E-Business:

The E-Business Legal Survival Kit

J.T. Westermeier
Lee J. Plave

Piper Rudnick LLP
1200 Nineteenth Street, N.W.
Washington, D.C. 20036-2430
Phone: (202) 861-3900
Fax: (202) 223-2085

1775 Wiehle Avenue, Suite 400
Reston, Virginia 20190-5159
Phone: (202) 773-4000
Fax: (202) 773-5000

http://www.piperrudnick.com

Piper Rudnick

© 2004 Piper Rudnick LLP. All Rights Reserved.

TABLE OF CONTENTS

Section	Page
Foreword	1
Introduction	2
What Makes E-Commerce Different	8
Jurisdiction	10
Franchise And Distribution Arrangements	16
Domain Names And Cybersquatting	24
Critical Websites Or Cybersmearing	35
Intellectual Property	39
Linking	44
Framing	47
Meta-Tags	50
Privacy	54
Agreements For E-Business Relationships	60
Web Crawlers, Spiders And Bots	63
Competition Issues	66
Electronic Agreements	71
Website Terms Of Use	75
Disclaimers	78
Consumer Laws	79
Direct Sale Regulations	81
Warranty Disclosures And Disclaimers	83
Acceptance Of Credit Cards	84
Liability For Acts Of Hackers	86
Spyware	88
Internet Usage Policy	90
Cyber Security	92
Anonymity	95
Export Controls	98
Trust And Confidence	99
Digital Signatures	101
Advertising Law	102
Sweepstakes And Promotions	107
Unsolicited E-Mail (Spam)	110
First Amendment	116
Special Applications	118
Insurance	120
Securities Law	121
Taxes	122
Customs Duties And Foreign Taxes	126
E-Commerce Outsourcing	127
Tort Liability	130
Criminal Liability	132
Americans With Disabilities Act Compliance	135
Appendix	137
About The Authors:	139

September 2004 (4094906.v10)

© 2004 Piper Rudnick LLP. All Rights Reserved.

INDEX

Section	Page
Acceptance Of Credit Cards	84
Advertising Law	102
Agreements For E-Business Relationships	60
Americans With Disabilities Act Compliance	135
Anonymity	95
Competition Issues	66
Consumer Laws	79
Criminal Liability	132
Critical Websites Or Cybersmearing	35
Customs Duties And Foreign Taxes	126
Cyber Security	92
Digital Signatures	101
Direct Sale Regulations	81
Disclaimers	78
Domain Names And Cybersquatting	24
E-Commerce Outsourcing	127
Electronic Agreements	71
Export Controls	98
First Amendment	116
Framing	47
Franchise And Distribution Arrangements	16
Insurance	120
Intellectual Property	39
Internet Usage Policy	90
Jurisdiction	10
Liability For Acts Of Hackers	86
Linking	44
Meta-Tags	50
Privacy	54
Securities Law	121
Special Applications	118
Spyware	88
Sweepstakes And Promotions	107
Taxes	122
Tort Liability	130
Trust And Confidence	99
Unsolicited E-Mail (Spam)	110
Warranty Disclosures And Disclaimers	83
Web Crawlers, Spiders And Bots	63
Website Terms Of Use	75
What Makes E-Commerce Different	8

© 2004 Piper Rudnick LLP. All Rights Reserved.

FOREWORD

These materials address the best practices, key legal strategies and current developments applicable to the fast-developing law relating to e-business.

Many of the current legal issues and developments applicable to e-business are described in these materials. The descriptions are not exhaustive. The internet has become a mainstream information resource and a medium of commerce and advertising. E-business is merely a form or procedure for conducting business transactions. E-business allows parties to buy products and services using the internet. It is a broad grouping of activities that allows products and services to be selected, purchased, received or serviced using electronic based technologies. All laws apply to e-business just like they apply to other forms of business activity. However, e-business applications have greater legal exposure than most brick and mortar business applications because they may be used by anyone anywhere in the world with internet access, twenty-four hours a day seven days a week.

These materials are designed to assist in identifying and avoiding legal problems in connection with an e-business application. The issues described in these materials focus on some of the legal issues that are more specific to e-business applications. These materials seek to provide legal risk management strategies and best practices that will be of particular help in connection with planning, setting up and operating e-business applications.

E-business uses the new family of technologies available on the internet. These technologies enable people to communicate in new ways, provide new business models, permit businesses to operate more efficiently and take advantage of the new global network economy.

INTRODUCTION

In May 1897, Mark Twain wrote that "[t]he report of my death was an exaggeration."[1] Over a century later, it seems that the same words can be said about reports of the demise of the internet in general, and e-business in particular. Indeed, the growth and expansion of the internet as a means for conducting business has indelibly marked the dawn of the 21st Century.

Today e-business[2] has emerged as a mainstream way to facilitate business transactions around the world. Even with the world's economy in a downturn and digesting the impact of the September 11, 2001 attacks on the United States, e-business has continued to grow. Forrester Research predicts that in 2004, North America will realize $3.5 trillion in e-commerce transactions, while the Asia-Pacific will realize $1.6 trillion, and Europe will realize $1.5 trillion.[3] During 2003, online spending in the United States, excluding travel and auctions, is reported to have exceeded $54.9 billion, and accounted for 1.5-2.0% of all sales.[4] This record total was propelled by online spending during the holiday season.[5] While Internet sales account

---

1 A copy of Twain's hand-written, and yet often misquoted and famous remark, can be found at *http://www.twainquotes.com/Death.html*.

2 The definition of e-business is broad, and encompasses e-commerce and all means by which people transact with one another over the internet. Among the variations are: (1) business-to-business e-commerce (B2B), involving the sale of goods and services by one business to another; (2) business-to-consumer e-commerce (B2C), involving the sale of goods and services by one business to consumers; (3) business-to-government e-commerce (B2G), involving the sale of goods and services by businesses to government agencies; (4) government-to-consumer (G2C), principally involving the provision of services to citizens; (5) peer-to-peer e-commerce (P2P), such as the much-vilified *Napster*, involving one person's provision of a good or service (such as a file containing an electronic copy of a song) to another person; (6) consumer-to-consumer e-commerce (C2C), such as consumer auctions on eBay's website; (7) exchange-to-exchange e-commerce (E2E), in which one industry-wide exchange transacts with another industry-wide exchange; and (8) mobile commerce (mCommerce), which is a variation on the other methods, and involves small wireless devices, such as the *DoCoMo* internet-enabled wireless telephones that are widely used in Japan.

3 eCommerce Statistics, ePaynews.com, http://www.epaynews.com/statistics/.

4 Michael Lear-Olimpi, *First Quarter E-Commerce Spending is Biggest Year-Start Ever*, 21 e-Commerce Law & Strategy 2, June 2004, at 1, 4 (reporting that first quarter 2004 online sales were $15.5 billion, accounting for 1.9% of all retail sales, a pace that was consistent with the level of purchasing during the holiday season in 2003; s*ee also A Perfect Market*, The Economist, May 15, 2004, at *Survey of E-Commerce* 3 (reporting that online retail sales in 2003 rose to $55 billion, noting that figure amounted to 1.6% of total retail sales for the year).

5 *Id.*

© 2004 Piper Rudnick LLP. All Rights Reserved.

for less than five percent of overall retail sales in the United States,[6] e business has already become a mainstream activity, as nearly one-third of U.S. adults reportedly shop online.[7]

The pervasive growth of broadband connections to the Internet is fueling new generations of development in terms of how content is displayed, delivered (e.g., streaming audio and video), how people use the web (*e.g.*, remote educational opportunities), and even how they converse (*e.g.*, videoconferencing and telephony using voice-over-internet-protocol (VoIP)). In an editor's note discussing a wide-ranging article on broadband, the editor of PC Magazine observed that "[o]ur surveys indicate that most of our readers have had broadband for some time now, and it's quickly becoming the mainstream method of connection to the Internet for large numbers of Americans."[8] Indeed, the article itself took note of a Nielsen survey reporting that 45% of U.S. households with Internet access (or approximately a third of all U.S. households) and 75% of the readers of PC Magazine had a broadband connection.[9] The result:

> Just five years ago, downloading an image or small sound file could bring your browsing to a sudden halt. But today, armed with a broadband connection, you can get immediate access to new music, blockbuster movies, and popular games without leaving the house. You can call friends in another state without paying for long distance, chat face-to-face with your family using videoconferencing software, and enter fantasy worlds with strangers from around the globe. You can even keep an eye on your house and use your home PC from hundreds of miles away. Plus, broadband isn't just for PCs anymore. We're seeing a growing number of devices – phones, cameras, and even a boom box – that tap right into your high-speed connection."[10]

And, of course, the possibility of combining 21st Century household appliances – like a digital video recorder – with the internet is more likely than ever before due to broadband connections.[11]

---

[6] *Id.*

[7] *Shoppers are Beating a Path to the web*, Bus. Week (Dec. 14, 2001) (BWonline, at *http://www.businessweek.com*). *See also* Bob Tedeschi, *E-Commerce Report*, The New York Times, Dec. 30, 2002 at C5 (sale of online gift certificates up by 64% over 2001, to $250 million).

[8] M. Miller, *Forward Thinking*, PC Magazine, Sept. 21, 2004, at 5.

[9] M. Graven, *The Broadband Lifestyle*, PC Magazine, Sept. 21, 2004, at 105.

[10] *Id.*

[11] For example, there have been reports of a possible collaboration between TiVo and Netflix, by which Netflix would deliver movies over a broadband connection to a customer's TiVo digital video recorder. *See* S. Olsen,

(footnote continued to next page)

© 2004 Piper Rudnick LLP. All Rights Reserved.

However, as good as it is, there are concerns that the growth of broadband in the U.S. is not as vigorous as it could be. A Business Week article observes that, when it comes to broadband, "[t]he U.S. has steadily fallen behind other nations, both in terms of the share of the population with broadband and the speed of those connections. Consider this: In 2000 the U.S. ranked third in broadband penetration among the nations in the Organization for Economic Cooperation & Development. Last year it dropped to 10th place. That's behind recognized leaders such as Japan and Korea, as well as countries like Belgium and Canada."[12] The author contrasted connections in Japan that are available at 100-megabit-per-second while in the U.S., high-speed links to the internet are typically in the range of 1.5-megabits-per-second.

By all accounts the growth of e-business promises to continue its explosive growth, even though the accelerated pace appears to be slowing.[13] Internet usage is now doubling every year rather than every 100 days the way it was in 2000.[14] But while the internet is prevalent and growing in the U.S.,[15] the expansion of the internet is most profound outside North America. In 2001, there were 513 million internet users worldwide, of whom 181 million are in North America (35%), 155 million in Europe (30%), 144 million in Asia and the Pacific (28%), 11

(footnote continued from previous page)

Picture imperfect for Netflix, TiVo, NYTimes.com, Sept. 8, 2004 (available at *http://www.nytimes.com/cnet/CNET_2100-1038_3-5357336.html*), and C. Schreiber, *Small-Stock Focus*, The Wall St. J., Sept. 8, 2004, at C4. Indeed, concern over this possibility has led at least two industry groups – the Motion Picture Association of America (MPAA) and its international counterpart, the Motion Picture Association (MPA) – to seek legislation protecting the works created by the motion picture industry. *See generally* the Anti-Piracy portion of the MPAA website, which is available at *http://www.mpaa.org/anti-piracy/index.htm*.

[12] *See* Catherine Yang, *Behind In Broadband, New policies are needed to help the U.S. catch up*, Bus. Week, Sept. 6, 2004.

[13] Hoffman, Keedy, and Roberts, *The unexpected return of B2B*, The McKinsey Quarterly, 2002 Number 3 (Oct. 2002); Tompkins, *Streamline Purchasing: E-Procurement Reduces Costs, Speeds Transactions, and Increases Supply-Chain Visibility*, IQ Magazine, March/April 2002, at 33. At the end of 1998, e-commerce was responsible for $50 billion and by 2003 was projected to reach $1.3 trillion. R. Comerford, *Technology 2000 Analysis & Forecast: The Internet*, IEEE Spectrum, Jan. 2000, at 40, 44. In the Internet Use article the annual growth rate for Internet usage in the United States slowed from 35% in 2000 to 15% in 2001. *See also* Bob Tedeschi, *The Net's Real Business Happens .Com to .Com, A Market That Dwarfs Retail E-Sales*, The New York Times, Apr. 19, 1999, at C3.

[14] Andy Grove, *We Can't Even Glimpse The Potential*, Bus. Week, Aug. 25, 2003, at 86 ("Andy Grove").

[15] The web is ubiquitous in the U.S. with nearly 75% of all U.S. homes having web access. "Home Access To Web Rises To Nearly 75% In The U.S.", *The Wall Street Journal*, March 18, 2004 at B5. Indeed, a survey reported that approximately 60% of those surveyed in a Pew study reported using the Internet regularly, and 80% of them *expect* to find reliable information online concerning news, health care, and government services. *Survey Cites Use of Internet to Gather Data*, The New York Times, Dec. 30, 2002, at C5.

© 2004 Piper Rudnick LLP. All Rights Reserved.

million in Latin America (2%), 5 million in Africa (1%), and 4 million in the Middle East (1%).[16] The State of the Internet 2001 report cites an estimate that by 2005, nearly 1.0 billion people will be online (of whom not more than a quarter would, or could, be in the U.S.), which would mark a 70% growth rate for the internet.[17] Another report suggests that by 2004, 60% of the overall European population will be using the internet.[18] Today, China has 80 million Internet users, second only to the U.S., but by 2006, China is expected to have 153 million Net users and bypass the U.S.[19] In the U.S. and Canada, women slightly outnumber men among web users.[20] In eleven countries, the Internet penetration rate has already exceeded one-half of the population: Austria, Canada, Denmark, Finland, Hong Kong, Japan, the Netherlands, Singapore, Sweden, Taiwan, and the United States.[21]

Not surprisingly, the internationalization of the web also shows up in the languages being spoken online. The majority of internet users are now non-English speakers. While English speakers remain, by far, the most prevalent group on the web (45% of web users, down from 51.3% in 2000), Japanese (9.8%), Chinese (8.4%), German (6.2%), Spanish (5.4%), and Korean (4.7%) speakers follow behind.[22]

Web and internet electronic business technologies promise to transform every aspect of the way companies conduct business and compete. The internet has created this business opportunity; in fact, it has fundamentally changed the economics of business transactions[23] and

---

[16] United States Internet Council and Int'l Tech. & Trade Associates, Inc., *State of the Internet* (2001 ed.) at 12 (Nov. 2001) (cited herein as "State of Internet").

[17] State of the Internet at 12-13.

[18] Angela Hall, 60% of European population may use internet by 2004, EuropeMedia.net, May 2, 2001 (available at *http*://www.*europemedia.net/shownews.asp?ArticleID=3050*).

[19] *China's Great March Online*, Bus. Week, July 12, 2004, at 14.

[20] In fact, during the 2001 holiday shopping season, 58% of online buyers were female. Dina ElBoghdady, *Women Take Lead in Web Shopping*, The Washington Post, Jan. 2, 2002, at D11.

[21] State of the Internet at 19-47. According to Mediamark Research, close to 80% of U.S. adults have Internet access. Industry Notes, Washington Internet Daily (June 23, 2004) at 5.

[22] State of the Internet at 13-14. *See also* "Leadership for the New Millennium: Delivering on Digital Progress and Prosperity;" The U.S. Government Working Group on Electronic Commerce, 3rd Annual Report (2000).

[23] For example, it has been reported that it costs between $1.25 and $1.77 to process a check, compared to 10¢ to process a purchase made on the Internet. C. Mollenkamp, *Bank of America Taps New Chief of E-Payments and Card Services*, The Wall Street Journal, Apr. 20, 2001, at B2. *See, e.g.*, Faith Keenan, *The Price is Really Right: With a Web-savvy system, companies can figure out just what the market will bear*, Bus. Week, Mar. 31, 2003, at 63 (highlighting companies' use of the web to establish pricing models).

© 2004 Piper Rudnick LLP. All Rights Reserved.

provided new and different ways of conducting business.[24] The internet has created new forms of empowerment for individuals, new types of communities and new tools for dealing with social issues.[25] Now the internet is reinventing entire markets. E-marketplaces promise to change the dynamics of many industries. Louis Gerstner, in his final letter to IBM's shareholders, commented on IBM's renewed emphasis on providing overall I/T services, and observed that:

> As I/T moves out of the back office and into the executive suite, value and growth in our industry are driven less than they used to be by technical innovation or product excellence, as necessary as those remain. *What matters today is the ability to integrate technology into the lifeblood of business.* The people who help customers apply technology to transform their businesses have increasing influence over everything from architecture and standards to hardware and software choices and partners.[26]

Several years later, Samuel Palmisano, the current IBM President, made similar remarks emphasizing integration:

> Companies have come to realize that if they're going to respond rapidly and effectively to today's volatile marketplace, they need to do more than web-enable discrete systems, processes or business units. They need to pull together all of the systems they've already got and integrate them securely with their core business activities horizontally, across not just their whole company but their entire value chain, from customers to suppliers.[27]

---

[24] B. Schlender, *The New Soul of a Wealth Machine*, Fortune, Apr. 5, 2004, at 102, 104, where Peter Drucker is said to have noted that the Internet has the power to fundamentally change the way companies do things and the markets in which they compete. "The Internet makes it possible for persons worldwide to buy, sell and ship goods to or from anywhere in the world from their own living room using a computer and an Internet hook-up." *See also Toys "R" Us, Inc. v. Step Two, S.A.*, 318 F.3d 446, 454 (3d Cir. 2003); *Euromarket Designs, Inc. v. Crate & Barrel Limited*, 96 F. Supp.2d 824, 827 (N.D. Ill. 2000); *Zippo Manufacturing Co. v. Zippo DotCom, Inc.*, 952 F. Supp.2d 1119, 1124 (W.D. Pa. 1997).

[25] J. Webber, *Culture of Risk*, The Industry Standard, June 5, 2000, at 11.

[26] Chairman's Foreword, IBM Annual Report for 2001 (2002), at 3 (emphasis added). Indeed, Wal-Mart's adoption of various technologies has the power to drive new developments. *See also* B. Feder, *Wal-Mart's tracking Tags Are Getting First Field Test*, The New York Times, May 1, 2004 at B14 (reporting on Wal-Mart's adoption of radio tags using "RFID" technology at the store level).

[27] Chairman's Letter, IBM Annual Report for 2003 (2004), at 4.

© 2004 Piper Rudnick LLP. All Rights Reserved.

Andrew Grove, the chairman of Intel Corporation, is quoted as having said five years ago that by now, all companies would be internet companies.[28] He was also quoted as saying that e-commerce is happening the way all the hype said it would.[29] Today, competition dictates that every company consider, adopt, and refine an e-business strategy. More than ever, management and mastery of business information is at the core of any company's competitive strategy. In considering the nature of such competition, Bill Gates wrote that:

> I have a simple but strong belief. The most meaningful way to differentiate your company from your competition, the best way to put distance between you and the crowd, is to do an outstanding job with information. *How you gather, manage, and use information will determine whether you win or lose.*[30]

To the same effect, Bill Gates notes that the companies that do not use information technologies effectively will fall behind.[31] Managing information effectively is an essential e-business strategy.

---

[28] G. Anders, *Buying Frenzy*, The Wall Street Journal, July 12, 1999, at R6.

[29] Andy Grove at 86.

[30] Bill Gates, Business @ The Speed of Thought: Succeeding in the Digital Economy 4 (2000) (emphasis supplied). *See also* T. Mullaney, *Using the Net to Stay Crisp: How Utz tracks its snacks from oven to grocery shelf*, Bus. Week, e.biz Section, Apr. 16, 2001, at EB34 (reporting on the development by Utz Quality Foods Inc. of an internet based application ("UtzFocus") for tracking orders, sales, and performance).

[31] Robert Hof, "*Why Tech Will Bloom Again*," Bus. Week, Aug. 25, 2003, at 64, 67.

© 2004 Piper Rudnick LLP. All Rights Reserved.

WHAT MAKES E-BUSINESS DIFFERENT

All e-business is potentially worldwide in scope. There are no national or territorial boundaries on the internet. The jurisdictional exposure to uncertain and possibly conflicting laws is great. The ease of access to e-business businesses through the internet coupled with their 24x7 availability presents a strong likelihood that customers from around the world will visit sites. This global exposure and related legal risks associated with the absence of territorial boundaries as well as business hour limitations need to be kept in mind.

E-business websites are private property. They may be thought of as a piece of virtual real estate in cyberspace. Because they are positioned in cyberspace there is an implied invitation to visit them. They are intended to be visited. Visitation is encouraged further by advertising. This is one reason why websites need to implement applicable Terms of Use so that customers and visitors are on notice as to the house rules applicable to the websites, their content, services and use. Website Terms of Use have become the principal legal strategy for managing the legal risks associated with e-business or virtual business websites.

Another major characteristic of e-commerce business applications is to recognize their dependence on information technology. The risks of computer errors, hackers, computer viruses, denial of service attacks, power outages, computer malfunctions and unplanned downtime need to be appreciated. Security, reliability and scalability are thus very important to e-commerce businesses and promise to become increasingly more important in the years ahead. Cyber security has become increasingly more important as the risks become increasingly more threatening.

Another factor is the anonymous nature of the relationship between e-buyers and e-sellers. Fraud is much more of a risk in e-business transactions because of the anonymous character of the relationship. There are concerns over possible export control violations, customers being children or other persons who are not competent to enter into a contract with the seller, or being someone using another party's identity or account number. Identity theft has become a major concern. These concerns are more problematic because of the anonymous, virtual relationship that exists in e-business transactions. It is also important to recognize that brand names and branding strategies are much more important in e-business. E-business companies need to recognize the importance of a trust relationship with their customers. Trust has emerged as a critical success factor.

It is important to recognize that most e-business applications involve intellectual property considerations. Linking, framing, caching and downloading, for example, all implicate the copyright laws. Access to and use of most of website content also may require copyright analysis. Patent, trademark, domain name and trade secret issues may also need to be considered. The intellectual property analysis should be an integral part of the early planning and design for new e-business applications.

E-commerce business models are usually based on the network effect. Network effects arise when the value of the e-business application increases with the addition of each participant. Supply and demand do not have the traditional economic relationship. E-business agreements tend to be short in duration with due regard to rapidly changing market conditions and advances

© 2004 Piper Rudnick LLP. All Rights Reserved.

in technology. Exponential improvements in technology keep occurring year after year. These differences need to be appreciated.

E-business transaction data and site usage data are becoming increasingly more valuable. "Click-histories" and customer data are considered to be very valuable commercially. Likewise, privacy policies and procedures are given more heightened concern in e-business transactions compared to other brick and mortar transactions.

The internet is a communications medium. First Amendment issues may arise. Much of e-business is carried out through electronic agreements and electronic communications which implicate some specific legal issues and requirements. Electronic communication and transactions are being carried out at internet speed. The speed of these communications and transactions also needs to be appreciated. There is less time for reflection and more potential for mistakes. Computer software errors and data input errors, for example, may cause serious problems.

Finally, the internet affords dramatic possibilities for opening up societies that are relatively insular and closed to the outside world, although that promise remains unfulfilled particularly in countries that block unfettered access to the internet or that control ISPs.[32] However, there are many countries that block access to the internet, or regulate the content that may be seen by citizens in their country.[33] Efforts to obstruct content stand starkly in the way of the free flow of information and technology that has led new markets to emerge, in part, as new technologies have matured.

These are some of the principal characteristics of e-business that make it different. These differences are useful to keep in mind when developing legal risk management strategies for today's e-business applications and tomorrow's potential problems.

---

[32] *See Caught in the Net: Instead of undermining repressive regimes, the internet might strengthen them*, The Economist, Jan. 25, 2003, at Internet-23 (commenting upon the control that some governments have exercised over ISP's and the internet backbone, which undercuts the goal of free-flowing information reaching all users).

[33] *See, e.g., Iranian authorities blocked access to 3 pro-reformist websites*, 4 Wash. Internet Daily 169, Sept. 1, 2004, at 3; Mahmood Saberi, *AOL site blocked for bypassing proxy*, Gulf News (Online Edition), Nov. 24, 2003 (available at http://www.gulf-news.com/Articles/news.asp?ArticleID=103693) (reporting on U.A.E. government action to block access to AOL, which in turn had made a "tunneling" service available that enabled users to bypass content restrictions); Jennifer Lee, *Saudi Censorship of Web Ranges Far Beyond Tenets of Islam, Study Finds*, The New York Times, Aug. 29, 2002, at E7; Shen, *China's Regulatory Scheme of Online Advertising and Foreign Investment*, 30 Int'l Bus. Lawyer 9, at 394 (Oct. 2002) (re content restrictions in China). Even outward signs of progress need to be considered in their context. For example, a report that China Unicom plans to open 3,000 Internet cafés in 2004 was considered a sign that the government would assert stronger control over a sector that was earlier dominated by private companies. *See China Unicom*, 5 Wash. Internet Daily 179, Sept. 16, 2004, at 5.

