the letters S-E-G-A at a specific location, with only one way to unlock the console, and thus was purely functional and not protected. Another aspect of the *Atari v. Nintendo* case, which appeared to affect the result, is that Atari had falsely represented to the copyright office that it needed Nintendo’s source code for purposes of pending litigation, and had then used that source code to reverse-engineer the console lock.

In further proceedings, the district court in *Atari* approved the copying of the non-copyrightable data stream “key”, but rejected the copying of the program code to generate that key as infringement, because it was done to ensure *future*, as opposed to present, compatibility, and so exceeded fair use.<sup>487</sup>

---

<sup>484</sup> *Tiffany Design Inc. v. Reno-Tahoe Specialty Inc.* No. CV-S-98-1207-PMP (D. Nev. July 12, 1999), reported in 58 PATENT, TRADEMARK & COPYRIGHT J. (BNA) 380 (1999).

<sup>485</sup> 977 F.2d 1510 (9th Cir. 1993).

<sup>486</sup> 975 F.2d 832 (Fed. Cir. 1992).

<sup>487</sup> *Atari Games Corp. v. Nintendo of America, Inc.*, Nos. C 88-4805 and C 89-0027, 1993 U.S. Dist. LEXIS 8183 (FMS) (N.D. Cal. 4/15/93) (also finding patent infringement by Atari), and 1993 U.S. Dist. LEXIS 6786 (N.D. Cal. 5/17/93).

C. In *Sony Computer Entertainment, Inc. v. Connectix Corp.*,<sup>488</sup> the Court held that the creation of an unauthorized intermediate copy of software in computer memory for the purpose of developing software to emulate the Sony PlayStation on a personal computer was infringing, even where the final product contained no infringing material, without the need to engage in the abstraction-filtration-comparison of *Computer Associates v. Altai*, *supra*. The Court found no fair use, distinguishing *Sega v. Accolade*, *supra*, on the ground that there, Accolade was developing its own games to operate on the Sega console, while here the emulation software would have been a substitute product for the PlayStation console. The Ninth Circuit reversed, relying on *SEGA v. Accolade*, stating that: “The intermediate copies made and used by Connectix during the course of its reverse engineering of the Sony BIOS were protected fair use, necessary to permit Connectix to make its non-infringing Virtual Game Station function with PlayStation games. Any other intermediate copies made by Connectix do not support injunctive relief, even if those copies were infringing.”<sup>489</sup> It found the intermediate copies necessary for Connectix to gain access to the unprotected functional elements of the Sony BIOS. As in *SEGA*, the Ninth Circuit’s conclusions about the extent to which the Connectix emulator would supplant the market for PlayStations are open to question.

D. In *Brooktree Corp. v. Advanced Micro Devices*,<sup>490</sup> fair use was not found because the defendant was found to have copied more than was essential for compatibility. The Federal Circuit’s approach seems to require that the copying be necessary to determine an unprotected element, to be for purposes of ensuring compatibility, and to be limited to copying only what is essential for that purpose. *DSC Communications Corp. v. DGI Technologies, Inc.*,<sup>491</sup> followed the Ninth Circuit *SEGA* decision in upholding a defense of fair use in the disassembly and reverse engineering of firmware. The court found that “when good reason exists for studying the unprotected aspects of a copyrighted program, disassembly for the purpose of study or examination of the disassembled program constitutes fair use.” The copying here was intermediate and for the purpose of making a compatible microprocessor card, which did not perform the same functions as the original, and so, the court said, would not interfere with its marketability. The court rejected the fair use defense, however, for the copying of operating system software the infringer had performed without the knowledge, and in violation of the license agreement of, a mutual customer. Fair use was available as a defense, said the court, only to the possessor of an authorized copy of the copyrighted work. The Fifth Circuit affirmed the limited grant of a preliminary injunction because use of license restrictions on copyrighted software “to obtain a patent-like monopoly over unpatented microprocessor cards” might well constitute copyright misuse under *Lasercomb America, Inc. v. Reynolds*,<sup>492</sup> discussed in Section IV of this paper.

F. *Lotus Development Corp. v. Borland Int’l, Inc.*<sup>493</sup> held that a feature of Borland’s Quattro Pro spreadsheet, which allowed it to read and execute macros written for Lotus 1-2-3, infringed Lotus copyrights by copying the 1-2-3 menu structure into a program file. That

---

<sup>488</sup> 48 F. Supp. 2d 1212 (N.D. Cal. 1999), *rev’d*, 203 F. 3d 596 (9th Cir.), *cert. denied*, 2000 U.S. LEXIS 5843, 148 L. Ed. 2d 118 (2000).

<sup>489</sup> 203 F. 3d at 599.

<sup>490</sup> 977 F.2d 1555 (Fed. Cir. 1992).

<sup>491</sup> 898 F. Supp. 1183 (N.D. Tex. 1995), *aff’d*, 81 F.3d 597 (5th Cir. 1996).

<sup>492</sup> 911 F.2d 970 (4th Cir. 1990).

<sup>493</sup> 831 F. Supp. 223 (D. Mass. 1993), *rev’d*, 49 F.3d 807 (1st Cir. 1995), *aff’d*, 516 U.S. 233, 116 S. Ct. 804 (1996).

copying was infringement, even if it was the only way to ensure macro compatibility. It was not fair use, because (i) it had a commercial purpose, (ii) the copying of the menu tree was identical, and (iii) it was likely to harm the market for 1-2-3. *Id.* at 240-45. (The First Circuit, in reversing, held the menu structure to be not protectible, and so did not address the fair use question.)