© 2004 Piper Rudnick LLP. All Rights Reserved.

JURISDICTION

An e-business website is a virtual storefront with worldwide exposure. The websites are available anytime to anyone, anywhere in the world with access to the internet. The internet is not limited by any geographic or jurisdictional boundaries and is believed to connect more than 159 countries. The primary overriding issue in the legal aspects of e-business concerns jurisdiction. What consumer laws, contract law, privacy laws and other laws apply to e-business transactions? Where does a transaction take place? How will conflicts in law be determined?

There has been a significant amount of litigation in the United States concerning the extent to which websites and other internet activities can subject a foreign out-of-state defendant to the personal jurisdiction in another state. The mere creation of a website may create additional liability entirely independent from e-mail communications and e-business sales over the internet. By mere virtue of its presence on the World Wide Web, a company's website (and the content on that site) will reach a virtually unlimited audience and thus could become a source of litigation. In the coming years it is estimated that most of web users will be international, and that countries other than the United States will account for nearly half of the worldwide e-commerce.

There is no question that internet activities have increased the jurisdictional exposure of most companies on the World Wide Web.[34] Generally, the law with respect to jurisdictional issues involving the internet is just evolving and is far from certain.[35] The courts in the United States have divided these jurisdictional cases involving websites and internet activities into three categories. These categories represent a continuum. At one end of the continuum jurisdiction definitely exists. The middle category requires analysis to determine whether jurisdiction is present. At the other end of the continuum jurisdiction is not present.

The first category concerns parties who merely establish a passive, informational website. In this category of cases, the courts usually find that the defendants are not subject to personal jurisdiction based solely on the plaintiff being able to access the defendant's website from such

---

[34] In *Gorman v. Ameritrade Holding Corp.*, 293 F.3d 506 (D.C. Cir. 2002), the D.C. Circuit noted that Ameritrade's website made it possible through real-time transactions, 24 hours per day, to have contacts with the District of Columbia that are continuous and systematic to a degree that traditional corporations can never approach.

[35] U.S. Courts appear to be raising the jurisdictional bar in reaction to concerns about jurisdictional exposure and are requiring a greater showing of purposeful availment or effect in the forum. *See, e.g.*, A. Mazumdar, *Zippo Scale for Testing Jurisdiction Giving Way to Purposeful Availment-Based Standard*, 6 Electronic Commerce L. Rep. (BNA) 45, at 1165-66 (Nov. 21, 2001). Compare *Bird v. Parsons*, 2 U.S. App. LEXIS 9543 (6th Cir. May 21, 2002) (registrar could be sued in Ohio because it had transacted about 5,000 domain name registrations with Ohio residents); with *Robbins v. Yutopian Enters., Inc.*, 2002 U.S. Dist. LEXIS 9012 (D. Md. May 15, 2002) (national accessibility to website deemed insufficient to establish "minimum contacts" with Maryland, even where there were 46 transactions with Maryland residents).

© 2004 Piper Rudnick LLP. All Rights Reserved.

jurisdiction.[36] Courts have found that merely providing an online purchase order form that must be mailed or faxed does not provide enough interactivity for jurisdiction.[37] Similarly, a return e-mail address or 800 telephone number along with a passive website is still not sufficient for jurisdiction. Moreover, a website that by its design does not "target" residents in a local forum is often deemed not sufficient grounds to find that the website operator is subject to personal jurisdiction in that forum. One such example was that of a German company sued in New York for trademark infringement where the court dismissed the case, noting that the website did not have sufficient contacts with New York residents, even thought it was accessible in the state, and observing that the site was even written in German.[38] The second category of cases requires an analysis of the nature and extent of the activities beyond a passive website to determine whether the exercise of personal jurisdiction is appropriate. The focus in this second category is on whether the defendant has purposely directed, targeted or availed itself of the forum in which jurisdiction is sought. The third category of cases is at the other end of the continuum from passive websites. This category concerns the conduct of commercial activities. E-commerce websites are intended to be much more interactive than merely passive websites and broad jurisdictional exposure is quite likely, including potential foreign jurisdictional exposure around the world.[39] To manage the jurisdictional risk, it is important not to target jurisdictions the e-commerce site wants to avoid.

A decision handed down by the U.S. Court of Appeals for the Third Circuit, while referring to *Zippo* and other cases, succinctly stated the jurisdiction issue thusly:

> [T]he mere operation of a commercially interactive web site should not subject the operator to jurisdiction anywhere in the world. Rather, there must be evidence that the defendant 'purposefully availed' itself of conducting activity in the forum state, by directly targeting its web site to the state, knowingly interacting with

---

[36] *See, e.g.*, *Soma Med. Int'l v. Standard Chartered Bank*, 196 F.3d 1292, 1296-97 (10th Cir. 1999), in which the Court of Appeals affirmed a dismissal for lack of personal jurisdiction where the defendant's website was deemed passive as it did "little more than make information available to those who are interested."

[37] *See, e.g*., *Mink v. AAAA Development, Inc*., 190 F. 3d 333 (5th Cir. 1999); *Pound v. Airosol Company, Inc.*, 2003 U.S. Dist. LEXIS 15869 (D. Kan. Aug. 21, 2003) (no personal jurisdiction over operator of informational website that did not allow for online ordering).

[38] *Stewart v. Vista Point Verlag*, 56 U.S.P.Q.2d 1842 (S.D.N.Y. 2000).

[39] *See, e.g., Euromarket Designs Inc. v. Crate & Barrel Limited*, 196 F. Supp.2d 284 (N.D. Ill. 2000) (Irish e-tailer subject to jurisdiction in Illinois); *cf. Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisenitime*, 169 F. Supp.2d 1181 (N.D. Cal. 2001), *summary judgment granted*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001) (French court could not order halt to an auction, and therefore, the exercise of free speech, in the U.S. among U.S. parties, even though website can also be seen in France); *reversed*, 2004 U.S. App. LEXIS 17869 (9th Cir. 2004) (U.S. court lacked personal jurisdiction over French defendant).

© 2004 Piper Rudnick LLP. All Rights Reserved.

residents of the forum state via its web site, or through sufficient other related contacts.[40]

In *Toys "R" Us*, the Third Circuit declined to exercise jurisdiction where a website originating from Spain did not appear to have been designed or intended to reach customers in New Jersey, and the court noted that the websites were entirely in Spanish, the prices for its merchandise were in Pesetas or Euros, the merchandise could only be shipped to addresses within Spain, and U.S. addresses were not accommodated.[41] A different outcome based on consistent reasoning was reached in *Euromarket Designs, Inc. v. Crate & Barrel Limited*.[42] In *Euromarket Design*, the defendant's website originally allowed U.S. customers to enter their address. After initiation of the lawsuit, the website bore the statement "Goods Sold Only in the Republic of Ireland" on its opening page and expressed prices in Irish pounds. However, users of defendant's website could ship and bill orders to U.S. addresses The court noted that the billing address information fields on defendant's website were clearly organized for US-formatted addresses.

European consumer protection laws, for example, are likely to apply when companies make e-commerce sales to European consumers. European Union legislation has been enacted to protect European consumers, was to have been implemented by Member States before January 17, 2002.[43] In addition to the EC Directive on e-commerce, there are numerous other EC Directives that apply to one or more aspects of e-commerce, for example, the Directive on

---

[40] *Toys "R" Us, Inc. v. Step Two, S.A.*, 318 F.3d 446, 454 (3d Cir. 2003). *See also Gator.com Corp. v. L.L. Bean, Inc.*, 2003 WL 22038396 (9th Cir. Sept. 2, 2003) (retailer's "continuous and systematic" contacts with Calif. residents via internet and catalog sufficient to invoke jurisdiction in Calif.); *Carefirst of Maryland v. Carefirst Pregnancy Centers*, 334 F.3d 390 (4th Cir. 2003) (in trademark infringement matter, a website directed to Chicago-area women was insufficient cause for jurisdiction in Md., even though Md. residents could use website to submit charitable donations; web-hosting relationship with Md. host also insufficient to invoke jurisdiction due to content of website); *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 713-14 (4th Cir. 2002) (adopting *Zippo* standard); *Neogen Corp. v. Neo Gen Screening, Inc.*, 282 F.3d 883, 890 (6th Cir. 2002); *Swarovski Optik N. Am. Limited v. Euro Optics, Inc.*, 2003 U.S. Dist. LEXIS 14881 (D. R.I. Aug. 25, 2003); *B.E.E. Int'l Ltd. v. Hawes*, 2003 U.S. Dist. LEXIS 10161 *7 (M.D.N.C. June 11, 2003) (directing e-mails into N.C. is not sufficient to invoke personal jurisdiction over a Belgian entity); *Internet Billions Domains, Inc. v. Venetian Casino Resort, LLC*, 2002 U.S. Dist. LEXIS 11805 at *15-*16 (E.D. Va. 2002) (court exercised jurisdiction, concluding that the actions alleged to violate the Lanham took place in US commerce, and noting that "the mere fact that the internet allows for worldwide access does not strip an American court of its subject matter jurisdiction under the Lanham Act over activities directed at the United States."). *Cf. Pavlovich v. DVD Copy Control Assoc., Inc.*, 29 Cal. 4th 262; 58 P.3d 2 (Cal. 2002) (lack of sufficient contact with Calif. doomed exercise of jurisdiction over Matthew Pavlovich, who founded a website on which it was alleged that he posted code to circumvent DVD copy control technology).

[41] *Toys "R" Us, Inc. v. Step Two, S.A.*, 318 F.3d at 454.

[42] 96 F. Supp. 2d 284 (N.D. Ill. 2000).

[43] 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, 2000 O.J. (L 178) 1.

© 2004 Piper Rudnick LLP. All Rights Reserved.

Distance Selling of Goods and Directive on Unfair Terms in Consumer Contracts.[44] In addition, there are several rules that touch upon the transmission of unsolicited e-mail and similar communications: The Distance Selling Directive[45] and the Electronic Commerce Directive.[46]

In late 2002, the High Court of Australia ruled in a landmark case, *Dow Jones & Co., Inc. v. Gutnick*,[47] that an Australian plaintiff can bring suit in Australia against the publisher of *The Wall Street Journal's* website, alleging that an article published on the *Journal's* website defamed the plaintiff. In the High Court's ruling, the judges reasoned that:

> [O]rdinarily, defamation [takes place] at the place where the damage to reputation occurs. Ordinarily that will be where the material which is alleged to be defamatory is available in *comprehensible form* assuming, of course, that the person defamed has in that place a reputation which is thereby damaged. It is only when the material is in comprehensible form that the damage to reputation is done and it is damage to reputation which is the principal focus of defamation, not any quality of the defendant's conduct. In the case of material on the World Wide Web, it is not available in comprehensible form until downloaded on to the computer of a person who has used a web browser to pull the material from the web server. It is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed.[48]

Efforts are also underway to adopt a treaty (thus far, labeled the Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters) that would establish uniform standards for jurisdiction and enforcement of judgments. Among the matters covered in this treaty, the discussion of which is being conducted through the auspices of the Hague Conference on Private International Law, would be intellectual property and disputes involving

---

[44] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, 1993 O.J. (L 95) 29-34.

[45] Directive 97/7/EC of the European Parliament and Council of 20 May 1997 on the protection of consumers in respect of distance contracts. 1997 O.J. (L 144) 19-28.

[46] 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, 2000 O.J. (L 178) 1.

[47] 194 A.L.R. 433 (Canberra, Australia 10 Dec. 2002). The *Gutnick* decision was followed by another, *Cullen v. White*, in which an American, William Howard White, was alleged to have published online defamatory comments with respect to an Australian, Trevor Cullen. 8 E. Com. & L. Rep. (BNA) 35 at 873 (Sept. 17, 2003). Cullen apparently obtained a judgment in the Supreme Court of Western Australia for approximately $62,000; the plaintiff is reported to be considering how to enforce the judgment in U.S. courts.

[48] 194 A.L.R. 433 at ¶ 44 (emphasis added).

© 2004 Piper Rudnick LLP. All Rights Reserved.

consumers.[49] Developing a consistent and certain worldwide legal infrastructure to support e-business is currently a major priority of many countries and companies. To reap the benefits of e-business a supportive legal infrastructure providing an acceptable level of legal certainty and uniformity must be present. Today this infrastructure, especially for e-business consumer transactions, does not exist.

Domestic law is still evolving on the type of conduct that will result on a finding of enough of a jurisdictional nexus to require an e-business provider to defend claims in another state. The use of off-line advertising directed at citizens of a state, toll-free phone numbers accessible from a state, and the use of newer "push" technologies for customer-specific on-line targeted advertising will in all likelihood erode a claim by the website owner that a site is merely passive.

In light of the multiplicity of laws that may apply to a website, one should consider requiring arbitration in the terms and conditions in any e-business agreements as the means of resolving disputes with users of a company's e-business sites. While this will not prevent the application of a foreign law in a company's state of domicile, it may serve to fend off class actions and similar suits and will likely allow greater control over claims in the various jurisdictions.[50] Arbitration clauses should expressly provide that class action arbitration is prohibited under the agreement if class action suits are to be avoided.[51] A number of other legal strategies are being used to minimize uncertain jurisdictional exposure. In some circumstances forum selection clauses may be included in click-wrap and terms of use agreements used in e-business transactions.

Some Website owners have sought to reduce their jurisdictional exposure through statements and disclaimers on their Websites. For example, one Website specifically indicated that it does not conduct sales, accept orders, or receive payments through its Website. It also indicates that the receipt of a file via internet FTP or e-mail is not a sales transaction and does not constitute placing an order. It also emphasizes and specifies the exclusive market served by its e-commerce business.[52] One court expressed concern over the jurisdictional exposure of

---

[49] A draft of the convention can be found on the website of the Hague Conference on Private International Law, at *http*://www.*hcch.net/e/workprog/jdgm.html*.

[50] *See, e.g., In re Real Networks, Inc. Privacy Litigation*, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. 2000) (End User License Agreement, with arbitration clause, applicable to downloaded software enforced even though class-wide arbitration not provided and arbitration in distant exclusive forum was costly for many licensees).

[51] *See Green Tree Financial Corp. v. Bazzle*, 123 S. Ct. 2402 (2003). It is also desirable to provide that the arbitration agreement is subject to the Federal Arbitration Act to preempt any conflicting state statutes. *See Discover Bank v. The Superior Court of Los Angeles County*, 105 Cal. App. 4th 326 (Cal. Ct. App., 2d Dist., Jan. 14, 2003).

[52] *See, e.g., Desktop Technologies, Inc. v. Colorworks Reproduction & Design, Inc.*, 1999 WL 98572 (E.D. Pa. 1999).

© 2004 Piper Rudnick LLP. All Rights Reserved.

small e-commerce businesses and suggested that the owner of a website could limit its exposure by including a disclaimer that it will not sell its products outside a certain geographic territory and a click-wrap agreement including a choice of venue clause.[53] Venue forum selection clauses have become a very important risk management strategy. They are commonly used in website terms of service and terms of use agreements.[54] Special consideration should be given to ensuring that arbitration provisions are enforceable in B2C consumer transactions, including developing a dispute resolution program where the business entity pays most of the cost of arbitration.[55] Companies found to be too aggressive in trying to deny consumers effective remedies may run the risk that an arbitration agreement clause will be found unconscionable and unenforceable.[56]

Some multinational companies are addressing the legal concerns relating to global e-business by setting up separate websites that are tailored to comply with the local laws in given countries. If an e-purchaser seeks to make a purchase online, the purchaser is directed by the master website to the website for his or her country so that the purchase will comply with local consumer and other laws, including any foreign language requirements. Building this type of infrastructure to support e-business is very expensive and will make it difficult to realize the cost-savings and efficiencies from e-business.

Other issues concerning global e-business include developing global credit card acceptance systems and support for multicurrency transactions, as well as establishing the fulfillment infrastructure and relationships to handle e-business sales and customer returns in the global marketplace. Other factors to consider include providing multilingual support, foreign language translations of the terms and conditions applicable to e-business transactions, recognizing cultural issues and localized content.

---

[53] *Stomp, Inc. v. Neat O, LLC*, 61 F. Supp.2d 1074, 1080-81 (C.D. Cal. 1999).

[54] *See, e.g., Decker v. Circus Circus Hotel*, 49 F. Supp.2d 743 (D.N.J. 1999); *America Online, Inc. v. Booker*, 781 So.2d 423 (Fla. Ct. App. 3d Dist. 2001); *Barnett v. Network Solutions, Inc.*, 38 S.W. 3d 200 (Tex. Ct. App. 2001); *DiLorenzo v. America Online, Inc.*, 2 ILR (P&F) 596 (N.Y. Sup. Ct. 1999); *Caspi v. The Microsoft Network*, 323 N. J. Super. 118, 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999).

[55] *See Green Tree Financial Corp. - Alabama v. Randolph*, 120 S. Ct. 1552 (2000) (upholding enforceability of arbitration clause, even where right to pursue class action effectively denied); *see also Green Tree Financial Corp. v. Bazzle*, 123 S. Ct. 2402 (2003) (question of whether a contract forbids class arbitrations is for the arbitrator to decide). The 2000 *Green Tree* decision suggests that an express cost-allocation should be considered for consumer arbitration agreements to avoid the possibility that the arbitration agreement will be determined unenforceable on the grounds that the cost of arbitration is too high, and that the costs effectively preclude the vindication of statutory rights. Companies need to consider a consumer-friendly dispute resolution program funded at least in part by the company so that the cost of dispute resolution does not in effect give consumers a chance to claim that they were denied a chance to seek remedies.

[56] *See Comb v. Pay Pal, Inc*, 2002 WL 2002 171 (N.D. Cal. Aug. 30, 2002) (Pay Pal's User agreement found to be both procedurally and substantively unconscionable).

© 2004 Piper Rudnick LLP. All Rights Reserved.

FRANCHISE AND DISTRIBUTION ARRANGEMENTS

Agreements granting rights to distribute traditional goods, software and other information products owned or controlled by a third party will typically identify the territory and channels of trade within which product distribution is authorized. Companies must be very sensitive to any preexisting distribution agreements that may affect e-commerce or electronic distribution to make sure that there is not a violation of any grant of "exclusive" or other rights by advertising, promoting, or selling through a website. Similarly, companies need to be sure that, as a distributor, they do not violate any territorial restrictions or other restrictions on the grant of distribution rights. Since e-commerce is global, it is very easy to create a conflict with prior distribution and marketing channels. Channel conflict and contention as the result of e-commerce sales is a real problem today, especially with manufacturers entering markets that were previously handled by distributors and retailers,[57] even if such channel competition is merely perceived.[58] Likewise there is more competition generally because e-tailers can serve a much broader market. While the internet is fundamentally changing the way distribution models work, it has not altered the fundamental effectiveness of bricks-and-mortar businesses.[59]

Agreements today should expressly contemplate and permit e-business, and it is even more important now to avoid any exclusive arrangements that could preclude e-business. This is particularly so in the case of franchise agreements, given the length of time that franchise agreements last, as these arrangements commonly have terms that run from 20-40 years. Any territorial restrictions may be difficult to enforce. For example, if a distributor is authorized to sell the products in a specified territory and that distributor establishes an e-commerce website in the territory that is accessible to customers outside the territory, potential problems exist without regard to whether the territory is an "exclusive" or "non-exclusive" territory.

The *Playboy Enterprises, Inc. v Chuckleberry Publishing Co.*, 939 F. Supp. 1032 (S.D.N.Y. 1996), case suggests how courts might try to deal with territorial distribution problems that arise in global e-commerce. There the Italian defendant was required to: (1) either shut down its internet site completely or refrain from accepting any new customers residing in the

---

[57] "*Sun Moves Into Online Auctions*," The Industry Standard, Aug. 16-23, 1999, at 30; K. Brooker, *First: E-Rivals Seem To Have Home Depot Awfully Nervous*, Fortune, Aug. 16, 1999, at 28.

[58] *See, e.g., First Jewellery Co. of Canada Inc. v. Internet Shopping Network LLC, 2000 U.S. Dist. LEXIS 794* (S.D.N.Y. 2000) (wholesaler concerned that customers would believe it was competing directly with its customers).

[59] *See, e.g.*, Ralph Kisiel, *Internet's impact at the dealership? Less than feared*, Automotive News, Jan. 20, 2003, at 27. *See also* Agrawal, Arjona, and Lemmens, *E-performance: The path to rational exuberance – successful e-commerce companies are following tried-and-true principles from the brick-and-mortar world*, The McKinsey Quarterly, 2001 Number 1, at 31. However, there are some industries that face the challenge of competing with technological innovation. *See, e.g., Goodbye to the video store*, The Economist, Sep. 19, 2002 (available online) (the article's subtitle is aptly descriptive: "Streaming video – for too long, 'video-on-demand' has promised more than it could deliver. But new ways are emerging for shrink-wrapping massive video files for delivery over the Internet.")

© 2004 Piper Rudnick LLP. All Rights Reserved.

United States; (2) invalidate the user names and passwords to the internet site previously issued to United States purchasers; and (3) revise its internet site to indicate that any purchase requests from United States customers will be denied. E-business websites may need to consider notices limiting their customers to customers in the authorized territory.[60]

Distributors must carefully review all distribution agreements to determine the extent each party's rights and obligations, to determine, for example, whether the contract addresses whether one party or the other is authorized to market, sell and distribute the products through e-business and electronic distribution, and, if so, subject to what territorial restrictions.

The internet also creates more of a problem with unauthorized distributors because the internet presents an easy and cheap way for unauthorized distributors to sell products and services. Gray marketers can easily obtain access to pricing information and take advantage of price differentials, even if the price differentials are due to taxes and import duties.[61] Pricing is more transparent on the Web. Suppliers may be disadvantaged by the increased cost transparency.

Typically distribution agreements authorize the distributor to use the manufacturer's trademark for purposes of the distribution agreement. If the trademark licensee uses the licensed trademark on its website to attract visitors and generate revenues other than the revenues on the licensed products, there may be an issue over whether the licensee is commercially exploiting the licensed trademark in an unauthorized manner.

In *Hard Rock Café International (USA) Inc. v. Morton*,[62] the court considered a trademark license restricted to licensed territories and licensed products in connection with the licensee's website. The license agreement prohibited the use or exploitation of the "Hard Rock Hotel" mark outside the specified territories to sell merchandise of any sort. The court found that the defendants were using their licensed trademark to attract visitors to their website and then to direct this traffic to other sites, through linking and framing, for commission revenue on the sale of unlicensed products not bearing the licensed trademark. This is just one example of the kind of problems that may arise in connection with trademark licenses. The use of licensed trademarks in connection with distribution over the internet needs to be considered carefully.

In the case of franchises with long-term contracts, many existing agreements did not directly address use of the marks on the internet, but do include provisions that nonetheless apply

---

[60] *See, e.g., Desktop Technologies, Inc. v. Colorworks Reproduction & Design, Inc.*, 1999 WL 98572 (E.D. Pa. 1999) (site disclaimer used to reduce jurisdictional exposure).

[61] L. Reisman, *Gray Market Blues*, The Industry Standard, July 19, 1999, at 114.

[62] 1999 U.S. Dist. LEXIS 8340 (S.D.N.Y. 1999), *amended by, injunction granted, in part*, 1999 U.S. Dist. LEXIS 13760 (S.D.N.Y. 1999).

© 2004 Piper Rudnick LLP. All Rights Reserved.

in that context. Several cases illustrate the point: *Hard Rock Café*, *California Closet Co., Inc. v. Space Organizational Sys., Inc.*,[63] and *Travel Impressions, Ltd. v. Kaufman.*[64]

In *California Closet*, the court looked to traditional franchise agreement clauses as the predicate for issuing a temporary restraining order at the franchisor's request. *California Closet* involved a franchisee who registered and used the domain name *californiacloset.com*, who operated a website at that address which appeared to be the franchisor's site, and who took system-wide sales leads from the website. The defendant-franchisee did not offer to pass these sales leads on to his fellow franchisees; rather, the defendant-franchisee offered to sell the leads to his fellow franchisees, and failing that, the defendant-franchisee threatened to sell the sales leads to third parties or to himself service the leads. The court ordered this franchisee to stop using a domain name that incorporated the plaintiff's trademarks, to stop making unauthorized use of the marks, and to stop engaging in unauthorized advertising – on the basis of a franchise agreement that provided for the franchisor's prior written consent to any proposed use of the marks and any proposed advertising.

While a contrary result was reached by the court in *Travel Impressions, Ltd. v. Kaufman*,[65] that case is consistent with *California Closet*. In *Travel Impressions*, the franchisor also sought a preliminary injunction to prevent its franchisee from continuing to use the domain name *www.empress.com* and the telephone number 1-800-EMPRESS. The court denied the injunction, noting (among other things) that it was not clear whether the language of the franchise agreement prohibited or permitted the franchisee's use of the marks in the manner that was central to the complaint. Had the franchise agreement clearly reserved to the franchisor the right – as in the *California Closet* case noted above, the outcome in *Travel Impressions* may have been different.

Most franchise agreements contain the two clauses that were central to the resolution of the *California Closet* case, and which vest the franchisor – as the trademark owner – with broad discretion as to trademark use relevant to the internet. First, most franchise agreements typically provide that the franchisee may use the franchisor's marks only to the extent specifically authorized by the franchisor. Second, most franchise agreements require the franchisor's advance approval before the franchisee may engage in proposed advertising and/or use promotional materials. To the extent that a franchisor wants to control or prevent franchisees' creation of independent websites, *California Closet* stands for the proposition that these clauses afford the franchisor with significant rights, since any website operated by a franchisee inevitably uses the franchisor's marks and is, almost by definition, promotional in nature. *Travel*

---

[63] Bus. Franchise Guide (CCH) ¶ 11,150 (E.D. Wis. 1997). *California Closet* was the first franchise case involving unauthorized B2C e-commerce and cybersquatting.

[64] 1997 U.S. Dist. LEXIS 23217 (E.D.N.Y. 1997) (reprinted at Bus. Franchise Guide (CCH) ¶¶ 11,470 and 11,471).

[65] *Id*.

© 2004 Piper Rudnick LLP. All Rights Reserved.

Impressions, an interim procedural decision, seems to reflect a less well-developed set of facts and, perhaps, contact language that is less unambiguous.

Although there are as yet no reported final decisions involving alternative distribution by franchisors using the internet, at least two such cases have been filed - and a preliminary injunction was granted in one of them (albeit an arbitral decision). One such case involves the H & R Block system. H & R Block was sued by 24 of its franchisees in an e-commerce dispute. In early 1999, H & R Block determined that it must offer do-it-yourself tax preparation software over the internet in order to compete with other increasingly computer/internet based competitors. H & R Block developed software that allows users to prepare their own tax returns on-line at a cost of approximately $10 versus approximately $90 at an H & R Block unit. Before rolling out the site, H & R Block offered to allow approximately 2,200 of its smaller franchisees to participate in the revenue from the site. H & R Block also approached approximately 20 of its largest franchisees with a proposal to share in the cost of establishing the web operations and to share in the revenue from those operations. The large franchisees declined, and H & R Block ultimately established web operations without their participation.

A group of 24 H & R Block franchisees subsequently filed suit in Missouri state court. *Angel v. H&R Block, Inc.*, No. 99-206379, Circuit Court of Jackson County, Missouri (filed April 13, 1999). In the suit, the franchisees alleged that H & R Block breached their franchise agreements by selling tax-preparation software directly to consumers in their exclusive franchise territories. According to the complaint, the franchise agreements, most originally written in the 1960's and 1970's, state that H & R Block cannot compete in the franchisees' territories in tax preparation and related services. Upon a violation of this covenant, certain of the agreements purportedly entitle the franchisees to receive a "competitive royalty" equal to 55% of the gross receipts from any such competitive activity. Other agreements purportedly require H & R Block to completely relinquish its rights in its proprietary marks in the franchisees' territories. The franchisees claimed breach of contract, breach of the implied covenant of good faith and fair dealing, unfair business practices, and violations of state antitrust laws. H & R Block contended that the agreements were contracts of indefinite duration and could be renewed only by mutual consent, leaving H & R Block free not to renew contracts on those terms. The Missouri Court of Appeals upheld H & R Block's position. *See Armstrong Business Services, Inc. v. H & R Block*, 96 S.W.3d 867 (Mo. Ct. Apps. 2002).

In another H&R Block case, a panel of arbitrators ruled 2-1 that the franchisor's offering of internet services was not contemplated in the franchise agreement's clause under which the franchisor agreed not to "operat[e] from a location" within a defined territory. The panel therefore refused to block the franchisor from offering internet services in the franchisee's territory. *In the Matter of the Arbitration Between 1989 Revocable Family Trust v. H&R Block*, Bus. Franchise Guide (CCH) ¶ 12,473 (American Arbitration Assn., Minneapolis, Minn., Dec. 31, 2002).

A panel of arbitrators issued a preliminary injunction in what was considered to be the first "internet encroachment" decision. In a AAA arbitration between *Emporium Drug Mart, Inc. of Shreveport, et al. and Drug Emporium, Inc. and Drugemporium.com, Inc.*, Bus. Franchise Guide (CCH) ¶ 11,966 (American Arbitration Assn., Dallas, Texas, Sept. 2, 2000), the arbitrators

© 2004 Piper Rudnick LLP. All Rights Reserved.

(in a two-to-one decision) issued a preliminary injunction enjoining the franchisor from selling products over the internet in franchisee territories.

In March 2000, a group of Drug Emporium franchisees filed an arbitration to stop their franchisor's e-commerce subsidiary, DrugEmporium.com, from selling products via the internet to consumers in their franchised territories. The franchisees argued that the franchise agreements gave the franchisees the exclusive right to operate "drug stores" within their territories using the name Drug Emporium. The franchisees presented evidence that DrugEmporium.com had promoted the website as "the full service online drugstore", "a virtual Drug Emporium store", and "Your neighborhood pharmacy for over 20 years." Drug Emporium claimed that it should not be bound by the language it used to describe the website because those were "marketing devices and do not alter the reality that [the website is] only a virtual store, not a brick and mortar store."

On September 2, 2000, the arbitrators issued a preliminary injunction preventing the franchisor from selling products at retail to any customer physically located within the franchisees' territories. While the *Drugemporium.com* arbitration panel's decision is noteworthy, it is significantly limited not only by the fact that it was an arbitral decision but also by the peculiar facts. Indeed, the arbitrators did not reach any broad conclusions or findings with respect to B2C e-commerce. Rather, they simply noted that in its franchise agreements, the franchisor promised not to establish a "store" within a particular area. The panel also noted that the franchisor often referred to its e-commerce website as an online "store." Without engaging in any analysis of whether a website is the functional equivalent of a "store" or any similar analysis, the panel simply compared the statements made by Drug Emporium (*e.g.*, visit our online "store") to the promises made in the relevant franchise agreement (*e.g.*, we will not open another "store" within the designated area). Consequently, the panel hoisted the franchisor on its own petard, and issued its injunctive order on the basis that the online "store", which made sales to customers within the areas where the franchisor promised (in the franchise agreements) not to open another store, was a breach of that contractual commitment.

In another arbitration case, *Hale v. Conroy's Inc.*, Bus. Franchise Guide (CCH) ¶ 12,177 (JAMS Dispute Resolution, Los Angeles, June 14, 2001), a similar issue was laid before the panel. Among other things, the franchisee objected to the franchisor's use of the "1-800-Flowers" phone and website network to solicit orders. The franchisee alleged, inter alia, that the franchisor violated the franchise agreement by operating the website and engaging in commerce through that model. The franchisee cited the *Drugemporium.com* arbitration decision as support for its position. The arbitrator disagreed.

The *Conroy's* arbitrator observed that the relevant franchise agreement granted exclusivity only with respect to another retail store, and the arbitrator further observed that a website is not another retail store. The arbitrator also concluded that the franchisee had been made aware of the chance that the franchisor might expand its phone-based system to include online sales efforts before the franchisee entered into an amendment to the original franchise agreement to add the "1-800-Flowers" business to the original franchise. The *Conroy's* arbitrator awarded the franchisor over $220,000 and ordered the franchisor to reimburse the franchisee for certain contractual obligations.

© 2004 Piper Rudnick LLP. All Rights Reserved.

Conroy's and *Drugemporium.com* are striking decisions. While franchisees will tout *Drugemporium.com* and franchisors will point to *Conroy's*, the fact is that only in Conroy's did the arbitrator engage in any substantive consideration of the central issue – which is whether an online sales effort violates a franchise agreement clause promising that the franchisor would not establish another store within a given area. While reasonable people may reasonably differ as to the outcome of these cases in particular circumstances, *Conroy's* is likely to be cited (even though it is merely an arbitral decision) for the proposition that a franchisee who knowingly entered into an agreement (there, an amendment) that gave the franchisor the right to engage in online sales cannot be heard to complain when the franchisor does, in fact, engage in online sales.

EU competition law also affects the way franchise agreements should deal with internet usage by franchisees and distributors. The Vertical Restraints Block Exemption,[66] interpreting Article 81(1) of the Treaty of Rome, prohibits any agreement or concerted practice which has the object or effect of "preventing, restricting, or distorting" competition. Breach of Article 81(1) may put a franchisor at risk of fines or of having non-compliant franchise agreements deemed unenforceable. In relevant portion, the Vertical Restraints Block Exemption addresses internet sales in an indirect manner. Article 4(c) of the Exemption bars limits on passive sales methods. Passive sales are those in which the seller responds to the buyer's request, and where the seller did not solicit the requests. Article 4(c) of the Exemption notes that in order to qualify for the exemption, a vertical agreement may not include:

> "the restriction of active or passive sales to end users by members of a selective distribution system operating at the retail level of trade, without prejudice to the possibility of prohibiting a member of the system from operating out of an unauthorised place of establishment …."

To provide guidance as to this standard, the Commission issued Guidelines on Vertical Restraints on November 13, 2000.[67] In relevant part, the Guidelines addressed internet sales as follows:

> Every distributor must be free to use the internet to advertise or to sell products. A restriction on the use of the internet by distributors could only be compatible with the Block Exemption Regulation to the extent that promotion on the internet or sales over the internet would lead to active selling into other distributors' exclusive territories or customer groups. In general, the use of the internet is not considered a form of active sales into such territories or customer groups, since it is a reasonable way to reach every customer. The fact that it may have effects outside one's own territory or customer group results from the technology, *i.e*. the

---

[66] Commission Regulation (EC) No 2790/1999 of 22 December 1999 on the application of Article 81(3) of the Treaty to categories of vertical agreements and concerted practices, 1999 O.J. (L 336) 21-25.

[67] Commission Notice (Guidelines on Vertical Restraints), 2000 O.J. (L 291) 1-44.

© 2004 Piper Rudnick LLP. All Rights Reserved.

> easy access from everywhere. If a customer visits the web site of a distributor and contacts the distributor and if such contact leads to a sale, including delivery, then that is considered passive selling. The language used on the website or in the communication plays normally no role in that respect. Insofar as a web site is not specifically targeted at customers primarily inside the territory or customer group exclusively allocated to another distributor, for instance with the use of banners or links in pages of providers specifically available to these exclusively allocated customers, the website is not considered a form of active selling. However, unsolicited e-mails sent to individual customers or specific customer groups are considered active selling. The same considerations apply to selling by catalogue. Notwithstanding what has been said before, the supplier may require quality standards for the use of the internet site to resell his goods, just as the supplier may require quality standards for a shop or for advertising and promotion in general. The latter may be relevant in particular for selective distribution. An outright ban on internet or catalogue selling is only possible if there is an objective justification. In any case, the supplier cannot reserve to itself sales and/or advertising over the internet.[68]

In effect, Article 4(c) has been interpreted to mean that a franchisee must be able to use the web to engage in passive off-site advertising and sales. A franchisor is free to impose quality control standards – for example, pertaining to the content, look and feel, and appearance of a franchisee's website – and, through the right to review and approve advertising and trademark usage, the domain name at which the website can be accessed. The franchisor cannot use these standards as a pretext for preventing franchisee use of the internet, and may only impose these conditions so long as the franchisee is not prevented from engaging in passive sales.

Another issue involving distribution systems may be a claim raised by some retailers that manufacturers use hyperlinks contained in products sold by retailers to pirate the retailer's customers. The National Association of Recording Merchandisers claimed that Sony used links on the Sony CDs that the retailers sell in order to direct the customers to websites owned or controlled by Sony. The retailers claim that the embedded link to Sony's website is an unlawful tying arrangement in violation of the Federal antitrust laws, since Sony will not sell CDs to the retailers without the links. The retailers claimed that their customers will eventually stop patronizing their stores to make purchases (preferring, instead, to shop online) because of Sony's alleged unlawful bundling practices (*i.e.*, that Sony would not sell CDs without the links that lead customers directly to Sony's website).

The issue of hyperlinks on a franchisee's website was addressed in a 2003 federal district court decision, *Voice-Tel Enters., Inc. v. JOBA, Inc.*, 258 F. Supp.2d 1353 (N.D. Ga. 2003). There, the franchisee's website contained a hyperlink to another site that was, initially, a mainstream commercial enterprise. At some time, the linked site went out of operation and,

---

[68] *Id.* at ¶ 51. There is not yet guidance on what conditions might rise to the level of "objective justification" for a franchisor seeking to ban a franchisee's web sales.

© 2004 Piper Rudnick LLP. All Rights Reserved.

unbeknownst to the franchisee (according to the court), was changed to a pornographic website. When the franchisor discovered that this was the case, it demanded that the franchisee remove the link (and the franchisee immediately complied). *Id*. at 1362. The franchisor sought to terminate the franchise because, among other things, the hyperlink to the pornographic site was alleged to have materially impaired the marks (which the parties had agreed would be grounds for termination) and diluted the marks. The court considered the issue and granted the franchisee's motion for summary judgment, dismissing the claim. In doing so, the court concluded that since it had heard no evidence of harm to the marks, and since harm could not be presumed merely because of the link to a pornographic site, there could have been no "material impairment" of the marks. Moreover, the court declined to extend a claim for trademark dilution to include a former hyperlink to another site that contained pornographic material. *Id*. at 1363.[69]

---

[69] The court in *JOBA* also declined to grant relief that it deemed disproportionate to the circumstances, given that the offending link had already been removed. *See* 258 F.Supp.2d at 1364.

© 2004 Piper Rudnick LLP. All Rights Reserved.

DOMAIN NAMES AND CYBERSQUATTING

There are two kinds of domain names – generic top-level domains (gTLD's) and country-code top-level domains (ccTLD's). Domain names have acquired added significance, as they become the main identifier used by e-business vendors to steer traffic to their site.[70] Not recognized as trademarks per se, domain names can be protected through trademark and unfair competition laws if the proper steps are taken in implementing their use. Domain names can also be protected in the U.S. under the Anticybersquatting Consumer Protection Act (the "ACPA"), internationally under ICANN's Uniform Dispute Resolution Procedures (the "UDRP"), and otherwise by similar means as discussed below.

Domain names may be used as a trademark if used to sell goods or service mark if used to sell services. The domain name itself may also be registered as trademarks, provided, in the case of the United States, that the domain name is used as the brand for the website or a portion of it. However, mere registration of a domain name does not by itself afford the domain name owner the right to obtain a trademark for the same name.[71]

One problem that has arisen in connection with domain names is with cybersquatters who register company domain names then seek payment from the company to transfer and assign the domain names to the company[72] or to simply use the domain name for profit.[73] Many companies are finding that a significant amount of time and attention needs to be paid to monitoring domain name usage and attacking cybersquatting when it occurs, in order to protect the company's intellectual property rights and investment in its internet operations.[74] In an article on the subject, a Cyveillance executive was quoted as saying that " '[w]e've never had a client whose jaw didn't drop when he or she saw some of the things that are uncovered. They just had no idea

---

[70] An Internet domain name is a unique name that identifies one or more Internet Protocol address. *See Internet Yellow Pages Network, Inc. v. Zconnexx Corp.*, 2000 U.S. Dist. LEXIS 15712 (W.D.N.Y. 2000). *See also Horseshoe Bay Resort Sales Co. v. Lake Lyndon B. Johnson Improvement Corp.*, 2001 App. LEXIS 5355 (Tex. Ct. App. 2001) ("domain names are valuable business assets because they function as the address for a site on the web"). For an excellent review of cases in which the term "domain name" is defined, and an excellent internet glossary, see Michael D. Scott, *Internet and Technology Law Desk Reference* (2003).

[71] *See, e.g., eCash Technologies, Inc. v. Guagliardo*, 2000 U.S. Dist. LEXIS 18314 (C.D. Cal. 2000), *citing Brookfield Communications, Inc. v. West Coast Enter. Corp.*, 174 F.3d 1036 (9th Cir. 1999).

[72] For an extensive summary of the impact that cybersquatting has on commerce, *see* the U.S. Senate Report in connection with the Anticybersquatting Consumer Protection Act (the "ACPA"), S. Rep. No. 106-140 (1999).

[73] *See, e.g., Target Advertising Inc. v. Miller*, 2002 U.S. Dist. LEXIS 8702 (S.D.N.Y. May 14, 2002) (ACPA applies not only to attempted profit from selling another party's domain name, but also profiting from use of another party's domain name as a web address).

[74] *See, e.g.*, Ritchenya Shepherd, *Counsels' Domain-Name Pains, Porno, Infringement, and Cybersquatters: The Web's New Frontier*, National L. J., Sept. 4, 2000, at B1.

© 2004 Piper Rudnick LLP. All Rights Reserved.

the extent was that great. Our average Fortune 500 client has an average of about 650 abuse situations out there, and that's growing.' "[75]

Cybersquatters' efforts include domain names with just one letter different (sometimes referred to as "typosquatters")[76] and to "*.net*," "*.org*" variations of the "*.com*" domain name, as well as ccTLD's (such as *.cc*, *.tv*, and other domain names that are marketed by U.S. registrars).[77] The courts have ruled consistently against cybersquatters usually under trademark infringement or trademark dilution grounds, or under the ACPA, as discussed below. This is sometimes referred to as abusive domain name registration. The ACPA provides a powerful remedy to combat cybersquatting. Corporate domain name strategies should contemplate registration of related domain names to guard against similar domain names being registered and used by others.[78]

One strategy is to consider "cluster registrations." By registering the domain name in all of the commercially available generic top level domain names and other ICANN-approved top level domain names, companies may avoid some confusion and dilutions. It may also be prudent

---

[75] Steven Andersen, *Law Departments Wrestle With Internet Infringement Issues*, 10 Corp. Legal Times 109 at 1, 24-27 (Dec. 2000).

[76] However, the courts will strike down typosquatting under the same rules that apply to more straightforward domain name hijacking. *See, e.g., Shields v. Zuccarini*, 254 F.3d 476 (3d Cir. 2001); *Toronto-Dominion Bank v. Karpachev*, 188 F. Supp.2d 110 (D. Mass. 2002). *See also* Declan McCullagh, *Court cracks down on URL copycat*, CNET news.com (Oct. 8, 2002) (at http://news.com.com/2100-1023-961276.html) (reporting on a court ruling threatening to hold defendant in contempt where defendant had registered the domain name WPNI.org, which is similar to the e-mail address (WPNI.com) used by many Washington Post reporters, in a confessed effort to divert e-mails intended for reporters, due to registrant's opposition to the newspaper's editorial policies).

[77] For example, in December 2001VeriSign Inc. (the exclusive registry of the *.com* gTLD until 2007 and the world's largest registrar of domain names) purchased eNIC, the registry for *.cc* ccTLD's (the Cocos Islands), and the exclusive worldwide rights to serve as the registry for the *.tv* ccTLD. VeriSign will use its considerable marketing muscle to promote and sell *.cc* and *.tv* domain names along with other domain name offerings, such as gTLD's *.com, .org, .net, .info,* and *.biz* and other ccTLD's such as *.bz* (Belize), and *.ws* (Western Samoa). *See* David McGuire, *VeriSign Buys .cc Internet Domain Name Registry*, NewsBytes.com (Dec. 18, 2001) (available at *http*://www.*newsbytes.com/news/01/173085.html*); Margaret Kane, *VeriSign buys .tv Web domain*, c|net News.com (Jan. 7, 2002) (available at *http://news.cnet.com/news/0-1005-200-8393177.html?tag=nbs*).

[78] Registrars themselves are largely shielded from claims that they have infringed on the basis that the registrar permitted a third party to register a domain name that contains a famous mark. *See, e.g., Lockheed Martin Corp. v. Network Solutions, Inc.*, 194 F.3d 980 (9th Cir. 1999) (Lanham Act claim); *Lockheed Martin Corp. v. Network Solutions, Inc.*, 141 F. Supp.2d 648 (N.D. Tex. 2001) (Anticybersquatting Act claim). One court has also concluded that registrars are shielded from liability under the ACPA when they offer to sell domain names for third parties. *See also Ford Motor Co. v. Great Domains.com, Inc*., 2001 U.S. Dist. LEXIS 21301 at *39-40 (E.D. Mich. 2001) (registrar offering to sell domain names on behalf of its own customers did not "traffic in" the domain name; "traffics in" element of the ACPA requires "a direct transfer or ownership interest in a domain name to or from the defendant").

© 2004 Piper Rudnick LLP. All Rights Reserved.

to register local misspellings of the company name, the company name and tradename in non-Latin character sets,[79] hyphenated versions of marks, foreign language translations, as well as common "nicknames" by which the company is known in the industry (*e.g.*, FedEx). Companies should also consider whether to acquire widely-used derogatory permutations of the domain name, such as "companysucks.com" and "companybeware.com."

Courts have not been hospitable to arguments that cybergripers (discussed generally in a separate section of these materials) are engaged in violations of the ACPA. In a case decided in April 2004 by the U.S. Court of Appeals for the Fifth Circuit, the court concluded that a defendant's registration of domain names used to run a website where the content was not commercial, but, rather was "to inform potential customers about a negative experience with the company." The court concluded that the defendant's conduct "is not the kind of harm that ACPA was designed to prevent."[80] A federal district court reviewing a similar claim, involving an attack on a domain name used to run a cybergripe site, concluded that:

> This Court finds that an analysis of the fourth factor under bad faith – whether Defendant had a "bona fide noncommercial or fair use of the mark" – speaks to the ultimate disposition of this case, and demonstrates why Defendant cannot be held liable under the ACPA. The purpose of this element is to protect domain name registrations and users engaged in protected activities such as critical commentary. This factor should be examined in tandem with the "safe harbor" in the ACPA which provides that bad faith intent shall "not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful." 15 U.S.C. § 1125(d)(1)(B)(2). As discussed herein, because Defendant had a "bona fide noncommercial" use of the mark, and had reasonable grounds to believe his use was lawful, Plaintiff's claim must fail.[81]

Companies should also consider proactively registering legitimate names before other parties who might have a successful defense are able to do so. For example, Nissan Motor Co. for years fought the owner of several domain names using the Nissan name (Nissan.com and Nissan.net), an individual named Uzi Nissan, who operates a company under the name Nissan

---

[79] A domain name registration in the *.com* gTLD can be obtained using any of 39 different character sets, ranging from Greek to Hebrew, Arabic to Kanji (Japanese), Cyrillic to Chinese, and Devanagari to Korean. A complete list can be found at *http://global.networksolutions.com/en_US/name-it/languagelist.jhtml*.

[80] *TMI Inc. v. Maxwell*, 368 F.3d 433, 439-440 (5th Cir. 2004) (citing *Lucas Nursery & Landscaping, Inc. v. Grosse*, 359 F.3d 806, 809 (6th Cir. 2004), in which the Sixth Circuit reached a similar conclusion as in *TMI*).

[81] *Mayflower Transit, LLC v. Prince*, 314 F.Supp. 2d 362, 369 (D.N.J. 2004).

© 2004 Piper Rudnick LLP. All Rights Reserved.