The district court's conclusion as to fair use seems a better reasoned application of traditional fair use analysis than the analysis in *SEGA*, and shows the serious obstacle posed by the crucial adverse economic impact factor used in fair use analysis. Competing programs will almost always be excluded by that analysis, and even add-in software must overcome the argument that the originator might enter the market.

Judge Keeton did distinguish a one-time translation of a 1-2-3 macro into a different macro language, which then could be run by Quattro Pro, from the continuous "on-the-fly" translation actually used, which requires ongoing reference to the 1-2-3 menu tree in the program file. He declined to reach the question raised by the first situation. That distinction seems to be without a legal difference, since both require use of a copy of the 1-2-3 menu structure and the only difference would seem to be how often that copy is referred to, which should not be determinative of whether there was infringement. The decision may, however, have been driven substantially by the facts, in which the program file at issue was essentially a direct replication of the Lotus menu tree. A less direct translation approach might have yielded a different result.

The *Lotus* district court's fair use analysis raises serious policy questions for publishers and consumers seeking to ensure that new software is operationally compatible with older programs. This analysis provides a great advantage to the company that is first to market and succeeds in establishing a large installed user base, since it prevents customers from switching software without losing their investment in custom-tailoring the program to their use by means of macros or otherwise. That advantage is not insuperable, however, as Lotus' declining market share demonstrates, and, of course, will disappear entirely if the First Circuit's exclusion of menu structures from the scope of copyright protection is upheld and applied to user interfaces generally.

The Digital Millennium Copyright Act<sup>494</sup>, enacted in October 1998, addresses but does not entirely resolve these issues. The Act prohibits circumvention of technological measures such as copy-protection and encryption that control access to a copyrighted work,<sup>495</sup> and the Librarian of Congress is to determine periodically whether users of a particular class of works are likely to be adversely affected by the non-circumvention provisions in their ability to make non-infringing copies of the class of works. If so, the prohibition does not apply to such users. In addition, the non-circumvention provisions do not apply to circumvention for purpose of reverse-engineering that is necessary to achieve interoperability of an independently created program, to the extent that the reverse-engineering does not constitute infringement. Thus, we are returned to the case law to determine whether the acts of reverse-engineering constitute fair

---

<sup>494</sup> H.R. 2281, Pub. L. No. 105-304, 17 U.S.C. §§ 1201 *et seq.*

<sup>495</sup> *See Universal City Studios Inc. v. Corley*, 273 F.3d 429 (2d Cir. Nov. 28, 2001) (holding defendants' posting of program to unscramble encrypted films in DVD format on their website violated the Digital Millennium Copyright Act); *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, 111 F. Supp. 2d 346, 2004 WL 1497688 (D.Mass. July 2, 2004); *Felten v. Recording Industry Ass'n of America*, No. CV-01-2669 (D. N.J. Nov. 27, 2001) (holding the Digital Millennium Copyright Act does not violate professor's First Amendment rights to publish research regarding weaknesses in a copy-right protection technology) *reported in* WORLD INTERNET L. REP. (BNA) (Jan. 2002), at 25.

use or are otherwise not infringing.<sup>496</sup> Note that interoperability is defined as the ability of programs to exchange information and use it, and thus would not appear to cover the development of substitute programs, as discussed in paragraph III.A. above.

The anti-circumvention provision was limited by the Sixth Circuit in its scope to restrictions on access to a copyrighted work itself, but not to the circumvention of lockout software that restricts use of a device without restricting access to the copyrighted work in *Lexmark Int'l Inc. v. Static Control Components, Inc.*<sup>497</sup> where the Court permitted a maker of replacement toner cartridges to circumvent a lockout program that prevented use of the printer except by cartridges made by the manufacturer. The Eighth Circuit has distinguished *Lexmark*, applying the DMCA to prohibit the circumvention of an authentication code required to access a video game, because the security code was not readily accessible to purchasers of the video game, as the *Lexmark* code was.<sup>498</sup> And a federal district court has held that an embedded description of license terms for fonts was not a technological measure protected from circumvention where the fonts were not encrypted or otherwise protected from unauthorized access.<sup>499</sup> Nor is the unauthorized use of a user name and password a circumvention under the DMCA.<sup>500</sup>

*Foreign Treatment.* The European Community permits decompilation where necessary to achieve the interoperability of an independently created program with the program being decompiled.<sup>501</sup>

---

<sup>496</sup> See *DVD Copy Control Ass'n v. Bunner*, 93 Cal. App. 4th 648 (Nov. 1, 2001) (holding that prohibition of future disclosures of computer program which unscrambled encrypted DVDs was an impermissible prior restraint on website operator's First Amendment right to publish program).

<sup>497</sup> 387 F.3d 522 (6th Cir. 2004).

<sup>498</sup> *Davidson & Assoc. d/b/a Blizzard Entertainment Inc. v. Jung*, 422 F. 3d 630 (8<sup>th</sup> Cir. 2005), reported in 70 PATENT, TRADEMARK & COPYRIGHT J. 524 (Sept. 16, 2005) available at <http://pub.bna.com/ptcj/043654Sept1.pdf>.

<sup>499</sup> *Agfa Monotype Corp. v. Adobe Systems Inc.*, 2005 WL 3430869 (N.D. Ill. Jan. 13, 2005), (N.D.Ill. 2005) available at <http://pub.bna.com/ptcj/026320Jan13.pdf>.

<sup>500</sup> *Engilman v. Keller & Heckman, LLP*, 2005 WL 3077260 (D.D.C. Nov. 10, 2005), available at <http://pub.bna.com/ptcj/0400876Nov10.pdf>.

<sup>501</sup> EC Directive on the Legal Protection of Computer Programs, Article 6.