Computer Corp.; ultimately, Mr. Nissan was allowed to operate a website at those names, but under tight restrictions.[82]

Country-code TLDs – such as *.ca* for Canada, *.uk* for the United Kingdom, *.jp* for Japan, *.au* for Australia – are available through the registrars for each ccTLD. Not surprisingly, a study released on December 6, 2001 by the Canadian Internet Registration Authority (CIRA) found that over 70% of Canadians would prefer to shop online at a website that uses the *.ca* ccTLD, which indicates that the merchant is Canadian, rather than the generic *.com* gTLD.[83] A similar survey conducted in the U.S. also found that consumers would prefer visiting a website that uses the new *.us* ccTLD than sites using generic *.com* TLDs.[84] When given the opportunity to do so, Australians seem to choose ccTLD names in the .com.au registry over names in the .com gTLD.[85]

Just as significantly, the United States ccTLD - *.us* – was made generally available in April 2002. The *.us* ccTLD was first opened for a sunrise period in which trademark owners could register, and then for general registration and use. A nexus to the U.S. is required in order to obtain a *.us* domain name. For the same reasons as discussed above, and due to the surge in patriotism after the attacks on the U.S. of September 11, 2001, it is anticipated that the *.us* ccTLD will generate considerable interest.[86] In just the first nine months that the .us domain

---

82 *Nissan Motor Co. Ltd. v. Nissan Computer Corp.*, 231 F.Supp.2d 977 (C.D. Cal. 2002) (defendants permanently enjoined from including certain content (commercial content, advertising, links to other websites, disparaging remarks or negative commentary about Nissan Motor Co., or links to other sites with such disparaging commentary). *See* Ralph Kisiel, *Automaker fought businessman with cybersquatting, trademark laws*, Automotive News at 5-IT (Dec. 16, 2002). *Cf. Virtual Works, Inc. v. Network Solutions, Inc.*, 106 F.Supp.2d 845, 847 (E.D. Va. 2000), *aff'd sub nom., Virtual Works, Inc. v. Volkswagen of Am., Inc.*, 238 F.3d 265 (4th Cir. 2001) (In assessing the defendant's registration of the name vw.net, the district court observed that "[t]he holder of a domain name should give up that domain name when it is 'an intuitive domain name' that belongs to another.").

83 Canadian Internet Registration Authority Press Release, Dec. 6, 2001 (*http://www.cira.ca/news-releases/55.html*).

84 Neustar Press Release, April 24, 2002 (*http://www.neustar.us*).

85 ZDNet: Australians still opting for local domain name (Jan. 10, 2003) (*http://www.nua.com/surveys/?f=vs&art_id=905358702&rel=true*). This trend was confirmed in June 2004, when the Australian Department of Communications, Information Technology & the Arts (DCITA) announced that the total number of .au domain name registrations grew to more than 433,000 of which there were more than 110,000 new ".com.au" names registered. Because of this growth and to spur additional registrations, the .au registry authority reduced the charge paid by registrars to register a new .au domain name to Aus$7.50. News Release, Minister for Communications, Information Technology and the Arts, "*Demand For Web Delivers Cost Savings To Consumers*" (June 17, 2004) (available at *http://www.dcita.gov.au/Article/0,,0_1-2_1-4_119204,00.html*).

86 The Federal Trade Commission took action in a case involving a company that marketed alternate TLD's under the names *.usa* and *.brit*, as well as others. *Federal Trade Commission v. TLD Network Ltd.*,

(footnote continued to next page)

© 2004 Piper Rudnick LLP. All Rights Reserved.

name was available (April through December 2002), 416,080 .us domain names were registered.[87]

One popular strategy for companies with similar domain names or similar company names but different domain names is to develop a separate website that serves as a traffic director to avoid confusion. Visitors will go to the master site bearing the logical domain name visitors would likely go to if they were searching the web. This directory site would have information about each company to help the visitor find the site they are seeking.

Companies are well-advised not to register or use another party's trademark as a domain name. Using another party's trademark as a domain name may constitute trademark infringement under traditional likelihood of confusion principles.[88] Such use directs attention to another website using the goodwill of the trademark owner and may be deemed to create initial interest confusion.

(footnote continued from previous page)

No. 02C-1475 (U.S. Dist. Ct., N.D. Ill., filed Feb. 28, 2002). In this case, the FTC invoked its jurisdiction under Section 13(b) of the Federal Trade Commission Act, and obtained a temporary restraining order against several British companies, as well as their principals, who marketed and sold domain names under alternate TLD's such as *.usa*, *.brit*, *.bet*, *.scot*, and *.sex*. The FTC alleged in a complaint filed with the court that the defendants marketed these TLD's in such a way as to give the purchaser the impression that the TLD's could be used on the internet in much the same way as a domain name using the *.com* gTLD, and that these representations were false and misleading. Another FTC action was settled in March 2002, involving a Canadian company's allegedly deceptive practices in connection with marketing domain names. The defendant agreed to a stipulated order under which it agreed, among other things, to pay $375,000 to the FTC for consumer redress. *Federal Trade Commission v. 1268957 Ontario, Inc., Darren J. Morgenstern, et al.*, No. 01-CV-0423-JEC (Mar. 29, 2002).

87 SnapNames: State of the Domain Total Registrations per gTLD (Q4 2002) (available at *https://www.sotd.info/content/documents/total_registrations.pdf*, visited April 7, 2003). In contrast, only a handful of other ccTLD's had higher registration totals as of October 2002: German (.de) (5.5 million), the British commercial name (.co.uk) (3.1 million), Italian (.it) (681,779), Dutch (.nl) (617,045), Argentine commercial name (.com.ar) (463,571), and Swiss (.ch) (442,512). Two additional ccTLD's – .cc (Cocos (Keeling) Islands (581,147) and .tv (Tuvalu) (473,168) – also had more registrations that the .us ccTLD, largely due to the fact that these names in these ccTLD's are marketed heavily in the U.S. and elsewhere as alternatives to traditional gTLD's. SnapNames: State of the Domain (Q3 2002) at 6 (Oct. 24, 2002).

88 *See, e.g., PACCAR, Inc. v. TeleScan Technologies, L.L.C.*, 319 F.3d 243 (6th Cir. 2003) (court upheld a preliminary injunction against the defendant's operation of websites at domain names that incorporated the plaintiff's marks, such as peterbiltnewtrucks.com; however court rejected injunction against use of the plaintiff's marks in the metatags of the defendant's websites, since the metatags properly identified the services referenced on the defendant's websites). *But see J.K. Harris & Co LLC v. Kassel*, 253 F. Supp. 2d 1120, 1126 (N.D. Cal. 2003) (defendants' use of trade name "J.K. Harris" to refer to the tax representation service was not actionable because all three elements of *New Kids on the Block* test were met (see discussion of the *New Kids on the Block* test, established in 971 F.2d 302 (9th Cir. 1992), in this paper in connection with the initial interest confusion standard, under the subheading "Meta-Tags.")).

© 2004 Piper Rudnick LLP. All Rights Reserved.

In May 1999, *Time Magazine* reported that approximately five million domains had been registered worldwide, of which eighty-five percent were ".com" domains.[89] It took four years to register the first one million domain names but only three months to go from four million to five million domain names.[90] Now there are 368,200 new domain names being registered each week,[91] and at the end of 2002, there were over 28.1 million domain names registered in the *.com*, *.org*, and *.net* gTLDs, and an additional 1.8 million registered domain names in the *.biz and .info* registries.[92] On November 16, 2000, ICANN announced that it had tentatively approved seven new generic top-level domain names (gTLDs), including *.aero*, *.biz*, *.coop*, *.info*, *.museum*, *.name*, and *.pro*. Of these seven, three - *.biz*, *.info*, and *.name* – are available to the public at large; the others are for use by individuals and organizations that qualify: *.aero* is intended for airlines as well as the aircraft and aeronautics industries; *.coop* is to be used by cooperatives; *.museum* is to be used by museums and similar organizations; and *.pro* is reserved for persons and firms operating in certain professions. The new gTLD's *.biz*, *.info*, and *.name* gTLD's were made available, starting with a sunrise period that opened in Fall 2001, to afford trademark owners a period within which to register their names before these gTLD's are opened up to the public. Inevitably, disputes involving the new gTLDs have already come before ICANN dispute resolution panels.[93]

Monitoring domain name use and handling disputes over domain names have proven to be a major issue for most companies. In the U.S., actions can be brought under the Anticybersquatting Consumer Protection Act, which took effect November 29, 1999.[94] Under this standard, among other things, the trademark owner must prove that the domain name was registered or used in "bad faith." The statute provides nine examples of the factors that courts may consider in assessing whether or not bad faith is present. The ACPA applies to foreign

---

[89] Paul Beban, *Master of Your Domain*, Time Magazine, May 17, 1999, available at 1999 WL 15941149.

[90] The Industry Standard, Sept. 20, 1999, at 208. *See Worldsport Networks Limited v. Artinternet S.A.*, 1999 WL 269719 (E.D. Pa. 1999).

[91] L. Carr, *Metrics: 100 Numbers You Need to Know*, TheStandard.com (Nov. 13, 2000) citing Network Solutions, Nov. 2000.

[92] SnapNames: State of the Domain Total Registrations per gTLD (Q4 2002) (available at *https://www.sotd.info/content/documents/total_registrations.pdf*, visited April 7, 2003).

[93] *See, e.g., STMicroelectronics Inc v. Stefano Trabalza*, Nat. Arbitration Forum Claim No. FA0110000100637 (Dec. 18, 2001) (decision available at *http://www.arbforum.com/domains/decisions/100637.htm*). WIPO reported in February 2002 that in 2001, it had already handled cases involving domain names with extensions in the *.biz*, *.info*, and *.name* gTLD's, as well as numerous cases in ccTLD's. *See* WIPO Press Release PR/2002/303, available at *http://*www.*wipo.int/pressroom.en/releases/2002/p303.htm.*

[94] Pub. L. 106-113, § 1000(a)(9) (incorporating by reference S. 1948), codified at 15 U.S.C. § 1125(d).

© 2004 Piper Rudnick LLP. All Rights Reserved.

trademarks used in U.S. commerce[95] as well as U.S. trademarks.[96] But the ACPA may not be used to enforce foreign trademark rights.[97] In a successful ACPA action for a domain name that was registered, used, or trafficked in after the Act took effect, the plaintiff can be awarded a transfer of the domain name, statutory damages ranging from $1,000 to $100,000 per domain name infringed, and legal fees.[98] In *Electronics Boutique Holdings Corp. v. Zuccarini*,[99] the court assessed the full range of penalties with respect to a repeat cybersquatter, including $500,000 in statutory damages and over $30,000 in legal fees.

The ACPA also provides for the possibility of *in rem* jurisdiction, where the plaintiff cannot locate the domain name registrant (*e.g.*, where the registrant gave incorrect contact information to the registrar or did not update the contact information on file), or where the registrant can be located but is not subject to the *in personam* (personal) jurisdiction of U.S. courts.[100] Under the *in rem* clause, the lawsuit is to be filed against the domain name itself.

---

95 *See International Bancorp, LLC v. Societe Des Bains De Mer et Du Cercle des Etrangers a Monaco*, No. 02-1364 (4th Cir. May 19, 2003) (upholding claim against European casino that advertised in U.S.).

96 *See Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona*, 2003 U.S. App. LEXIS 10840 (4th Cir. June 2, 2003) (ACPA and U.S. trademark law apply to dispute involving claim by Barcelona (Spain) city council against two residents of Spain who formed a Delaware corporation, Barcelona.com, Inc., reversing lower court and UDRP panel).

97 *Id*. The Fourth Circuit ruled that the ACPA explicitly requires application of the Lanham Act, not foreign law. The district court's reliance on Spanish trademark law was found erroneous.

98 In *Ernest and Julio Gallo Winery v. Spider Webs Ltd.*, 129 F. Supp.2d 1033, 1047-48 (S.D. Tex. 2001), *aff'd*, 286 F.3d 270 (5th Cir. 2002), the court awarded statutory damages of $25,000 for violations of the ACPA and the Texas Anti-Dilution Statute. The court noted that even though the domain name had been registered before the ACPA took effect, the defendants (who warehoused nearly 2000 domain names) used and trafficked in the domain name after the ACPA's November 29, 1999 effective date. *Id*. On appeal, the U.S. Court of Appeals for the Fifth Circuit affirmed, and in doing so rejected the defendants' argument that it was not acting in bad faith because it was holding the domain name to sell it only if the ACPA was declared unconstitutional. *Ernest and Julio Gallo Winery v. Spider Webs Ltd*., 286 F.3d 270 (5th Cir. 2002); s*ee also Virtual Works, Inc. v. Volkswagen of Am., Inc.*, 238 F.3d 265, 268 (4th Cir. 2001) (same).

99 56 U.S.P.Q.2d (BNA) 1705 (E.D. Pa. 2000), *motion to set aside denied*, 2001 U.S. Dist. LEXIS 765 (E.D. Pa. 2001). *See also Victoria's Cyber Secret v. V Secret Catalogue, Inc.*, 161 F. Supp.2d 1339 (S.D. Fla. 2001) ($120,000 plus legal fees and transfer of four domain names). *See also* the discussion, *infra*, in this heading concerning the Federal Trade Commission's action under the FTC Act against a cybersquatter, John Zuccarini, where the court awarded $1,897,166 million. *See FTC v. Zuccarini*, 2002 U.S. Dist. LEXIS 13324 (E.D. Pa. April 10, 2002).

100 15 U.S.C. § 1125(d)(2). *See, e.g., Alitalia-Linee Aree Italiane, S.p.A v. Casinolitalia.com*, 128 F. Supp.2d 340 (E.D. Va. 2001) (*in rem* case can only be brought if *in personam* jurisdiction cannot be obtained in U.S.)

© 2004 Piper Rudnick LLP. All Rights Reserved.

Jurisdiction is typically in the district where the registrar or registry is located.[101] *In rem* jurisdiction continues to exist once determined.[102] The *in rem* clause has withstood several challenges to its constitutionality.[103] In an *in rem* action, the plaintiff usually is required to establish the registrant's bad faith,[104] and if the action is successful, the court will order that the domain name in question be transferred, but the court cannot assess monetary damages. *In rem* actions also require the plaintiff to meet the publication requirements to perfect service of process under the ACPA.[105] Trademark infringement and dilution claims may also be brought in connection with an *in rem* ACPA lawsuit.[106]

In addition to the ACPA, there is also the option of initiating action under the Uniform Domain Name Dispute Resolution Policy ("UDRP"), effective January 3, 2000, which also covers domain name disputes.[107] The Internet Corporation for Assigned Names and Numbers

---

[101] *See, e.g., Mattell, Inc. v. Barbie-Club*.com, 2002 U.S. App. LEXIS 23149 (2d Cir. 2002); *Fleetboston Financial Corp. v. fleetbostonfinancial.com*, 138 F. Supp.2d 121 (D. Mass. 2001).

[102] *See, e.g., Porsche Cars North America, Inc. v. Porsche.net*, 302 F.3d 248 (4th Cir. 2002).

[103] *See, e.g., Cable News Network LP v. cnnnews.com*, 162 F. Supp.2d 484 (E.D. Va. 2001). *Cf. Parents Choice Foundation v. parentschoice.com*, No. 02-223-A (E.D. Va. filed Feb. 21, 2002) (domain name successfully transferred in court where registry is located, through settlement with Hong Kong-based registrant that used Canadian registrar).

[104] *See, e.g., Cable News Network LP v. cnnnews.com*, 2001 U.S. Dist. LEXIS 21388 (E.D. Va. 2001) (on remand); and *Harrods Ltd. v. Sixty Internet Domain Names*, 302 F.3d 214 (4th Cir. 2002); *but see Jack in the Box Inc. v. jackinthebox.org*, 143 F. Supp.2d 590 (E.D. Va. 2001) (demonstration of bad faith not necessary in an *in rem* action).

[105] *See, e.g., Cable News Network LP v. Cnnnews.com*, 162 F. Supp.2d 484 (E.D. Va. 2001) (publication in Chinese and English in Hong Kong newspapers); *Shri Ram Chandra, Mission v. Sahajinorg.org*, 139 F. Supp.2d 721 (E.D. Va. 2001) (publication in India Abroad, India Abroad Online, and The Washington Post). In an *in rem* case involving a domain name that was registered through a Korean registrar, the U.S. District Court for the Eastern District of Virginia ordered a transfer even though the cybersquatter, who had defaulted in the U.S. *in rem* suit, obtained an order from a Korean court to prevent the Korean registrar from transferring the name. *GlobalSantaFe Corp. v. Globalsantafe.com*, 250 F. Supp. 2d 610 (E.D. Va. 2003).

[106] *Harrods Ltd. v. Sixty Internet Domain Names*, 302 F. 2d 214 (4th Cir. 2002). However, dilution claims may be tougher to prove after the U.S. Supreme Court's holding in *Moseley v. V Secret Catalogue, Inc*., 123 S. Ct. 1115 (2003), in which the Court found that the Federal Trademark Dilution Act, 15 U.S.C. § 1125(c), requires that evidence of actual dilution must be proven, instead of proving the likelihood that dilution had or would occur. *See also Voice-Tel Enters., Inc. v. JOBA, Inc*., 258 F. Supp.2d 1353, 1363 (N.D. Ga. 2003) (absent evidence of harm to franchisor's mark, court dismissed claim that its marks were diluted by a franchisee; moreover, the court declined to conclude that a hyperlink to an offending site was actionable under the dilution standard).

[107] For an example of the dispute policies outside the U.S., see the policy adopted by Nominet, the registrar of U.K. domain names, at *http*://www.*nic.uk.*

© 2004 Piper Rudnick LLP. All Rights Reserved.

(ICANN) established the UDRP to deal with domain name disputes. The ICANN dispute resolution process is global in perspective and can be invoke to address domain name registrants not located in the U.S., as well as domain names registered under certain country-code top-level domain names (ccTLD's) that have agreed to abide by the UDRP (registrars of ccTLD's are not required to follow the UDRP, but some do). The UDRP recognizes that in some cases a trademark owner has priority rights over a domain name owner. For a trademark owner to prevail,[108] the trademark owner must establish three elements that: (1) the contested domain name is identical or confusingly similar to a trademark or service mark to which they have rights;[109] (2) the current holder has no rights or legitimate interests in the domain name; and (3) the domain name was registered, and is being used in bad faith.[110] Proceedings under the UDRP are quick and awards are limited to orders that the domain name in question be transferred. Approximately three-quarters of the rulings issued thus far have been in favor of the trademark owner.[111] These proceedings are in the nature of arbitration; however, federal courts have ruled that they are not conducted in such a manner as to have the shield ordinarily accorded under the Federal Arbitration Act.[112] In fact, an arbitral decision rendered under the UDRP is subject to judicial review pursuant to the terms of the UDRP itself;[113] a conclusion that has been confirmed by the federal courts.[114] As such, the ACPA may be used to overturn an UDRP decision on a

---

[108] It goes without saying that ICANN proceedings should be brought by the actual trademark owner. In *NBA Properties, Inc. v. Adirondack Software Corp.,* WIPO No. D-2000-1211 (Dec. 8, 2000), the arbitration panel refused to transfer the domain name *knicks.com* citing, among other reasons, that the trademark *Knicks* was not owned by NBA Properties (a licensee for limited purposes), but, rather, by Madison Square Garden, L.P.

[109] *See, e.g., Lundy v. Idmaond*, WIPO No. D2001-1327 (Feb. 14, 2002) (in which the Panel refused to order a transfer a domain name after the Panel it found, *inter alia*, that the complainant (Marvin Lundy) "failed to establish common law service mark rights" in the law firm name Marvin Lundy).

[110] In a case involving non-use, and mere registration of a domain name, an ICANN panel deemed the registration tantamount to bad faith under the UDRP where the registered name was widely know (here, the name Mario Lemieux, a NHL Hall of Fame player), there was no showing a good faith use of the name by the registrant, and there was no demonstrable legitimate use of the name by the registrant. *Lemieux v. Creato*, eResolution No. AF-0791, May 24, 2001 (decision found at *http://www.disputes.org/eresolution/decisions/0791.htm)*.

[111] *See* ICANN website statistics at *http://www.icann.org/udrp/proceedings-stat.htm.*

[112] *See Dluhos v. Strasberg,* 321 F.3d 365 (3d Cir. 2003); *Parisi v. Netlearning, Inc.*, 139 F. Supp.2d 745, 751-52 (E.D. Va. 2001).

[113] UDRP, ¶ 4(k).

[114] *Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona*, 2003 U.S. App. LEXIS 10840 (4th Cir. June 2, 2003); *Sallen v. Corinthians Licenciamentos Ltda*., 273 F.3d 14 (1st Cir. 2001); *Weber-Stephen Products Co. v. Armitage Hardware and Building Supply, Inc*., 2000 U.S. Dist. LEXIS 6335 (N.D. Ill. 2000). *Cf. Storey v. Cello Holdings, LLC*, 182 F. Supp. 2d 355 (S.D.N.Y. Jan. 23, 2002) (the final disposition of a trademark infringement case – here, dismissal with prejudice – serves as a decision on the merits in favor of the defendant, and precludes the filing of an arbitration proceeding under the UDRP).

© 2004 Piper Rudnick LLP. All Rights Reserved.

disputed domain name and obtain the return of a wrongfully transferred domain name. In 2004, Nike, Inc. brought an ACPA action to recover a domain name (www.justdoit.net) that Nike alleged had infringed on its "Just Do It" mark, after an WIPO panel had earlier refused to transfer the domain name because it found a lack of the "bad faith" needed to rule on Nike's behalf.[115]

In yet another arena, the Federal Trade Commission filed a complaint against John Zuccarini, an infamous cybersquatter, alleging three violations of Section 5 of the FTC Act.[116] After issuing a temporary restraining order against Zuccarini, and finding that the defendant attempted to evade service of process and transferred or concealed evidence, the court subsequently entered a preliminary injunction against Zuccarini, which among other things, ordered Zuccarini to discontinue operating certain websites, ordered a freeze on his registration and pseudonymous use of domain names,[117] imposed an asset freeze, redirecting persons to his websites, or otherwise "obstructing consumers on the internet or World Wide Web." His practice of obstructing consumers from exiting his websites was viewed as a deceptive and unfair practice. The court awarded $1,897,166 million for equitable monetary relief, imposed record-keeping and document retention requirements on Zuccarini and imposed notification requirements on Zuccarini respecting his domain name registration. *See FTC v. Zuccarini*, 2002 U.S. Dist. LEXIS 13324 (E.D. Pa. Apr. 10, 2002).

Mr. Zuccarini also has the dubious distinction of being the first person charged, convicted, and sentenced to prison under a federal law that makes it illegal to use a misleading domain name to deceive a person into viewing obscene material.[118] That law, colloquially called the "Truth in Domain Names" Act (passed in 2003 as part of the federal "Amber Law"

---

[115] *Nike, Inc. v. Circle Group Internet*, 2004 U.S. Dist. LEXIS 9341 (N.D. Ill. 2004) (the prior ruling, WIPO No. D2002-0544, is available at *http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0544.html*).

[116] *FTC v. Zuccarini*, 2002 U.S. Dist. LEXIS 13.

[117] A German court, however, struck down the long-standing use of a pseudonym by a domain name registrant that precluded a person from registering and using his own last name. *See Domain Using Owner's Pseudonym Infringed Rights of Person with Identical Given Name*, 8 E. Com. & L. Rep. 27, at 695 (July 16, 2003) (reporting on *Maxem v. Maxem, Bundesgerichtshof*, No. 1 ZR 296/00, decided June 26, 2003).

[118] 18 U.S.C. § 2252B. *See also* Benjamin Weiser, *Spelling It Dinsey, Children on Web Got XXX*¸ The New York Times, Sept. 4, 2003 (reporting on Mr. Zuccarini's arrest under the new law with respect to his registration and use of domain names that include typographical misspellings of popular names). Apparently, the criminal complaint cited Mr. Zuccarini's admissions in prior cybersquatting suits brought by the FTC and private parties with respect to his practice of buying typographically similar domain names and redirecting them, as well as his admission that he "mousetrapped" browsers. Mark Hamblett, *First Charges Filed under New Internet Porn Law*, 1 Internet L. & Strat. 9, at 3 (Sept. 2003). On February 26, 2004, a federal judge sentenced Mr. Zuccarini to 30 months in prison after he plead guilty to the charges against him. Press Release, U.S. Attorney for the Southern District of New York, *Cyberscammer Sentenced to 30 Months for Using Deceptive Internet Names to Mislead Minors to X-Rated Sites* (Feb. 26, 2004) (available at *http://www.usdoj.gov/usao/nys/Press%20Releases/FEBRUARY04/zuccarini%20sentence%20pr.pdf*)

© 2004 Piper Rudnick LLP. All Rights Reserved.

legislation"), is also credited with convincing the owner of the website www.whitehouse.com (a website that directs browsers looking for the Executive Office of the President of the U.S., located at www.whitehouse.gov, to an adult content website instead) to sell that domain name.[119] The federal judge hearing the case sentenced Mr. Zuccarini to 2½ years in prison, ending a criminal prosecution that followed numerous civil efforts to contain Mr. Zuccarini's recidivism as a cybersquatter and evasion of court orders.[120]

On September 3, 2001, the World Intellectual Property Organization (WIPO) issued its second report on cybersquatting, entitled the "Report of the Second WIPO Internet Domain Name Process: The Recognition of Rights and the Use of Names in the Internet Domain Name System."[121] The second report addressed, among other things, problems with cybersquatting involving non-proprietary names for pharmaceutical substances, names of intergovernmental organizations, personal names, geographic identifiers, and trade names in general. WIPO's first report, issued in April 1999, led to the adoption of the UDRP later that same year. The second report proposes changes that even further clamp down on the practice of cybersquatting. It is likely that the second report will lead to changes in the law and that it will ultimately have as significant an impact as did the adoption of the UDRP in 1999 after the first WIPO report.

---

[119] Dana Milbank, *Curtain Goes Up on Glass-House Attack*, The Washington Post, Feb. 15, 2004, at A4.

[120] *See* Lewis, *New York Federal Court Sends 'Typosquatter' to Prison*, Legal Times, Oct. 18, 2004, at 28.

[121] The report is available at *http://wipo2.wipo.int.*

© 2004 Piper Rudnick LLP. All Rights Reserved.

CRITICAL WEBSITES OR CYBERSMEARING

Any person or organization with a computer connected to the internet can "publish" information. One problem with the internet is that disgruntled employees and unhappy customers can establish websites that are critical of companies and the products and services they sell, whether or not such criticism may be warranted. The internet gives everyone an inexpensive, broad-reaching, semi-permanent, and largely unregulated public soapbox to talk about companies, their products, brands and services.

Critical websites are protected by the First Amendment and may prove very hard, if not impossible, to shut down. In *Bally Total Fitness Holding Corp. v. Faber*, 29 F. Supp.2d 1161 (C.D. Cal. 1998), Bally brought suit against Faber with respect to his "Bally Sucks" website. Bally sued Faber for trademark infringement, unfair competition and trademark dilution. The court ruled against Bally, finding that the goods and services offered by Faber were unrelated to Bally's goods and services and that no consumer would confuse the source of the "Bally Sucks" website. Faber's use of the Bally's mark was also found to be non-commercial and the court declined to conclude that his use of the Bally mark tarnished that mark. The court observed as well that Faber's use was in the nature of a consumer commentary protected by the First Amendment.

Other recent cases involving critical websites suggest that obtaining injunctions against the operators of such websites is extremely difficult. In *Taubman Co. v. Webfeats*,[122] the U.S. Court of Appeals examined a complaint website operated and accessible through various "sucks" domain names, including taubmansucks.com. The defendant asserted that its operation of these sites, and use of the "sucks" domain names, was an expression of Free Speech entitled to protection under the First Amendment. The appeals court reversed the lower court's injunction against the use of the domain names, writing that:

> Mishkoff's use of Taubman's mark in the domain name "taubmansucks.com" is purely an expression of Free Speech and the Lanham Act is not invoked. And although economic damage might be an intended effect of [defendant's] expression [of Free Speech], the First Amendment protects critical commentary when there is no confusion as to source, even when it involves the criticism of a business. … Taubman concedes that Mishkoff is 'free to shout Taubman Sucks! from the rooftops. Essentially, this is what he has done in his domain name. The rooftops of our past have evolved into the internet domain names of our present.

In *SNA, Inc. v. Array*,[123] the court refused to enjoin a website operator's statements, holding that damages are a proper remedy for past statements and an injunction against future

---

[122] 319 F.3d 770 (6th Cir. 2003). See also *J.K. Harris & Co LLC v. Kassel*, 2003 U.S. Dist. LEXIS 6022 (N.D. Cal. Mar. 28, 2003) (nominative fair use of the tradename "J.K. Harris" on a consumer complaint site was not actionable).

[123] 51 F. Supp.2d 542, 547 (E.D. Pa. 1999)

© 2004 Piper Rudnick LLP. All Rights Reserved.

speech would be an unconstitutional prior restraint. In *Lucent Technologies, Inc. v. Lucentsucks.com,*[124] the district court commented on Lucent's legal difficulty in challenging a critical website that might be able to show it was either an effective parody or a forum for critical commentary. In either case the district court noted the elements for trademark infringement and trademark dilution claims are seriously undermined. In *CPC Int'l, Inc. v. Skippy Inc.*, the Court of Appeals for the Fourth Circuit noted that if a trademark owner could shield itself from criticism about itself and its business practices by a website owner, a corporation could forbid the use of its name in commentaries critical of its conduct.[125]

However, in *People for the Ethical Treatment of Animals, Inc. v. Doughney,*[126] the district court dismissed a First Amendment defense, observing that the defendant contended that the case was brought to "quash his First Amendment rights to express disagreement with their organization." The court noted that:

> PETA does not seek to keep Doughney from criticizing PETA. They ask that Doughney not use their mark. When Network Solutions, Inc. placed "PETA.ORG" on 'hold' status, Doughney transferred the entire web page to one of his other internet sites, 'mtd.com/tasty.' PETA has not complained about that web site and even concedes that Doughney has a right to criticize PETA or any organization.[127]

---

[124] 2000 U.S. Dist. LEXIS 6159 (E.D. Va. 2000). After this procedural decision, Lucent refiled the case. In that proceeding, the defendant moved to dismiss the claim on the basis that "yourcompanysucks.com" domain names are entitled to a safe harbor under the First Amendment to the U.S. Constitution. The court denied that motion. *Lucent Technologies, Inc. v. Johnson*, 56 U.S.P.Q.2d 1637 (C.D. Cal. 2000). *Cf. Wal-Mart Stores Inc. v wallmartcandadasucks.com*, WIPO No. D2000-1104 (Nov. 23, 2000) (in an ICANN UDRP proceeding, the panel denied the applicant's request to transfer allegedly infringing domain name).

[125] *CPC Int'l, Inc. v. Skippy Inc.*, 214 F. 3d 456 (4th Cir. 2000). *See also L.L. Bean, Inc. v. Drake Publishers, Inc.*, 811 F.2d 26, 31 (1st Cir. 1987) ("Since a trademark may frequently be the most effective means of focusing attention on the trademark owner or its product, the recognition of exclusive right encompassing such use would permit the stifling of unwelcome discussion.").

[126] *People for the Ethical Treatment of Animals, Inc. v. Doughney*, 113 F. Supp.2d 915, 921 (E.D. Va. 2000) *aff'd*, 263 F.3d 359 (4th Cir. 2001). For other "issue oriented" cybersquatting cases, *see also Morrison & Foerster LLP v. Wick*, 94 F. Supp. 1125, 1134 (D. Colo. 2000) (involving *morrisonfoerster.com*); *Jews for Jesus v. Brodsky*, 993 F. Supp.282 (D. N.J. 1998), *aff'd mem.*, 159 F.3d 1351 (3d Cir. 1998) (involving *jewsforjesus.com*); *Planned Parenthood Fed. of Am., Inc. v. Bucci*, 42 U.S.P.Q.2d (BNA) 1430 (S.D.N.Y. 1997), *aff'd mem.*, 152 F.3d (2d Cir.), *cert. denied*, 199 S. Ct. 90 (1998) (involving *plannedparenthood.com*).

[127] *People for the Ethical Treatment of Animals, Inc. v. Doughney*, 113 F. Supp.2d at 921, *aff'd*, 263 F.3d 359 (4th Cir. 2001).

© 2004 Piper Rudnick LLP. All Rights Reserved.

However, in many instances, even obtaining damages may be difficult. In *Nicosia v. DeRooy*,[128] the website operator published derogatory comments, including statements that the plaintiff was a "fraud" and a "criminal" who had embezzled funds from third parties, on her personal website and through internet discussion groups. The court held that the website operator's comments had to be considered in context to determine whether they were assertions of fact or opinion. After reviewing the defendant's website and associated links, the court determined that the defendant's statements did not amount to defamation because they were mere hyperbole or because the defendant had included links to information on her website that supported her conclusions, even if she was wrong. In another case, *Bihari v. Gross*,[129] the court found that the purpose of the defendant's websites was to injure the plaintiff commercially. However, because the websites concerned the business practices and alleged fraud of a well-known interior designer, it found such speech to be " 'arguably within the sphere of legitimate public concern,' which imbues the speech with a heavy presumption of constitutional protection."[130]

Another aspect of this problem is that on the internet, each entity or individual with a website is a publisher. Some website owners use the internet to publish the specifics of their disputes. This includes publishing letters (often demand letters) and pleadings in lawsuits on their websites. Thus, the internet may make the risk of adverse publicity associated with disputes much greater by providing worldwide access to the adverse information, exacerbated by the website owner's spin to place the information in the worst light possible. Once the content is posted to the internet, it is available to most other internet users worldwide. Placing the content under the confidentiality provisions of a subsequent settlement agreement may be wholly ineffective, especially to the extent the content has been included on third-party mirror websites over which neither party has any relationship.

Traditional defamation law also plays an important role in connection with online postings that are defamatory or libelous. For example, in December 2001, a jury in California awarded $245,000 in actual damages, and suggested the possibility that punitive damages might also be awarded, in a case brought by a company and two of its managers against two disgruntled

---

[128] 72 F. Supp.2d 1093, 1101 (N.D. Cal. 1999).

[129] 119 F. Supp.2d 309, 325-26 (S.D.N.Y. 2000).

[130] *Id.* In *Nissan Motor Co. Ltd. v. Nissan Computer Corp*., 231 F.Supp.2d 977 (C.D. Cal. 2002), the court addressed a dispute between Nissan Motor Co. and a computer company operated by Mr. Uzi Nissan involving the domain names Nissan.com and Nissan.net. The court entered an order allowing the names to be used by the defendants, but permanently enjoining the defendants from including certain content on the website (commercial content, advertising, links to other websites, disparaging remarks or negative commentary about Nissan Motor Co., or links to other sites with such disparaging commentary), reasoning that such content would exploit the goodwill of the "Nissan" mark in order to injure Nissan Motor Co.

© 2004 Piper Rudnick LLP. All Rights Reserved.

former employees.[131] In *Mathis v. Cannon*, the Georgia Court of Appeals found certain messages posted in an internet chat room to be libelous *per se* and further concluded that punitive damages were not avoided by failure to demand a retraction, as the court determined that the retraction rules do not apply to internet postings.[132] Libel cases regarding the Internet appear to be increasing.[133]

Companies go to great lengths to protect their e-brands from derogatory references. Wal-Mart Stores, for example, has requested registration for more than 200 anti-Wal-Mart names.[134] Bell Atlantic's experience when it changed its corporate name to *Verizon* illustrates how difficult, if not impossible, it is to preempt the domain names for these critical websites. Bell Atlantic reportedly filed more that 650 domain names relating to "verizon.com" including "verizonsucks.com." However, others registered the domain name "verizonreallysucks.com" and the domain name "VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com."[135] Critical websites will be more difficult to preempt as new upper level domain registries are added.

Some vendors are now including an express prohibition against publishing disparaging remarks in their Acceptable Use Policies in their web hosting, Application Service Provider and other agreements where Acceptable Use Policies are applicable.

---

[131] Shannon Lafferty, *California Internet Libel Suit Yields Big Verdict*, The Recorder (Dec. 14, 2001) (*http://www.law.com*). A similar result was obtained in a French lawsuit brought by Disneyland Paris, which discovered a website (*http://fuckmickey.multimania.com* – which is no longer active) on which there appeared photos of Disney employees, altered to depict the employees in pornographic scenes and otherwise in an unflattering manner. A French court (the Tribunal of First Instance of Meaux) assessed damages against the website's creator, on grounds of libel and insult. *La Soceiete Eurodisney S.C.A.* (T.G.I. Meaux, No. LJ4410, Nov. 23, 2001).

[132] 252 Ga. App. 282, 556 S.E.2d 172 (Ga. Ct. Apps. 2001).

[133] *See generally Van Buskirk v. The New York Times Co*., 325 F.3d 87 (2d Cir. 2003); *J. K. Harris & Company, LLC v. Kassel*, 253 F.Supp.2d 1120 (N.D. Cal. 2003); *Jane Doe v. Oliver*, 2003 Conn. Super. LEXIS 1498 (Conn. Sup. Ct. May 19, 2003).

[134] D. Streitfeld, *Making Bad Names for Themselves*, The Washington Post, Sept. 8, 2000, at A1, A30.

[135] *Id*. In *Ford Motor Co. v. 2600 Enterprise*, 177 F. Supp.2d 661 (E.D. Mich. 2001), the court denied Ford's motion for a preliminary injunction because it failed to show that defendant's use of the domain name *fuckgeneralmotors.com*, which was linked to *Ford.com*, satisfied the commercial use requirements for trademark dilution, trademark infringement, or unfair competition.

© 2004 Piper Rudnick LLP. All Rights Reserved.

INTELLECTUAL PROPERTY

Intellectual property rights exist on the internet. Intellectual property owners need to protect their intellectual property rights so they do not inadvertently forfeit or otherwise lose any rights in connection with their internet activities. Conversely, e-commerce businesses and other internet users need to appreciate the existence of third-party intellectual property rights and possible liability resulting from the infringement, misappropriation or violation of these third-party rights. Intellectual property is the "web's war zone."[136] Whole industries have their futures dependent on the outcomes of these intellectual property battles.

These intellectual property considerations involve copyright, patent, trademark and trade secret law to one extent or another. Probably the most misunderstood intellectual property law risk concerns the copyright laws. Many information products and other materials available from websites are protected by copyright. This is the case irrespective of whether the materials actually bear a copyright notice. Copying is inherent in the nature of the internet medium and pervades virtually every activity such as browsing, linking, caching, accessing information and operation of an online service. Posting materials on the web is considered a public display implicating the exclusive copyright right to display a work publicly.[137] Since copyright rights vest automatically in the author by operation of law from the moment of creation and fixation in tangible media, the author of the materials has a copyright in and to the materials without regard to whether copyright rights were sought and irrespective of whether the materials include a copyright notice. The prudent strategy is to assume that copyrightable subject matter found on the internet is subject to the exclusive rights of a copyright holder.

Much of the material on the internet will be subject to use agreements that may govern what can and cannot be done with the materials available over the internet. Except as specifically covered by website use agreements, much of the material on the internet can be analogized to shareware. Users have an implied license to download and copy the material for their own use but not to use the material to create derivative works or to distribute the material commercially.

Many company internet policies provide that materials on the internet should be considered to be copyrighted works unless otherwise specified. Thus policies often prohibit employees from downloading such materials and/or modifying such files without the permission of the copyright holder.

---

[136] T. J. Mullaney and Spencer E. Ante, *Info Wars*, Bus. Week, e.biz Section, at EB 107 (June 5, 2000).

[137] *Getaped.com, Inc. v. Cangemi*, 188 F. Supp.2d 398 (S.D.N.Y. 2002) (website deemed a publication for copyright purposes). In *New York Times Company, Inc. v. Tasini*, 121 S. Ct. 2381 (2001), the U.S. Supreme noted the Copyright Office Register's argument that the electronic databases including the infringing freelance articles publicly display the articles. In denying copyright compilation protection to the individual articles the Court emphasized that when a user conducts a search for an electronic database each article appears as a separate item within the search result.

© 2004 Piper Rudnick LLP. All Rights Reserved.

There also needs to be a recognition of the risks of contributory infringement arising from linking to other sites or encouraging users to visit other sites, or in connection with facilitating the infringement or misappropriation of someone else's intellectual property on the internet.[138]

It is important to make sure that trade secret information is not posted on the internet without being secured. Trade secret rights may be lost once the information is posted on the internet. Security measures should be employed to avoid publication. Such precautionary measures include encryption, firewalls, intrusion detection, network monitoring, filtering and internet usage policies as part of an overall trade secret program. Electronic security measures - such as the use of digital certificates - and enhanced physical security measures - such as the use of graphical "passwords"[139] and biometrics[140] to secure individual computers and other devices - will become more prevalent in the next few years. In fact, the events of September 11, 2001 will only serve to hasten the use of biometrics as a means to enhance the reliability of id cards and to combat identity theft. An article in The New York Times suggested that "[s]tirred by charges that a Virginia public notary helped one or more of the Sep. 11 hijackers obtain fraudulent ID's, the National Notary Public Association is urging its members to put their own thumbprints and their clients' thumbprints on all transaction documents."[141]

Trademark usage on the Web should conform to common trademark usage rules. Trademarks used on websites should be designated with the "TM" or "®" symbols as appropriate, with notice of the trademark owner. There is a tendency on the Web not to clutter websites with legal notices. This may prove fatal to recovery of trademark infringement damages. One recent case sought to deny a well-known trademark owner damages from a website that used a counterfeit trademark because the trademark owner had not given notice that its trademark was registered.[142]

Another issue with trademarks on the internet concerns licensed trademarks. Trademark owners need to make sure that their licensed trademarks are being used solely for the purposes

---

138 *See, e.g., Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp.2d 1290 (D. Utah 1999) (links result in liability for contributory infringement).

139 *See* Anne Eisenberg, *Instead of a Password, Well-Placed Clicks,"* The New York Times, May 1, 2002, at E7.

140 Biometrics are various automated methods of verifying a person's identity using a person's unique physiological or behavioral characteristics. For a comprehensive review of biometric devices already on the market, as well as biometrics in general, *see* Sally Grotta, *Bio-Keys*, PC Magazine, June 12, 2001, at 163. *See also Biometric fact and fiction: Body-scanning technology has its drawbacks*, The Economist, Oct. 26, 2002, at 12; David Lake, *Aye for An Eye: More Companies are Looking to Retinal and Finger Scans for Better Security*, The Industry Standard, July 23, 2001, at 56; Cynthia Webb, *ID in the Blink of an Eye*, The Washington Post, Mar. 9, 2001, at E1.

141 Peter Kilborn, *Your Thumb Here: Newest ID of Choice At Store and on Job*, The New York Times, Feb. 20, 2002, at A1 and A16.

142 *See, e.g., Playboy Enterprises, Inc. v. Universal Tel-A Talk, Inc.*, 1999 WL 285883 (E.D. Pa. 1999).

© 2004 Piper Rudnick LLP. All Rights Reserved.

authorized.[143] Trademark law rewards the vigilant. E-business companies should conduct periodic searches to discover whether its trademarks have been improperly incorporated into websites of unlicensed third parties. Courts have consistently recognized that the use of the internet exacerbates the likelihood of trademark confusion.[144]

E-business methods of doing business patents are an integral part of many business plans. E-business companies are using patents to help them defend their first-to-market positions. The number of business-method patent applications is soaring, from 2821 in 1999 to 7800 in 2000.[145] The number of business-method patents granted has increased from 583 in 1999 to 899 in 2000,[146] but decreased to 433 in 2001 and 492 in 2002. The success rate for such applications in 2001 went down to 45% compared to 70% for all other technologies.[147] Amazon.com's patent infringement lawsuit against BarnesandNoble.com relating to its one-click purchase patent,[148] Priceline's patent infringement suit against Microsoft concerning its online reverse auction patent, and SBH's patent infringement lawsuit against Yahoo! relating to SBH's shopping cart patent suggest that patent rights are very important in e-business. E-business business model patents, or method of doing business patent claims, are quite common and need to be appreciated. Open Market, Inc. has a patent relating to an electronic payment system for ordering merchandise. Cybergold has a patent relating to a system for viewing online advertising. IBM and Microsoft are stockpiling e-commerce business patents. E-commerce patents promise to be even more important in the future to obtaining a first-to-market position and early brand loyalty. Many believe that a strong patent portfolio is necessary in today's highly competitive environment, even if only used for defensive purposes.[149] One reason why business method patents have become important to e-business companies is that once an e-business company goes live in cyberspace, other companies can easily duplicate their innovative

---

143 *See, e.g., Hard Rock Café International (USA) Inc. v. Morton*, 1999 WL 701388 (S.D.N.Y. 1999).

144 *See, e.g., Horseshoe Bay Resort Sales Co. v. Lake Lyndon B. Johnson Improvement Corp.*, 2001 Tex. App. Lexis 5355 (Tex. Ct. App. 2001).

145 *See* "*Raising the Bar on Business Patents*," Bus. Week at 46 (Apr. 2, 2001); *see also* The Intellectual Property Strategist at 8 (Oct. 2000).

146 *Id.* (Bus. Week).

147 John J. Love, "Business Method Patents from Past to Present, Keeping Pace with Today's Emerging Technologies" (Feb. 2002).

148 The U.S. Court of Appeals for the Federal Circuit ultimately lifted the injunction that had theretofore prevented Barnesandnoble.com, Inc. from using a one-click online ordering method. *Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343 (Fed. Cir. 2001), *reversing* 73 F. Supp.2d 1228 (W.D. Wash. 1999) (settlement announced W.D. Wash. Mar. 6, 2002).

149 T.J. Mullaney and S.E. Ante, *Info Wars*, Bus. Week, June 5, 2000, e.biz Section, at EB 107-108.

© 2004 Piper Rudnick LLP. All Rights Reserved.

business model unless patent protection is available. Trade secret protection will not be available to protect transparent e-commerce business models.

In 1999, the American Inventors Protection Act was enacted to give protection to businesses that can show by clear and convincing evidence that they previously were using the patented method of doing business. This statute is difficult to apply but nevertheless it reflects the concern over internet method of doing business patents. There have been no cases filed to date under this statute. Another reaction is the PTO's adoption of a second level of review for these patents as a quality assurance check.

One of the major problems on the internet is the unauthorized use of logos and images including the use of a competitor's name on the site. Some of the unauthorized use includes the use of logos or images in a pornographic context. Domain name abuse is prevalent. Software, music and video piracy is also quite common. These are some of the more common intellectual property problems found on the internet.

Trademark, copyright and other intellectual property legends need to be used with full recognition that each web page is addressable separately. A proprietary rights notice or legend on the home page may not be included on specific pages unless specifically referenced on each applicable page. One approach is to consider including a corporate logo on each page of a website so that there is no confusion as to whom the customer is dealing.[150]

E-business companies should take advantage of the tools that are available today to mark their proprietary content with electronic fingerprints and monitor cyberspace with software agents and bots to determine whether their intellectual property rights are being infringed or abused. One commentator recommends that trademarks and logos used online be purposefully designed to incorporate an electronic fingerprint for purposes of finding them in cyberspace.[151]

A party that permits third-party postings on its website should take advantage of the Digital Millennium Copyright Act's "Safe Harbor" provisions to avoid potential copyright liability for this third party content. Attached at Appendix A is a brief memorandum and sample clause relating to the DMCA notice and takedown safe harbor procedures. These "safe harbor" provisions protect online services providers and have been broadly enforced.[152] For example, eBay avoided liability in connection with sale of unauthorized copies of a film.[153] After designating a copyright agent for DMCA notice, website operators should make sure that the

---

[150] *See, e.g., Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 12907 (C.D. Cal. 2000).

[151] William A. Tanenbaum, *Bricks to Clicks – Special E-Commerce Legal Issues for Taking Brick and Mortar Companies Online*, PLI's Sixth Annual Institute For Intellectual Property Law Conference, Sept. 22, 2000.

[152] *See ALS Scan, Inc. v. RemarQ Communications Inc.*, 239 F.3d 619 (4th Cir. 2001); *CoStar Group, Inc. v. LoopNet, Inc.*, 164 F. Supp.2d 688 (D. Md. 2001).

[153] *Hendrickson v. eBay Inc.*, 2001 U.S. Dist. LEXIS 14420 (C.D. Cal. 2001).

© 2004 Piper Rudnick LLP. All Rights Reserved.

notice designation remains current and accurate to avoid issues respecting the sufficiency of any notice provided.[154]

The DMCA includes very powerful anti-circumvention provisions.[155] E-commerce business models involving copyrighted content should be implemented with these anti-circumvention provisions in mind. These DMCA anti-circumvention provisions provide a legal remedy against persons who (1) circumvent technological protection measures that control access to copyrighted works, (2) manufacture or distribute devices or services that circumvent access controls, or (3) manufacture or distribute devices or services that circumvent a technological measure that effectively protects a right of the copyright owner. The term "circumvent protection afforded by a technological measure" means "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."[156] The DMCA provides the legal framework to support a digital rights management program and enabling technology for many e-commerce business models.

If nothing else, the *Napster* case highlights the critical importance of developing prudent, well-considered intellectual property strategies for e-commerce applications from the start.[157]

---

[154] *See Ellison v. Robertson*, 189 F. Supp. 2d 1051 (C.D. Cal. 2002) (AOL failed to update the contact information for its designated DMCA copyright agent).

[155] 17 U.S.C. §§ 1201 et seq. (enacted Oct. 28, 1998), *see, e.g., Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *RealNetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311 (W.D. Wash. 2000) (settled).

[156] 17 U.S.C. §§ 1201(a)(3).

[157] *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp.2d 896 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 2001 WL 11503 (9th Cir. 2001).

© 2004 Piper Rudnick LLP. All Rights Reserved.

LINKING

Linking is the fundamental navigational technology that has made the internet so successful. A link is simply an instruction to a browser to go to another web page. It serves as a connection between two files. The general view is that by publishing a website, the website publisher makes the site available for linking. However, weblinking agreements are used when the link involves economic considerations and in other situations, especially where the linking party wants protection against any claim for contributory liability, negligent referral, endorsement liability or other liability. The new adage is: *think before you link*. Linking agreements may be advisable in a number of situations. One of those situations is where the linking is to an interior page of a website directly rather than through the website owner's home page.

Deep linking was challenged by Ticketmaster Corp. in *Ticketmaster Corp. v. Microsoft Corp*., No. 97-3055 DDP (C.D. Cal. filed April 28, 1997). Here Ticketmaster alleged that Microsoft's unauthorized links to interior pages of Ticketmaster's site represented a form of "electronic piracy" and alleged Microsoft was "feathering its own nest at Ticketmaster's expense." Ticketmaster complained that Microsoft's site wrongfully linked users directly to the internal page within its website where tickets for local events could be purchased. Ticketmaster's complaint included claims for trademark infringement, trademark dilution, and unfair competition. Ticketmaster brought the suit because Microsoft's deep link allowed users to bypass advertising which was contained on the Ticketmaster home page, thereby decreasing the viewing audience for and effectiveness of Ticketmaster's ads. Ticketmaster viewed Microsoft's deep link as a threat to its advertising revenues.

This *Ticketmaster* case was settled with Microsoft agreeing to stop its direct internal deep link and to link to Ticketmaster's website solely through the home page.[158] However, another Ticketmaster case has suggested that deep-linking may be difficult to stop legally. The *Ticketmaster Corp. v. Tickets.com, Inc.*[159] litigation has also focused on deep-linking. There the district court declined to enjoin Tickets.com from deep-linking to the ticket-purchasing pages of the Ticketmaster website. The law is very unclear today on deep-linking. The propriety will depend on the specific facts. Under these circumstances, linking should only be effected to a website's homepage rather than an internal page without the third-party's consent, especially where there are possible adverse economic consequences to the linked site.

Deep linking may be a concern for other reasons as well. With deep linking the visitor does not enter the website through the front door, *i.e.*, the Home Page. As such, deep linking may result in the user by-passing disclaimers, disclosures and website use agreements.

---

[158] *See* MS, Ticketmaster Bury Hatchet, Wired News Report (Feb. 16, 1999) (and at *http://www.wired.com/news/business/0,1367,17943,00.html*).

[159] *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 4553, 54 U.S.P.Q. 2d (BNA) 1344 (C.D. Cal. 2000); *injunction denied*, *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. 2000), *aff'd*, 248 F. 3d 1173 (9th Cir. 2001).

© 2004 Piper Rudnick LLP. All Rights Reserved.

Linking to sites containing materials, which infringe a third party's intellectual property rights, could subject the linking party to a contributory infringement claim[160] or direct infringement.[161] There is, as well, a potential controversy concerning a claim by a company that it has a patent on the use of hyperlinks on the web.[162]

Reasonable steps should be taken to ensure that websites to which a link is made do not, in turn, contain any content that infringes upon a third party's intellectual property rights. This risk can be allocated under a linking agreement. Another risk management technique is to use disclaimers. These disclaimers would contain a simple disclaimer of responsibility for the content of the linked website, and further explain that the does not constitute a referral or endorsement of any product or service advertised or distributed through the linked website. Often times, the disclaimer will provide in effect that the links are provided solely for informational purposes and as a convenience to customers and visitors and do not constitute an endorsement or referral to the linked company or any of its products and services. These disclaimers are often included in the terms of use agreement for a website.

---

[160] In *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp.2d 1290 (D. Utah 1999), the District Court determined that by virtue of the website links to infringing sites the plaintiff could be liable for contributory infringement and inducement of infringement because browsing a website could constitute copyright infringement. The Court determined that each time the users browsed the linked websites, the users loaded webpages into the random access memory of their computers. A copy of the loaded webpage is cached on the IP server serving the user. *See also Bernstein v. J. C. Penney, Inc.*, 50 U.S.P.Q.2d 1063 (C.D. Cal. 1998) (contributory infringement alleged by virtue of links to other sites containing infringing material). Allegations of contributory infringement were also raised against Google Inc., one of the premiere search engine operators on the internet, which received DMCA notices from the Church of Scientology. The Church's DMCA notices objected to Google's search results that linked the browser to sites that the Church alleged displayed infringing material. Google removed those sites from its search results but instead referred browsers to an index on an internet rights site that displayed the Church's DMCA letter, from which, therefore, browsers could find the very sites to which the Church raised an objection. Margery Gordon, *The Google Way,* Corporate Counsel (July 2002) at 13-14; David Gallagher, *New Economy: A copyright dispute with the Church of Scientology is forcing Google to do some creative thinking*, The New York Times, Apr. 22, 2002, at C4).

[161] *Getaped.com, Inc. v. Cangemi*, 188 F. Supp.2d 398 (S.D.N.Y. 2002) (website deemed a publication for copyright purposes).

[162] *British Telecommunications PLC v. Prodigy Communications Corp.*, No. 7:00-CV-9451 (S.D.N.Y., filed Dec. 14, 2000). The patent at the heart of this lawsuit, U.S. Patent No. 4,783,662, was issued in 1989 an includes an element in which the hyperlink is stored in a central computer. The complaint includes both a claim that the defendant's hyperlinks infringe upon the '662 patent both literally as well as under the doctrine of equivalents. (In an interim ruling in this case, the judge ruled that while the patent covers linking within one computer system, the patent may not extend to cover the internet, which has millions of computers, not just one central computer system. 2002 U.S. Dist. LEXIS 4110 (S.D.N.Y. Mar. 13, 2002).) The application of the doctrine of equivalents in certain cases was validated in *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co. Ltd.*, 122 S. Ct. 1831 (2002), in which the U.S. Supreme Court generally upheld the right of patent holders to rely on the doctrine of equivalents, which must be evaluated on a case-by-case basis. *But see Johnson & Johnson Assocs., Inc. v. R.E. Service Co.*, Nos. 99-1076, 99-1179, 99-1180 (Fed. Cir., Mar. 28, 2002) (doctrine of equivalents cannot be invoked to cover subject matters that were left unclaimed in original claim).

© 2004 Piper Rudnick LLP. All Rights Reserved.

There may be other issues where linking agreements are desirable. When the logo or trademark of the linked-to-party is used, or descriptive text is used regarding the linked-to site or company, a linking agreement is appropriate. There also may be issues requiring the link to be maintained. For example, some regulatory requirements may stipulate that a link be continuously available. Another reason for a linking agreement is that companies may want to document the independent third-party nature of a link to avoid any implication of collusion or concerted action arising from a hyperlink to another site. It may also be desirable to restrict the linked-to-site by agreement from linking to objectionable content that may adversely affect your e-brand, other trademarks or reputation.[163]

Increasingly companies are also adopting policies prohibiting customers from creating or establishing links with their site. eBay, for example, recently prohibited their customers from establishing links. eBay found that customers were using links to avoid paying commissions to eBay. Others are concerned that through the link they will be associated with people, companies, products, content or services they do not want to be associated. It remains to be seen whether courts will enforce such policies in cases of simple, unadorned, and plain-text hyperlinks that do not claim or imply any affiliation between the website where the link is located and the linked site.

---

[163] In *Morrison & Forrester LLP v. Wick*, 94 F. Supp.2d 1125 (D. Colo. 2000), the Court observed that links to Anti-Semitic, racists and other offensive domain names may cause users to be unsure about the website owner's affiliation with the sites or endorsement of the site.

© 2004 Piper Rudnick LLP. All Rights Reserved.

FRAMING

Framing is a variation of linking and may be used in various e-business applications. The practice uses frames to incorporate third-party content into a website. The user may reasonably believe that all information displayed is from the same website. Framing allows the display of the contents of two or more websites on the same web page even though the content is located on different sites. Pages from other websites can be presented as the content of the "framed" website without the casual observer being aware that the "framed" web page is from a different site. Another form of framing is "inlining." Inlining content from other websites is framing without the border around the framed content. The practice of framing has proven quite controversial.

Several cases illustrate the potential liability for framing. In *Washington Post Co. v. Total News*, No. 97-1190 (S.D.N.Y. 1997), Total News hosted a website that provided a list of news services. These services were identified by their respective trademarks. The Total News website also included a content window and an advertising banner. When a user "clicked" on a news service, the content from that news service appeared in the content window for the Total News website. Total News was obtaining advertising revenues based primarily on the content from the news services. The plaintiffs in the *Total News* case (The Washington Post, CNN, Time, The Los Angeles Times, Reuters and Dow Jones) alleged copyright and trademark infringement, false designation of origin under the Lanham Act, and unfair competition. While this case was settled without any definitive court rulings, it does underscore the potential legal liability from framing.

In another framing case, *Futuredontics, Inc. v. Applied Anagramics, Inc.*, 45 USPQ2d (BNA) 2005, 1998 U.S. Dist. LEXIS 2265 (C.D. Cal.), *aff'd*, 1998 WL 417413 (9th Cir. 1998) (unpub. op.), the defendant Anagramics, a dental marketing service, created a website which framed portions of Futuredontics' website. Here Anagramics, the owner of the "1-800-DENTIST" trademark, had licensed the trademark exclusively to Futuredontics but, despite the license, displayed the 1-800-DENTIST mark by framing the Futuredontics' website. Futuredontics sued for copyright infringement and false advertising. In a subsequent action, the U.S. Court of Appeals affirmed the issuance of an injunction against Futuredontics, noting that Futuredontics had ignored the disapproval of a proposed advertisement. Rejecting Futuredontics' claim that it was entitled to engage in free speech, the court noted that "the First Amendment protects free speech only when it concerns lawful activity and is not misleading."[164]

A case brought in Scotland, *Shetland Times, Ltd. v. Jonathan Wills and Another*, 1997 F.S.R. (Ct. Sess. O.H.), 24 October 1996, may have been the first "linking" case, and addressed the problem of "deeplinking." On the Web site for the Shetland News ("News"), several hypertext-link headlines transported the internet user to Shetland Times ("Times") articles on the Times Web site. The transportation of the user to the embedded page on the Times Web site bypassed the Times front page with its advertising, and removed the Times "frame" from view.

---

[164] *Futuredontics, Inc. v. Goodman*, 1999 U.S. App. LEXIS 26257 (9th Cir. Oct. 14, 1999) (not for publication).

© 2004 Piper Rudnick LLP. All Rights Reserved.

The issue in the case was whether "deeplinking" to internal or embedded pages of the Times Web site by the News through the use of the plaintiff Web site's news headlines was an act of copyright infringement under the U.K.'s Copyright Designs and Patents Act of 1988. The plaintiff sought, and received, an injunction precluding such deeplinking. The News appealed this ruling and the matter settled before trial. As part of the settlement, the News agreed to link only through the Times' Web site's front page and agreed to include a legend identifying the headlines as from the Times wherever such headlines were posted on the News' Web site. A similar claim was brought in England in January 2001 by Haymarket Publishing against an oil company, Burmah Castrol, which is alleged to have engaged in unauthorized framing of two of the publisher's websites.[165] In another case, the EU Directive on Copyright and Databases Regulations was invoked by a company that successfully obtained an injunction against deep linking.[166]

Framing may give rise to copyright infringement, violations of the Lanham Act and other potential liability. The content in the outside frame may be objectionable to the owner of the content inside the frame. There are a number of potential legal problems with framing. Framing will distort the accounting for advertising royalties because the users visiting the framed site are not recorded at the content owner's website. Copyright infringement arises because the content is being copied without the copyright owner's permission and this copying is not likely to be viewed as a fair use.

Until the law respecting framing has been settled, framing of other website content should only be undertaken with the express permission of the content owner. In negotiating e-business relationships, the parties should consider whether framing will be authorized and, if authorized, any contractual restrictions to be imposed on the framing.

Attention must also be paid to the risk that others will frame the content of a website without the owner's authorization. E-business is very competitive. Particular vigilance is called for whenever a third party attempts to frame a company's website, for example, to ensure that intellectual property rights are protected adequately.

Framing is one good reason for registering the copyright claims in a website within ninety days of publication. In *Getaped.com, Inc. v. Cangemi*[167] the court ruled that making a website available constitutes a publication for copyright purposes. Timely registration with the

---

[165] *See* Jean Eaglesham, *Publisher sues over web link*, Financial Times, Jan. 10, 2001 (available at *http://*www.*ft.com*).

[166] *See* Jean Eaglesham, *Online recruiter wins ban on rival's web links*, Financial Times, Jan. 17, 2001 (available at *http://*www.*ft.com*) (reporting on injunction obtained by StepStone ASA against OFiA). *See also Imax Corp. v. Showmax Inc.*, [2000] FCJ No. 69 (FCC) (Canada), a 2000 case in which the Federal Court of Canada enjoined framing of the Showmax website.

[167] 188 F. Supp. 2d 398 (S.D.N.Y. 2002). Interestingly, the court determined the HTML code for the website had been published because of the ease with which the HTML code could be read.

© 2004 Piper Rudnick LLP. All Rights Reserved.

Copyright Office enables recovery of statutory damages and attorney's fees for unauthorized framing of a website's content. This strategy is especially important because one of the real problems on the internet is that it is often very difficult to prove actual damages from a third-party's use of content. As such, assuring the recovery of statutory damages and attorneys fees, even if the award of attorney's fees is discretionary and becoming increasingly more difficult to obtain unless the infringement suit or defense is objectively unreasonable, is quite important. A copyright registration strategy for a website will help a company manage this risk of framing and any copyright infringement applicable to its website and the content on that site.

© 2004 Piper Rudnick LLP. All Rights Reserved.

META-TAGS

Meta-tags are embedded in the hypertext markup language (HTML) for websites. These meta-tags are invisible to the user, but may be seen when viewing the HTML source code. Meta-tags are key words inserted by the website designed to describe the site. Search engines use these "keyword" fields to evaluate whether to return a link to the site when a user initiates a search request. The meta keyword tags or invisible tags embedded in the website allow the website designer to manipulate to a certain extent the results a search engine will return in response to a user request. The use of meta-tags has generated litigation.

To date the cases involving meta-tags concern one party using another party's trademark or company name as a meta-tag on their website. In *Playboy Enterprises, Inc. v. Calvin Designer Label*,[168] for example, the defendant was found to have infringed on Playboy Enterprises' rights by embedding references to the term "Playboy" in the HTML coding underlying the defendant's website. Courts have generally been concerned about meta-tags using a competitor's trademarks. In *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*,[169] the Court of Appeals concluded that the defendant's use of another party's trademarks in a website's meta-tags created "initial interest confusion" and, therefore, also violated the Lanham Act. However, in *Bihari v. Gross*,[170] the court reached the opposite conclusion, noting that while the allegedly infringing site used meta-tags that included the plaintiffs' mark, searches that found the site displayed the information from the associated meta-description, which indicated that the website was for the purpose of discussing consumer problems with the plaintiffs business. Understanding "initial interest confusion" is important to assessing trademark infringement and dilution risks in connection with e-commerce. The conclusion in *Brookfield* was echoed in a Seventh Circuit opinion, *Promatek Industries, Ltd. v. Equitrac Corp.*, in which the court concluded that an infringing use of a competitor's name in a metatag was improper, but observed as well that "it is not the case that trademarks can *never* appear in metatags, but that they may only do so where a legitimate use of the trademark is being made."[171] The *Promatek* court observed that "[t]he problem here is not that Equitrac, which repairs Promatek products, use Promatek's mark in its metatag, but that it used that trademark in a way calculated to deceive consumers into thinking that Equitrac was Promatek."[172]

---

[168] 1997 U.S. Dist. LEXIS 14345 (N.D. Cal. 1997).

[169] 174 F. 3d 1036 (9th Cir. 1999). In the *Brookfield* case, the technology and function of meta-tags is explained. *Id*. at 1061-62, n. 23.

[170] 119 F. Supp.2d 309 (S.D.N.Y. 2000). *See also Northland Insur. Cos. v. Blaylock*, 115 F. Supp.2d 1108 (D. Minn. 2000) (refusing to apply initial interest confusion doctrine in case of consumer complaint site).

[171] 300 F.3d 808, 814 n.13 (7th Cir. 2002) (as amended, Oct. 18, 2002) (emphasis supplied).

[172] *Id*. at 814. A similar result was reached in a March 2004 decision handed down by German court, which ruled that the use of a competitor's mark in a website's metatag was an infringing use. *See Competitor's Use of*

(footnote continued to next page)

© 2004 Piper Rudnick LLP. All Rights Reserved.

In *Playboy Enters., Inc. v. Welles*,[173] the court also declined to find that use of another party's trademarks was an infringement. In this case, the defendant, a model who earned the title "Playmate of the Year," used that phrase in her website's meta-tags and elsewhere in the website, which the court found to be a fair usage of the term, since it accurately described the appellation that plaintiff awarded to her. On appeal however, the Ninth Circuit, while agreeing that Welles' use of "playboy" and "playmate" in her metatags and banner ads were merely nominative and non-infringing, found that Welles' repeated stylized use of "PMOY 81" in the background or wallpaper for her site failed the nominative use test.[174]

In an earlier decision, *New Kids on the Block v. News Am. Publishing, Inc.*,[175] the U.S. Court of Appeals set up a three part test to determine when "nominative fair use" was present, under which unauthorized use of another party's trademark would be permitted:

> First, the product or service in question must be one not readily identifiable without use of the trademark; second, only so much of the mark or marks may be used as is reasonably necessary to identify the product or service; and third, the user must do nothing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder.[176]

The *New Kids on the Block* court further explained that "a soft drink competitor would be entitled to compare its product to Coca-Cola or Coke, but would not be entitled to use Coca-Cola's distinctive lettering.[177]

In one meta-tag infringement matter the website for a competitor used a company's marks as keywords as well as a number of keywords that were confusingly similar (virtually identical phonetically) to our client's marks. This meta-tag technique may result in the

---

(footnote continued from previous page)

Rival's Mark As Metatag Held to Be Infringing Use, 9 E. Commerce & L. Rep. (BNA) 30, at 679 (Aug. 4, 2004).

173 7 F. Supp.2d 1098 (S.D. Cal.); *aff'd* 162 F.3d 1169 (9th Cir. 1998); *on remand*, 60 F. Supp.2d 1050 (S.D. Cal. 1999); *summary judgment granted for defendant*, 78 F. Supp.2d 1066 (S.D. Cal. 1999) (distinguishing *Brookfield Communications*). "Much like the subject index of a card catalog, the meta-tags give the web surfer using a search engine a clearer indication of the content of the website." 7 F. Supp.2d at 1104.

174 *Playboy Enterprises, Inc. v. Welles*, 279 F.3d (9th Cir. 2002). *See also PACCAR, Inc. v. TeleScan Technologies, L.L.C.*, 319 F.3d 243 (6th Cir. 2003) (court upheld injunction against use of domain names incorporating plaintiff's trademarks, but upheld rejection of injunction against use of trademarks in metatags).

175 971 F.2d 302 (9th Cir. 1992).

176 *Id*. at 308.

177 *Id*. at 308 n.7. *But see Horphag Research Ltd. v Pellegrini*, No. 01-56733 (9th Cir. May 9, 2003) (excessive and "unreasonably pervasive" use of a competitor's mark was not protected by fair use defense).

© 2004 Piper Rudnick LLP. All Rights Reserved.

competitor's website being returned more often than the trademark owner's site itself. In one reported case, this actually happened. The competitor's website was returned more often than the trademark owner's site based on the use of meta-tags.

Meta-tags are a form of advertising. A website's meta-tags should not mislead site visitors as to the nature of the website. For example, the Federal Trade Commission filed a complaint against a website that included meta-tags relating to cancer on the grounds that meta-tags were deceptive and misleading even though the site's advertising did not claim the herbal products were a cure for cancer.[178]

Meta-tags should be selected carefully with due consideration to potential trademark infringement and deceptive advertising claims. Generic terms should be used, as well as a company's own trademarks (or those of parties with which there is a license for such usage). It is advisable to include specific reference in a trademark license authorizing the licensee to use the licensed trademark in meta-tags. Generally speaking, it is also advisable for companies to avoid using the trademarks or names of competitors.

Using a competitor's name or trademark in the meta-tag key words for a website or in hidden text "stealthing" at the site are just several of the strategies e-competitors are using to divert traffic from one website to another. These include key word advertising,[179] search engine diversions, page jacking, spamdexing, pixel-tagging, cyber-stuffing[180] and mousetrapping.[181] Spamdexing is the practice of placing the trademark in the text of the webpage itself. It is important to be "streetwise" as to the techniques companies are using to divert traffic. Some of these techniques may be legal. Some may not be, especially when viewed in the aggregate. In the aggregate these activities may constitute unfair competition.

---

[178] In *FTC v. Lane Labs USA, Inc.*, No. 00 CV 3174 (D. N.J. June 28, 2000), the FTC challenged the use of embedded words relating to cancer therapy in metatags for shark cartilage product and in *Natural Heritage Enterprises*, C-3941 (FTC May 23, 2000) the FTC challenged the use of meta-tags that represented essiac tea could treat cancer, diabetes and HIV/AIDS.

[179] *See* B. Elgin, *Web Searches: The Fix Is In*, Bus. Week, Oct. 6, 2003, at 89, reporting on the impact of paid inclusion on search engines, browsers, and advertisers.

[180] Cyber-stuffing is the practice of repeating a term numerous times in a website's meta-tags in order to lure the attention of Internet search engines. *Trans Union LLC v. Credit Research, Inc.*, 142 F. Supp.2d 1029, n. 8 (N.D. Ill. 2001).

[181] *See Electronics Boutique Holdings Corp. v. Zuccarini*, 56 U.S.P.Q.2d (BNA) 1705 (E.D. Pa. 2000), *motion to set aside denied*, 2001 U.S. Dist. LEXIS 765 (E.D. Pa. 2001), *aff'd*, 2002 U.S. App. LEXIS 9247 (3d Cir. Apr. 25, 2002), for an explanation of mousetrapping. In this case, the court noted that Zuccarini's website used domain misspellings to draw visitors to his site, which was designed to automatically display a succession of advertisements. Advertisers paid Zuccarini 10-25¢ for every click. Browsers were unable to exit Zuccarini's site until they clicked on each advertisement; hence the term "mousetrapping." This evidence was later cited in a criminal complaint filed against Zuccarini in Sept. 2003, alleging that he violated a federal law intended to prevent diversion of web browsers to pornographic websites by the use of misleading domain names. Mark Hamblett, *First Charges Filed under New Internet Porn Law*, 1 Internet L. & Strat. 9, at 3 (Sept. 2003).

© 2004 Piper Rudnick LLP. All Rights Reserved.

It is more difficult to prevent competitors from using key words as meta-tags if the words used are words in the dictionary as opposed to fanciful, coined words. This is another reason for adopting trademarks that are fanciful and not descriptive or suggestive.

© 2004 Piper Rudnick LLP. All Rights Reserved.

PRIVACY

Privacy concerns are widely regarded as one of the main issues delaying wider use of the internet and e-business. Surveys have shown potential e-business customers shy away from buying online because of fears that their personal information will be misused. Privacy protection is a major issue in e-business today. Privacy concerns have grown in part from the emphasis on data mining and marketing directly to consumers based on who clicked where, who bought what, site visitations and individual click histories.[182]

Privacy on the internet is largely self-regulated. There have been efforts in the past several years by businesses that deal with personal information to create industry standards to protect the privacy of consumer information stored on databases and available through the internet. Recently, Microsoft and IBM, the number one and two advertisers on the internet, announced they would not advertise on sites that do not post privacy policies.[183] Disney's Go Network group of sites, which includes Disney.com, Infoseek, ABCNEWS.com, and ESPN.com and others, declared that they would neither advertise on nor accept advertising from sites lacking a comprehensive privacy policy. The Direct Marketing Association will expel members who do not follow basic privacy safeguards. The Georgetown Internet Privacy study found that 94% of the top 100 websites have posted a privacy policy.[184] Websites posting privacy policies has increased significantly.[185] Industry has been trying to obviate the possibility of federal regulation by promoting self-regulation.

California passed the first law in the U.S. that requires companies to publish and conspicuously post a privacy policy on their Website if they collect information from California consumers over the age of 13.[186] The new law, which took effect on July 1, 2004, applies whether the Website operator is located in California or elsewhere. The new law covers any collection of personally identifiable information – which is a broader category that collecting physical addresses – and therefore all Website operators need to consider what information they do collect in practice before deciding how to deal with the new California law. The law requires that posted privacy policies to identify what personally identifiable information is collected, explain the categories of third-parties with which the Website operator may share that information, describe whether (and if so, how) a consumer may review and make changes to

---

182 *See generally No hiding place: The protection of privacy will be a huge problem for the internet society*, The Economist, Jan. 25, 2003, at Internet 5.

183 The Wall Street Journal, Mar. 31, 1998, at B1 (IBM).

184 The Industry Standard, Sept. 20, 1999, at 208.

185 In "Leadership for the New Millennium: Delivering on Digital Progress and Prosperity," the U.S. Government Working Group on Electronic Commerce, 3rd Annual Report (2000) at viii the Working Group reports the number of commercial websites that post privacy policies has jumped from 2% in 1998 to 62% in 2000.

186 The California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575 *et seq*.

© 2004 Piper Rudnick LLP. All Rights Reserved.

their personal information, explain how consumers can learn of changes in the privacy policy, and note the date when the privacy policy took effect.

In the U.S., the Federal Trade Commission has not recommended any internet privacy legislation except with respect to children. A recent FTC survey of major e-commerce Websites found that only about 20% met the FTC's standards for protecting consumer privacy, even though the FTC also found nearly 90% compliance rate by internet companies with respect to posting their privacy policies on their Websites.[187] However, in October 2001, FTC Chairman Timothy Muris suggested that Congress hold off enacting additional privacy laws, and instead expressed a preference for vigilant enforcement of the present standards and for letting industry innovate and self-regulate in the field.[188]

Congress passed the Children's Online Privacy Protection Act ("COPPA")[189] with the support of industry. This Act regulates sites aimed at children or where the site has actual knowledge that the user is a child. The FTC, on October 20, 1999, released its Final Rule on COPPA.[190] This Rule went into effect April 21, 2000. The Rule applies only prospectively to the collection of personal information collected online from children. It requires sites that are "directed" at children under the age of 13 to: (1) obtain "verifiable consent" from a parent before they collect personal information from these children or disclose personally identifiable information to third-parties; (2) offer notice of what type of information they collect from children and how it will be used; and (3) provide a means for parents to review information that is collected from children. This Rule adopts a sliding-scale approach for providing verifiable parental consent. This sliding scale approach will be in effect for at least a two-year period. This approach allows websites to use an e-mail-plus mechanism as consent for internal uses of the data. Most importantly, e-commerce providers need to appreciate that if they collect age data showing that a child is using the site or otherwise realize a child is using the site, then compliance with the verifiable parental consent provisions is required. For example, kids often sign up for sweepstakes used as an incentive for registrations or may be discovered to be kids during support telephone calls. Actual knowledge that the user is less than 13 years old requires compliance with COPPA. Kids represent a major portion of the internet users and need to be

---

[187] Glenn Simpson, *FTC Finds Websites Fail to Guard Privacy*, The Wall Street Journal, May 11, 2000, at B12.

[188] *See* Remarks of FTC Chairman Timothy J. Muris at The Privacy 2001 Conference, Cleveland, Ohio (Oct. 4, 2001) (*http://www.ftc.gov/speeches/muris/privisp1002.htm*).

[189] 15 U.S.C. § 6501 et seq., which is to be distinguished from the Child Online Protection Act (called COPA), codified at 47 U.S. C. § 231. Enforcement of COPA was enjoined by a federal district court because of questions as to whether the content restrictions in the statute were the least restrictive means of protecting children from harmful content. *ACLU v. Reno*, 31 F.Supp. 2d 473 (1999). That decision was ultimately upheld by the U.S. Supreme Court in *Ashcroft v. ACLU*, 542 U.S. ____, 2004 WL 1439998 (June 29, 2004), and the case was remanded to the district court for further consideration of the other possible means of accomplishing the same goal.

[190] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (1999) (codified at 16 C.F.R. Part 312).

© 2004 Piper Rudnick LLP. All Rights Reserved.

considered. COPPA compliance procedures need to be in place for many sites even though the sites are not targeted at children. If an area in a site is for children compliance is required. If age data is collected, compliance will inevitably be required. The cost of complying with COPPA may be considerable. Companies subject to COPPA, as well as privacy obligations arising under the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Telemarketing Sales Rule cannot avoid their obligations by transferring their data-processing activities overseas, according to Tim Muris, the FTC's Chairman, in a letter to Rep. Edward J. Markey (D-Mass.).[191]

The FTC had concluded that the level of voluntary adoption of privacy policies on the internet has fallen short of what is needed to protect personal privacy on the internet. The FTC has outlined five widely accepted principles for protecting consumer privacy online:

- Notice to consumers about how personal information online is used.
- Choice for consumers about whether and how their personal information is used.
- Security of personal information, if e-commerce is to flourish on the internet.
- Access for consumers to their own personal information to ensure accuracy.
- Enhancement/Redress alternatives, including industry self-regulation and civil or criminal sanctions.

E-commerce companies that collect personal information should disclose why they are collecting information; for what purposes they expect to use the information; what steps will be taken to protect the confidentiality, quality and integrity of information collected; the consequences of providing or withholding information; and any rights of redress that are available to individuals for wrongful or inaccurate disclosure of their information. The privacy policy should also clearly and concisely inform visitors to the sites what information the site collects about individuals. The Direct Marketing Association (the DMA.org) provides a questionnaire to assist companies in developing their privacy policies. Privacy policies should be clearly labeled and easily assessed when someone visits a website. One key point to emphasize is that once a company enunciates its privacy policy, the company must consistently adhere to that policy. Third party disclosures may be required to a shipper, for a credit card authorization approval, to law enforcement or otherwise to protect a company's legal interests. Special care should be paid to assure that privacy policies contemplate disclosure to administer the site and facilitate the owner's ability to execute transactions through the site. Privacy policies should also recognize that unintentional releases of data may occur due to faulty web design, program error, or faulty communications security. The FTC has taken action against companies who misrepresent their privacy policies. There is also the possibility that class actions could be brought by consumers against websites that violate their own privacy policies.

---

[191] *FTC's Muris Tells Market Laws Apply to Data Activities Wherever Conducted*, 9 Elec. Com. & Law Rep. 22, June 2, 2004, at 509.

© 2004 Piper Rudnick LLP. All Rights Reserved.

The *GeoCities* case is the leading FTC case dealing with online privacy protection.[192] GeoCities (now a business unit of Yahoo!) provides a "virtual community" of members' home pages. In order to become members of the GeoCities virtual community, membership applications containing personal information had to be completed. The FTC complaint alleged that GeoCities misrepresented that the information would be used in a limited manner when, in fact, information was disclosed to third parties who then used it to target members for marketing solicitations.

As the authors of the *Law of Electronic Commerce* state: ". . . [o]ne can, to a certain degree, avoid privacy law problems by using common sense and good judgment. Ask yourself: 'Would members of my family be comfortable with their personal information being handled in this way?'

Many e-commerce companies are trying to place their privacy policy statements at specific locations on the websites where customers may find the statements most meaningful. For example, the privacy policy statements might be prominently displayed at the point the customer is asked to submit personal information or hypertext or hotlinks to the privacy policy statements can be provided at such key points. In today's environment implementing a privacy policy is a business necessity for many e-commerce business and legally advisable for all. Privacy policies should be a part of the website terms of use, including the limitations on liability, dispute resolution and governing law provisions.[193] Privacy policies are liable to be treated as contractual commitments without any limitation on liability or other contractual protection unless they are integrated in other contractual documents.

Several organizations, such as the Better Business Bureau Online (BBB Online), TRUSTe and Consumer.net, are accepting applications for a privacy seal that enables consumers to identify websites that process information ethically. In addition, the Direct Marketing Association, the Online Privacy Alliance, and the Individual Reference Services Group have adopted a self-regulatory program.

In October 1998, the "European Commission's Council Directive" on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Directive") became effective. The EU Directive is important to e-commerce companies. It requires that personal data be collected only for specified and legitimate purposes and "not be processed in a way incompatible with those purposes." Prior consumer consent is

---

[192] *GeoCities, Inc.*, Docket No. C-3849, 1999 FTC LEXIS 17 (FTC Feb. 5, 1999).

[193] In *Crowley v. CyberSource Corp.*, 166 F. Supp.2d 1263 (N.D. Cal. 2001), plaintiff claimed Amazon.com, Inc. violated its privacy policy arising from Amazon.com's disclosure of plaintiff's personal information to CyberSource to verify the identity of the person making an online purchase from Amazon.com. Amazon.com sought the protection of its Participation Agreement's terms and conditions. However, the court ruled these terms and conditions did not apply since the claim arose under Amazon's privacy policy. Amazon.com has since changed its privacy policy and expressly adopted the new policy under, and subject to, its terms and conditions that are generally applicable to purchasers.

© 2004 Piper Rudnick LLP. All Rights Reserved.

the key to complying with the EU Directive on data privacy. Data must be adequate, relevant, accurate, current, not excessive, and must not be kept in identifying form for any longer than necessary. Personal data may be processed only if the person has consented "unambiguously" or if the processing falls within one of the exceptions. The EU Directive requires member states to ensure that personal data is transferred only to other countries with "adequate" privacy protection.

The U.S. and the European Commission have finally reached agreement on safe harbor provisions U.S. companies must meet to comply with the EU Directive on data privacy to permit the export of personal data. The accord will enable U.S. companies to comply with European privacy regulations and continue to receive personal data from Europe. On November 1, 2000, the U.S. Department of Commerce announced an online certification from U.S. companies can use to take advantage of the Safe Harbor Agreement. The "Safe Harbor" offers a way for e-commerce companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. The TRUSTe website privacy seal program has announced a new "EU Safe Harbor Privacy Seal" program. Key to the European Commission agreeing to the safe harbor provisions is their belief that the FTC will take action against U.S. companies who violate the safe harbor provisions. Accordingly, the FTC has indicated it will take action against U.S. companies who violate the safe harbor provisions which became operational in November 2000. Companies excluded from FTC or Department of Transportation jurisdiction cannot enter into the Safe Harbor Agreement and must find other ways to comply with the requirements of the EU Directive on Data Protection.[194]

Internet privacy is coming under added scrutiny based in part on prominent and highly controversial data collection and sharing practices, advances in data mining, and data profiling technologies. These developments are increasing the public pressure for greater privacy protection. Among the more recent developments in this area are the enactment of two statutes of seemingly narrow application; in practice, however, both of these laws will affect a broader range of businesses than would seem likely at first blush:

- The Health Insurance Portability and Accountability Act of 1996 (known as "HIPAA") deals with health care information privacy by setting standards for electronic health information transactions. In December 2000, the final rules for guaranteeing the privacy of medical

---

[194] Ironically, a review concluded that "[t]he U.S. model of voluntary self-regulation of the use of private data collected online appears to work better, according to a [European] Commission-funded study by United Kingdom-based Consumers International …. The study reveals, for example, that 80% of European Web sites don't comply with the current EU law that gives customers the chance to opt out of allowing their personal data to be stored and reused. In the U.S., however, almost 60% of the most-popular sites offer their users the chance of opting out of having their data stored and reused." Ben Vickers, *Europe Lags Behind U.S. on Web Privacy*, The Wall Street Journal, Feb. 20, 2001.

© 2004 Piper Rudnick LLP. All Rights Reserved.

information under HIPAA were issued.[195] The HIPAA rules will apply not just to medical providers and plans, but also to associated businesses and, in some cases, to companies that provide or collect health insurance usage information; in the aggregate, these constitute approximately 13% of the U.S. economy.[196]

- The Gramm-Leach-Bliley Act (known as "GLB") limits when a "financial institution" may disclose non-public information about consumers.[197] Because "financial institutions" are defined extremely broadly under the FTC's regulations that implement GLB, many types of businesses, especially businesses engaged in the extension of credit to consumers, are covered by the notice, opt-out, and disclosure requirements.[198]

---

[195] The HIPAA privacy rules published December 28, 2000 were supposed to be effective February 26, 2001 but did not become effective until April 14, 2001, because the U.S. Department of Health and Human Services reopened the already-issued privacy rules to comments.

[196] *See* "Leadership for the New Millennium: Delivering on Digital Progress and Prosperity," The U.S. Government Working Group on Electronic Commerce, 3rd Annual Report (2000) at xiii.

[197] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, Title V, Privacy, 113 Stat. 1338, 1436-1450 (1999) (codified at 15 U.S.C. §§ 6801-6809).

[198] Privacy of Consumer Financial Information, 16 C.F.R. Part 313 (*see also* the FTC notice announcing the issuance of the new rule, at 65 Fed. Reg. 11,174 (2000)).

© 2004 Piper Rudnick LLP. All Rights Reserved.

AGREEMENTS FOR E-BUSINESS RELATIONSHIPS

Most e-business behaves as a network economy and obeys different laws from traditional commerce. The network economy rests on communications, not commodities. Success on the internet requires a large presence. In network economies supply creates demand. New business practices need to recognize the differences in conduct in business in a network economy and the network effects.

The whole field of e-business is relatively new. The business and legal models for e-commerce business relationships are evolving very quickly. It is difficult to sustain a competitive advantage with most of these models because they can be easily replicated or rendered obsolete.[199] Some of these models are proving not to be sustainable over the long term. These e-commerce business relationships require an appreciation of the technology, the network economy, unique intellectual property issues, and business models applicable to web development agreements, web hosting agreements, web linking agreements, web affiliation agreements, content provider agreements, Web advertising, co-branding and co-marketing agreements, fulfillment agreements, merchandising agreements, channel partner agreements, electronic distribution agreements, and other forms of e-commerce relationships.

One issue that is often heavily negotiated is the ownership, control and use of information pertaining to customers and site visitors. In the e-commerce world it is possible to track every "click" by a visitor. Web marketing is being based on individual "click histories."[200] The rights in and to this usage information pertaining to customers and visitors are becoming extremely valuable. It needs to be considered in many e-commerce relationships. The focus of e-commerce is to use this user information to build a unique marketing profile for each customer so that e-customers can be marketed to individually. Advances in data mining and customer profiling technologies are making this "click stream" information increasingly more valuable. One-to-one marketing is a goal shared by many e-commerce purveyors. Permission marketing is becoming increasingly more prevalent.

Successful e-commerce businesses are "listening" to their customers and recognizing the closed-loop advantages arising from an e-commerce customer relationship to conduct focus groups online, get customer feedback, get user ideas and input and quickly adjust to customer needs and preferences. eBay has built a strong brand and personal one-to-one relationships with many of its customers by keeping in close touch with its customers.[201]

---

[199] Nicholas Carr, *Decoding Business Giant Steps*, The Industry Standard at 139 (Sept. 4, 2000).

[200] The information collection practices based on "cookies" have proven quite controversial but not illegal. *See, e.g., In re Double Click Inc. Privacy Litigation*, 154 F. Supp.2d 497 (S.D.N.Y. 2001); *Chance v. Avenue A, Inc.*, 165 F. Supp.2d 1153 (W.D. Wash. 2001); *In re Intuit Privacy Litigation*, 138 F. Supp.2d 1271 (C.D. Cal. 2001).

[201] R. Hof, *The People's Company*, Bus. Week, Dec. 3, 2001, e.biz Section, at EB15.

© 2004 Piper Rudnick LLP. All Rights Reserved.

There are many different advertising business models. One model is based on cost-per-million (CPM) impressions. The CPM cost for advertising has been decreasing recently. Another model is based on flat fees, *i.e.*, a flat fee for a fixed period of time. The CPM rate often ranges from $5 to $20 per thousand impressions served or viewed.[202] When demand for online ad space decreased in 2001, prices dropped to about half what they were in 2000.[203] Images may include banners, buttons, textlinks, moving graphic icons, pop-up windows and other methods of advertisements.[204] Also fees can be assessed based on click-throughs. For example, fees are generated based on each time a user clicks on a banner ad. One concern with this type of advertising model is to make sure the click-throughs are bona fide. It is often specified in these agreements that computer-generated click-throughs should not count among the revenue-generating click-throughs. Companies must pay careful attention to the definition of "click-throughs" used to calculate revenues.[205]

Sponsorship packages are also used.[206] An advertiser might be the sponsor of certain content or Web pages. This may include impressions, click-throughs and other forms of revenue-sharing. The prominence, rotation and placement of ads are often negotiated in these advertising deals. Sponsorship packages typically cost from $30 to $75 per thousand viewers depending on the site and whether exclusivity is included.[207]

Many advertising arrangements are being restructured to reward concrete results instead of the traditional advertising models.[208] For example, under a conversion-rate scheme an advertiser pays only for "converted" users who actually buy a product or service as a result of an advertisement. Similarly, with electronic coupons the advertiser only pays upon coupon

---

202 Ron Dreben and Johanna Werbach, *Portal Agreements: 10 Tacks for Smooth Sailing*, 5 Cyberspace Lawyer 6 (Dec. 2000). With affinity marketing providing segmented audiences for ads, the CPM rate may be increased as much as $8 more per thousand impressions for demographically targeted ads. *See* N. Wingfield, *Calling The Shots*, The Wall Street Journal, Apr. 23, 2001, at R16.

203 V. O'Connell, . . . *Advertise*, The Wall St. J., Nov. 12, 2001, at R13 ("O'Connell") (prices reduced from $20 to $10 per thousand impressions).

204 *Id*.

205 *See Go2 Net, Inc. v. C. I. Host, Inc.*, 115 Wash. App. 73 (Wash. Ct. App., Div. One, 2003) (dispute over method of counting "impressions" in an Internet advertising contract).

206 In the Fourth Quarter of 2000 approximately 31% of the online ad revenues came from sponsorships. *See* O'Connell.

207 *See* J. Rewick, *Choices, Choices: A Look at the Pros and Cons of Various Types of Web Advertising*, The Wall St. J., Apr. 23, 2001, at R12.

208 A. Brunel & G. Sapire, Beyond Banners: Restructuring Portal Advertising Deals, 33 Computer Law Reporter 226 (Apr. 2001). See also J. Rewick, *Choices, Choices: A Look at the Pros and Cons of Various Types of Web Advertising*, The Wall Street Journal, Apr. 23, 2001, at R12.

© 2004 Piper Rudnick LLP. All Rights Reserved.

redemption. With result-oriented advertising, the website bears the risk that web surfers will not respond to the ads.[209]

Some business models include auctions, reverse auctions, name your price, haggling, group buying, wanted classifieds, gift registries, product reviewers, online malls, selling below cost, and e-exchanges of all sorts.

There are many intellectual property issues that are implicated in many of the business models. Copyright law, including the new Digital Millennium Copyright Act amendments, will affect the way e-business deals are structured. In addition, the growing body of patents in the area of e-business may also have a significant impact.

Legal considerations are increasingly becoming an integral part of the business model design process. E-business agreements tend to be shorter in duration with due regard to rapidly changing market condition and advances in technology.[210] For these reasons e-business relationships often try to build in a certain degree of flexibility to react to changes in the market and technology. Barter deals have been common in the internet industry. These barter deals are raising accounting and tax issues. Early consideration of legal strategies and legal considerations will often help build a much more viable e-commerce business model and may help avoid substantial redesign and litigation costs applicable to business models.

---

[209] N. Wingfield, *Calling The Shots*, The Wall Street Journal, Apr. 23, 2001, at R16.

[210] For example, Half.com claims it now includes a 48-hour termination clause in its online advertising contracts. *Id.*

© 2004 Piper Rudnick LLP. All Rights Reserved.

WEB CRAWLERS, SPIDERS AND BOTS

Many e-commerce business models include web crawlers, spiders or bots. One recent case illustrates how search engines may be integrated into e-commerce applications as a matter of fair use under the Federal Copyright laws. In *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003), the Ninth Circuit approved as a matter of fair use, the transformative, thumbnail image-based search engine used to build an indexing system for images on the internet.

In the *Kelly* case, the Defendant Ditto (formerly known as Arriba) operated a "visual search engine" on the internet. The search engine retrieved images and produced a list of reduced "thumbnail" pictures relating to the user's query. By "clicking" on a thumbnail the user could view the "image attributes" window displaying the full-size version of the image, a description of its dimensions, and ad address for the Website where it originated. By clicking on the address, the user may then link to the originating Website for the image. The thumbnails are collected by Ditto's crawler program that searches for images.

In the *Kelly* case Ditto did not dispute that it reproduced plaintiff's images in thumbnail form without authorization but asserted a fair use defense. Ditto, as the defendant, had the burden of proof on this affirmative defense. The images were not exploited in any particular way. They were collected in an indiscriminate manner using the Ditto crawler to obtain large numbers of images from numerous sources without seeking authorization. The court found the use to be largely transformative. The transformative nature of the use was critical.

Ditto argued there is no likely negative impact because its search engine does not compete with plaintiff's websites and actually increases the number of users finding their way to plaintiff's websites. While the court discussed the possible adverse consequences of deeplinking and bypassing the front page of the websites, plaintiff did not show any evidence of any harm or adverse impact. Here the court did not discern any market harm to the plaintiff and determined that Ditto's inherently transformative process provided internet users with a better way to find images on the internet.

The court in the *Kelly* matter found Ditto's unauthorized copying under these circumstances to be permissible under the fair use doctrine. The court also did not find any violation of the Digital Millennium Copyright Act. There was no removal of any copyright management information that was shown to exist. Here the user was given the name of the Website from which Ditto obtained the image and warned the user that use restrictions and copyright limitations may apply to images retrieved by Ditto's search engine. The court did not suggest it was at all concerned that Ditto's search engine may not have complied with the use restrictions and copyright limitations applicable to the site from which the thumbnails were indexed.

© 2004 Piper Rudnick LLP. All Rights Reserved.

In *eBay, Inc. v. Bidder's Edge, Inc.*,[211] the court did find the terms of use on eBay's site to be relevant in its determination to prohibit Bidder's Edge from continuing to spider eBay's computer system without written authorization for the purpose of copying part of eBay's auction database. Here, eBay expressly prohibited in its User Agreement the use of "any robot, spider, other automatic device, or manual process to monitor or copy our web pages or the content contained herein without our prior written permission." The evidence showed that Bidder's Edge accessed eBay's site by spidering 80,000 to 100,000 times a day. Under these circumstances, the court found Bidder's Edge's electronic signals were sufficiently tangible to support a trespass cause of action and that Bidder's Edge was most likely liable for trespass to chattels by virtue of exceeding the scope of access permitted by eBay to its site.[212] The theory of cyber-trespass has been expanded in several court decisions and is likely to be invoked as courts wrestle with the question of how to apply established legal precedent in the electronic context.[213] However, in 2003, the California Supreme Court limited the application of the "trespass to chattles" theory with respect to the damages caused by the *content* of the e-mails sent by a former Intel Corp. employee to a large number of Intel employees, in contrast to the functional impact on a company's computer resources that might be shown to flow from a large number of unsolicited e-mails.[214]

In *Intel Corp. v. Hamidi*, the California Supreme Court declined to extend the cyber trespass theory to electronic communications that do not cause actual damage to the recipient's computer system or impair its functioning.[215] There the alleged trespass involved e-mails sent to between 8,000 and 35,000 Intel employees. The majority determined that Hamidi's e-mails only consumed a small part of Intel's computer system without affecting its operation. The Hamidi case diminishes greatly the applicability of cyber trespass. The law with respect to web crawlers,

---

[211] 100 F. Supp.2d 1058 (N.D. Cal. 2000) (settled). The *Bidder's Edge* appeal was heard by the U.S. Court of Appeals for the Ninth Circuit in February 2001 and was subsequently settled when Bidder's Edge went out of business and paid eBay an undisclosed amount.

[212] *See also Oyster Software Inc. v. Forms Processing Inc.*, No. 00-0724 (N.D. Cal. Dec. 6, 2001) (citing *Bidder's Edge*; web bot's unauthorized searching through the plaintiff's website was sufficient to state a claim in trespass to chattel).

[213] *See Register.com, Inc. v. Verio, Inc.*, 126 F. Supp.2d 238, 251 (S.D.N.Y. 2000) (citing *Bidder's Edge*, court took notice that plaintiff had expressed "fear that its servers will be flooded by search robots deployed by competitors…."); *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997) (enjoining the transmission of spam to CompuServe customers, because those e-mails clogged the CompuServe network, damaged CompuServe's reputation, and caused customers to pay more in connection fees to download unsolicited e-mails); and *Thrifty-Tel Inc. v. Bezenek*, 54 Cal. Rptr.2d 468 (Cal. Ct. App. 4th 1996) (involving hacking into phone system and making calls without payment; court found that electronic signals are tangible enough to support claim of trespass to chattel).

[214] *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003).

[215] *Id*.

© 2004 Piper Rudnick LLP. All Rights Reserved.

spiders and bots is just beginning to take shape.[216] The *Kelly* case shows how web crawlers can be used to create new transformative products and services and the *eBay* and *Register.com v. Verio, Inc.* cases demonstrate that web crawlers may be prohibited as a trespass to private property, especially where the amount of spidering consumes a significant amount of the website's resources and capacity, thereby causing actual damage to the website's computer systems or otherwise impairs its functioning.

Three other cases are worth noting. In *EF Cultural Travel BV v. Zefer Corporation*,[217] Zefer was prohibited from using a "scraper tool" to collect pricing information from EF's pricing information. The First Circuit emphasized the importance of explicit prohibitions in the Terms of Use for a website noting that a website provider can easily spell out explicitly what is forbidden by stating "no scrapers may be used." In the *Ticketmaster* case,[218] Tickets.com employed "spiders" to review the internal web pages of Ticketmaster and extract electronic information respecting events. The spiders temporarily loaded the electronic information into the RAM memory of Tickets.com's computers for a period of 10 to 15 seconds. During this 10 to 15 second period, Tickets.com extracted factual information (event, date, time, ticket prices and URL) and then discarded the rest (which consisted of Ticketmaster identification, logos, ads and other information Tickets.com did not intend to use; much of the discarded material was protected by copyright). The factual information Tickets.com extracted was then displayed on the Tickets.com web page. The court found that Tickets.com's spidering activities did not constitute a trespass to chattels because there was no tangible interference with the use or operation of the computer being invaded. The court also reasoned that taking a temporary copy of electronic information for the limited purpose of extracting unprotected public facts leads to the conclusion that the temporary use of electronic signals was "fair use" and not actionable.

In *Nautical Solutions Marketing, Inc. v. Boats.com*,[219] the district court found that the use of an Internet "spider" to visit public websites, extract facts from the websites, and index the facts in a searchable database accessible to users on another website, Yachtbroker.com was permissible. Like the *Ticketmaster* case, the spider here copied the whole web page for the yacht listing, then extracted the prescribed facts and discarded the rest of the web page. Even though Yachtbroker.com "copied and pasted" certain content, including pictures and descriptions, from yacht listings on Yachtworld.com and posted the content on Yachtbroker.com in a different format, Boats.com was not the copyright owner of the content that was copied and pasted on the other website.

---

[216] *See, e.g., Register.com v. Verio, Inc.*, 126 F.Supp.2d 238 (S.D.N.Y. 2000), in which the court enjoined Verio from using spider technology to search Register.com's WHOIS database for the purpose of culling out marketing information.

[217] 318 F.3d 58 (lst Cir. 2003).

[218] *Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. March 7, 2003).

[219] Case No. 8:02-cv-760-T-23TGW (M.D. Fla. April 1, 2004).

© 2004 Piper Rudnick LLP. All Rights Reserved.

COMPETITION ISSUES

Competition is everywhere on the internet. Many new competitors and new e-commerce business models are creating immense competitive pressures. Competitor sites are only a click away. Once a potential customer clicks to the next site the former site may never see the potential customer again. There are numerous competitive issues that have been brought about by the internet or which have particular significance in connection with the internet or e-commerce. These issues include: (1) distribution; (2) electronic B2B and B2C marketplaces; (3) standards setting; (4) meta-tags and other anticompetitive practices; (5) intellectual property issues; and (6) market power.

There are many opportunities in e-business for the creation and exploitation of market power. Competition on the internet today is different than we have seen before. The barrier to entry for websites is low. It is relatively easy to set up a retail website. These websites are worldwide storefronts available 24 hours a day seven days a week to any one anywhere that has access to the internet. The absence of boundaries on the internet means that there are many more competitors. The internet eliminates many of the inefficiences in the marketplace. These inefficiencies are reduced by giving buyers and sellers in e-markets immediate access to endless information about products, services and prices and by enabling an unlimited number of buyers and sellers to transact business, through these virtual marketplaces.

One recent case deals with monopolization claims relating to the internet market for Yellow Page telephone listings. In *GTE New Media Services, Inc. v. Ameritech Corp.*, 21 F. Supp.2d 27 (D.D.C. 1998), *dismissed on personal jurisdiction grounds*, 199 F. 3d 1343 (D.C. Cir. 2000), the defendant Regional Bell Operating Companies, allegedly agreed to allocate geographic territories and customers in the Internet Yellow Pages market in violation of Section 1 and Section 2 of the Sherman Antitrust Act. GTE New Media Services alleged that the defendants conspired to restrain trade and to monopolize the Internet Yellow Pages market by controlling internet access points through which competing Internet Yellow Pages providers offer their services. The case illustrates the critical nature of portals like Yahoo! as a marketplace for internet surfers.

GTE also alleged that the defendants used their collective power to coerce Netscape to terminate its links to GTE's Super Pages, including hyperlinks on Netscape's Guide by Yahoo! The defendants' exclusionary acts were alleged to have injured GTE in the Internet Yellow Pages market by disrupting the primary means for GTE to generate income from its website and directly limiting GTE's ability to generate advertising revenue for its Yellow Super Pages. Even though the case was dismissed as to some defendants based on lack of personal jurisdiction, the district court found that GTE had properly alleged antitrust injury in the Internet Yellow Pages market.

The case is illustrative of the new issues relating to competition on the internet. Here the defendants formed a master directory site. Anyone "clicking" on a city or area on the virtual map of the United States was hot-linked to a defendant's Internet Yellow Pages for that city or area. The defendants had allocated the markets for Internet Yellow Pages geographically among themselves. Through their collective market power allegedly they were able to negotiate an exclusive hyperlink on Netscape and Netscape's Guide by Yahoo! These exclusionary acts

© 2004 Piper Rudnick LLP. All Rights Reserved.

allegedly effectively foreclosed a significant portion of the Internet Yellow Pages customers from GTE.

Portals have become key access points to the virtual e-commerce marketplace. Assuring reasonable non-discriminatory access to e-marketplaces is certain to be an issue in the formation and operation of e-business exchanges. Internet retailers need access to actual goods and the means to deliver the goods to businesses and consumers.

Bottlenecks may arise in distribution for e-commerce in much the same way as bottlenecks arise in the "brick-and-mortar" world. These bottlenecks in the distribution channels are likely to cause antitrust concerns.

One of the greatest growth areas in e-commerce are the B2B "net markets", web sites that bring together many buyers and sellers on a single site. Most B2B internet exchanges have been around for less than one year. But some commentators have already voiced antitrust and competition concerns about these new electronic markets.[220] Many of these are trading raw materials and finished parts. Examples include Covisint, AviationX, eChemicals, eSteel, PaperExchange, PlasticsNet, and MetalSite.[221] One article states that there are now more than 1,000 B2B exchanges that will do about $720 billion in business in 2001.[222] These optimistic predictions are no longer valid in this new economy but B2B exchanges are still a major growth area.

While these electronic markets raise concerns because of the size of the players they should not create antitrust problems as long as they remain open to competitors on a non-discriminatory basis. They are being established as neutral, open marketplaces. Their objective is to bring together as many buyers and sellers as possible to create price competition in a dynamic market exchange environment. The proponents believe the exchanges will lower the procurement costs for buyers and broaden the base of potential buyers for sellers.[223] The internet enables buyers to easily obtain extensive information about prices, features and quality. The greatest impact for B2B exchanges is likely to be in providing supply chain management and product collaboration services.

The electronic marketplaces are designed to be for-profit, open, neutral marketplace entities in and of themselves. The competitive pressures, relative low barrier of entry and low cost for establishing B2B e-market exchanges should militate in favor of these exchanges being

---

[220] William Woods, *Premature Regulation*, The Industry Standard, May 8, 2000, at 214-215, 218, 222 ("Woods").

[221] *Id.* at 215.

[222] Robert Bell and William Adkinson, *Antitrust Issues Raised by B2B Exchanges*, 15 Antitrust at 18 (Fall 2000) ("Bell").

[223] Woods at 215, 218.

© 2004 Piper Rudnick LLP. All Rights Reserved.

operated in a fair and non-discriminatory manner because buyers and suppliers from all over the world will have access to the internet competitive bidding and pricing. Through auctions and reverse auctions, buyers and suppliers can both benefit. B2B exchanges will develop the most efficient trading mechanisms for suppliers and buyers participating in their exchanges.[224]

One commentator believes these B2B exchanges have shifted the balance of power from the supplier to the buyer. However, he does not believe regulatory structures are necessary to monitor and regulate these B2B exchanges. It is rather free markets, low barriers to entry and easy access to startup capital that will ensure B2B electronic exchanges remain open competitive marketplaces.[225]

Equal access to information and other aspects of these markets will no doubt be a concern to all competitors participating in the B2B markets. All participants will want to be sure they have equal access to information and opportunities. They will want to be treated fairly compared to all other participants. One relevant historical area of legal precedent that may presage the issues with B2B exchanges concerns the legal cases relating to database access. These cases underscore the importance of not restricting access to these internet markets in a discriminatory or unfair manner.

The Antitrust Guidelines for Collaboration Among Competitors[226] will be used to assess the anticompetitive risk and activities of B2B exchanges. Restrictions in the collaboration may be attacked as anticompetitive. Every restriction in a B2B venture should be directly related to the B2B venture's procompetitive purposes.[227] The restrictions cannot be justified on efficiency grounds if there is a better way to achieve the efficiency.[228]

The two major antitrust concerns with B2B exchanges are collusion and exclusion, either by outright exclusion or discriminatory treatment.[229] The concern over collusion increases greatly if the members or participants of the B2B exchange constitute a large share of the total supply.[230] The main concern is that B2B exchanges could serve as a mechanism for sharing price

---

[224] *Id.* at 215.

[225] *Id.* at 222.

[226] Federal Trade Commission and U.S. Department of Justice, Antitrust Guidelines for Collaborations Among Competitors (2000), reprinted in 4 Trade Reg. Rep. (CCH) ¶ 13,161.

[227] Bell at 19.

[228] *Id.*

[229] *Id.*

[230] *Id*.

© 2004 Piper Rudnick LLP. All Rights Reserved.

and other competitively sensitive information.[231] Safeguards against potentially anticompetitive information sharing need to be adopted through a combination of encryption, software design and firewalls. Purchase orders, payment and shipping information should be protected against unauthorized disclosure.[232] Information concerning volumes, prices, capacity, and other details of particular transactions should not be available to anyone other than the seller and the buyer, unless necessary to serve a legitimate purpose.[233]

B2B exchanges should also adopt strong anti-discrimination policies. There should be neutral standards governing access to and participation in the exchange. The exchange should not require that participants in the exchange use the exchange exclusively or primarily for their transactions or refrain from using other exchanges or other means of transacting business.[234]

Joint buying on B2B sites may also raise antitrust concerns. Exchanges should adopt rules and protocols to prevent buyers from pooling and reducing their purchases where doing so will give the buyers the ability to decrease the price they pay.[235]

E-Commerce and the internet are growing at lightening speed. Technological development is accelerating at an astonishing pace. The utility of these developments depends often upon single standards for interoperability and communication protocols. But settling on a single standard necessarily requires concerted action among horizontal competitors raising potentially serious antitrust concerns. Collusion among competitors can lead to depression of innovation, increased prices, reduced output and quality, and the exclusion of new entrants. The Federal Trade Commission has conducted workshops relating to B2B trading exchanges. As such, standards setting is very much a part of the competitive analysis to ensure standards are non-discriminatory. As a general rule, standards should not unfairly exclude competitors or competition. They should be neutral.

As the *GTE* case and discussion above illustrates, market power issues are not going to be eliminated by the growth of the internet. In many areas, barriers to entry will be lowered dramatically. The importance of intellectual property rights will increase in connection with the internet and e-commerce, and as that happens, market power concerns will be raised.

Competition on the internet may be different than competition among "brick and mortar" companies. There are numerous issues relating to distribution, B2B and B2C exchanges, meta-

---

[231] *Id.*

[232] *Id.*

[233] *Id.* at 23.

[234] *Id.* at 22.

[235] *Id.* at 21.

© 2004 Piper Rudnick LLP. All Rights Reserved.

tags, intellectual property rights, standards setting and market power. Competition is fierce and whatever the differences are in the shape, manner, and form of this competition, restraints on competition still require antitrust compliance and vigilance. Competition laws and policies are certain to be tested by the new business models, new distribution channels and increased competition in cyberspace.

© 2004 Piper Rudnick LLP. All Rights Reserved.

ELECTRONIC AGREEMENTS

On June 30, 2000, the President of the United States signed into law the Millennium Digital Commerce Act, also known as the Digital Signatures or E-SIGN legislation ("E-SIGN").[236] The E-SIGN statute is the most significant e-commerce online contracting legislation adopted at the federal level to date. By granting nationwide legal recognition to electronic signatures and records in the United States notwithstanding laws that require "written" documents, E-SIGN will make online transactions and online notices to consumers significantly easier. E-SIGN establishes a nationwide rule that gives the same legal effect to electronic signatures, contracts, and records that is accorded to paper and ink signatures, contracts and records. It contains provisions that insure legal validity of electronic signatures and contracts, permits the electronic delivery of legally-required notices and disclosures, and allows for the satisfaction of record retention requirements through electronic means. At the same time, E-SIGN contains consumer protection measures requiring consumer notice and consent before electronic records can be binding. E-SIGN took effect October 1, 2000, except for several provisions that took effect on later dates.

Prior to E-SIGN, 49 U.S. states either had enacted or were considering enacting some form of electronic signature legislation. As of December 2001, 37 states and the District of Columbia had adopted UETA in one form or another.[237] However, even states that enacted UETA had not done so in a uniform way. Despite the broad consensus on the need for electronic signature legislation, there has previously been little uniformity in the approaches considered by state legislatures. Some states authorize electronic signatures only in limited circumstances, while others authorize electronic signatures in a broad variety of circumstances. In 1999, the National Conference of Commissioners on Uniform State Laws in the United States developed and approved the Uniform Electronic Transactions Act ("UETA"), a model law for each state to adopt. E-SIGN is designed to promote uniform legal standards across all 50 states, thus facilitating interstate electronic commerce. By increasing the speed of transactions and reducing paperwork, E-SIGN should facilitate electronic business and produce cost savings for businesses and consumers alike.

Today, information is being used, stored and transmitted in digital form. Electronic records are essential to the conduct of business today.[238]

Click-wrap, browse-wrap, or web-wrap agreements are commonly used in connection with e-business transactions. These agreements are typically used to specify the terms and conditions applicable to the use of the website as well as to the products and services purchased

---

[236] P.L. 106-229.

[237] *See 37 States Adopt UETA*, 18 e-Commerce Law & Strategy 8 at 1, 10-12 (Dec. 2001).

[238] *In re Bristol-Myers Squibb Securities Litigation*, 205 F.R.D. 437, 2002 U.S. Dist. LEXIS 13808 (D.N.J. Feb. 4, 2002) (In 1999, 93% of all information generated by companies was in digital form on computers.)

© 2004 Piper Rudnick LLP. All Rights Reserved.

over the internet. With these agreements the buyer or user usually explicitly assents to these terms by clicking on a button stating "I agree" or "I accept" after having had an opportunity to review the terms. An act by the buyer affirmatively assenting to the terms of the click-wrap agreement significantly enhances its enforceability. Some sites, for instance, indicate that continuing use of the site by the user or buyer manifests assent to be bound by the terms and conditions applicable to using the site. It is critical that the users have an opportunity to review the terms of use applicable to the site. If they are buried or otherwise inconspicuous, they will be more difficult to enforce.

Recent case law has enforced various forms of click-wrap agreements. Most courts have found click-wrap agreements to be valid and enforceable.[239] Click-wrap agreements are considered to be more enforceable than "shrink-wrap" which are entered into based on the licensee opening the software products' packaging or failing to return the product within a specified period, typically 7 to 30 days. Click-wrap agreements are entered into by an affirmative assent as opposed to the failure to act. In contrast, a "browse-wrap agreement" was not enforced where the agreement was available in the form of an on-screen icon to a browser seeking to download software, but where the browser could complete the download without clicking on the agreement, viewing the agreement, or otherwise manifesting affirmative assent.[240]

Additionally, if the agreements are too overbearing or contain unusually harsh terms it is possible, especially in a consumer law context that the click-wrap agreement, even if assented to, may be found unconscionable and unenforceable. To mitigate that possibility, click-wrap agreements should provide a clear and simple mechanism allowing the consumer to return the products for a refund within a reasonable period of time. It is also recommended that the terms and conditions of the agreement be available for inspection in booklet form at physical locations.

In order for a company to establish that it gave effective disclaimers to users and entered into enforceable agreements with purchasers, that company must establish a policy of maintaining records of the disclaimers and contract terms contained on its website, including any changes made over through time. On the first page of the website, a company should include a prominent notice instructing users to review the terms and conditions of usage and alerting users to changes in the terms as they occur.

To rely on an electronic message, the parties should take steps to make sure the contract is binding, *e.g.*, that the essential terms of the contract are manifested,[241] agreed upon, and that

---

[239] *See Comb v. Pay Pal, Inc*, 2002 WL 2002 171 (N.D. Cal. Aug. 30, 2002) (Pay Pal's User agreement found to be both procedurally and substantively unconscionable). One of the reasons for the result was that Pay Pal sought to make amendments to their Terms of Use effective unilaterally merely by posting the changes.

[240] *Specht v. Netscape Communications Corp.*, 150 F. Supp.2d 585 (S.D.N.Y. 2001), *aff'd*, 2002 U.S. App. LEXIS 20714 (2d Cir. Oct. 1, 2002).

[241] In *Shattuck v. Klotzbach*, 2001 Mass. Super. LEXIS 542 (Mass. Super. Ct. Dec. 11, 2001), the court enforced a contract that the parties made through a series of e-mails for the sale of real property, in which all of the

(footnote continued to next page)

© 2004 Piper Rudnick LLP. All Rights Reserved.

the persons who are parties to the electronic "contract" have the legal competence and capacity to enter into an agreement. One particular problem area is with children who are not old enough to enter into a contract. Where children are potential purchasers, parental consent should be sought. In specific applications additional representations may be sought from the customer.

E-SIGN gives legal legitimacy to electronic signatures, contracts and records. E-SIGN defines the term "electronic signature" to mean an electronic sound, symbol, or process that is attached to or logically associated with the record and intended to act as a signature. In addition to E-SIGN, click-wrap agreements are also countenanced by the Uniform Computer Information Transaction Act ("UCITA" formerly known as Article 2B to the Uniform Commercial Code) which was recently adopted by the National Conference of Commissioners on Uniform State Laws ("NCCUSL") on July 29, 1999. UCITA was enacted by Virginia (effective July 2001), Maryland (effective October 1, 2000), and is being considered by other state legislatures.

In June 2001, the FTC and Commerce Department issued a report to the Congress, as required under Section 105(b) of E-SIGN.[242] The FTC/Commerce Report addressed the impact of the consumer protection provisions under the law. In sum, the FTC/Commerce report concluded that while it is still early to reach definitive conclusions, "[t]he consumer consent provision in ESIGN [sic] appears to be working satisfactorily at this stage of the Act's implementation. Almost all participants in the study recommended that, for the foreseeable future, implementation issues should be worked out in the marketplace and through state and federal regulations. Therefore, Commerce and the FTC recommend that Congress take no action at this time to amend the statute.

E-businesses must keep records showing what version of their electronic agreement applied to what e-customer at what time. This was one of the problems Pay Pal experienced in *Comb v. Pay Pal, Inc.*,[243] where Pay Pal was unable to show which of the six versions of its Terms of Use applied to which plaintiff making it very difficult for Pay Pal to prosecute its breach of contract claims. Besides the record-keeping requirements necessitated by electronic agreements there is also the risk that an exchange of e-mails may be treated as a binding contract inadvertently. Some companies specifically note that unless an email is explicitly and conspicuously designated as "E-Contract Intended", the email does not constitute a contract

---

(footnote continued from previous page)

essential business terms were communicated. The court also concluded that the seller's typed signature at the end of the e-mails constituted authentication of the seller's intent to engage in the transaction. *Id*. at *7-*10. *See also I.LAN Systems, Inc. v. NextPoint Networks, Inc.*, 183 F.Supp.2d 328 (D. Mass. 2002) ("I agree" box clicked).

[242] Federal Trade Commission and U.S. Department of Commerce, "Report to Congress: Electronic Signatures in Global and National Commerce Act, The Consumer Consent Provision in Section 101(c)(1)(C)(ii)" (June 2001) (available at *http://www.ftc.gov/os/2001/06/esignreport.pdf*).

[243] 2002 WL 20002171 (N.D. Cal. Aug. 30, 2002).

© 2004 Piper Rudnick LLP. All Rights Reserved.

offer, a contract amendment, or an acceptance of a contract offer.[244] Some contracts today expressly provide that they may not be amended electronically.

[244] With the accepted enforceability of electronic agreements a new concern is that unwanted contracts may be formed by e-mail. Companies need to be sensitive to this risk. One strategy is to add a provision to standard e-mail legends, such as one that states that: *This email does not constitute a contract offer, a contract amendment, or an acceptance of a contract offer unless conspicuously designated as "E-Contract Intended".*

© 2004 Piper Rudnick LLP. All Rights Reserved.

WEBSITE TERMS OF USE

Today website owners are using terms of use/terms of service agreements posted at their website to allocate, limit, reduce, mitigate, avoid and otherwise manage potential risks in cyberspace.

Terms of service or use agreements are one of the most important strategies for managing the risks on an e-commerce website. Think of the website as a piece of virtual real estate in cyberspace. By posting "NO TRESPASSING" terms of service on its site, a company can allocate many of the legal risks to its visitors and customers and otherwise limit many of its legal risks. These agreements are generally enforceable. One court, for example, suggests using a click-wrap agreement to limit the jurisdictional exposure of e-commerce merchants who would otherwise be subject to being hauled into court wherever they sell products. Terms of Use agreements should include venue-selection provisions and otherwise be used to limit legal exposure and minimize legal risks.[245]

The risks associated with each website need to be identified. Website terms of use should be adopted to creatively manage, allocate, mitigate, limit and avoid the risks associated with e-commerce. For example, contract terms should deal with errors in content including errors in pricing, specify who is eligible to use the site, provide protection for intellectual property rights, and include warranty disclaimers and liability limitations.

Typically the website Terms of Use will state in essence "IF YOU DO NOT ACCEPT THIS AGREEMENT, YOU MAY NOT ACCESS THIS WEBSITE OR USE ANY OF THE SERVICES PROVIDED ON OR THROUGH THE WEBSITE." The website owner usually reserves the right to change the terms to allow for new services, new concerns and flexibility in the dynamic internet arena.

Privacy policies, spam policies and other policies are often separately addressable but incorporated in the website Terms of Use by a hyperlink. Make sure that there are no conflicting agreements with the Terms of Use. All agreements relating to the website should be subject to the general terms and conditions in the website Terms and Conditions, including any limitations on liability dispute resolution and governing law provisions.

In the terms of use website owners typically specify who is eligible to use the website and the services. Many sites require users to be at least 18 years old, live within the United States (or other specified countries), and be able to form legally binding contracts under applicable law.

---

[245] *See, e.g., Stomp, Inc. v. NeatO, LLC*, 61 F. Supp.2d 1074, 1080-81 (C.D. Cal. 1999). The contents of a webpage can be protected from unauthorized access. In *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp.2d 238 (S.D.N.Y. 2000), the district court enforced the terms of agreement which took effect upon access and use of Register.com's WHOIS database and exclusive jurisdiction and arbitration provisions were enforced in *In re Real Networks, Inc. Privacy Litigation*, 2000 U.S. Dist. LEXIS 6584 (N.D Ill. 2000) in connection with an End User License Agreement on Real Networks' site.

© 2004 Piper Rudnick LLP. All Rights Reserved.

Registration obligations are usually provided. For example, users often agree to provide current, complete and accurate registration information and to maintain such information to keep it accurate, current and complete.

User conduct prohibitions are often specified:

> You are solely responsible for your transactions, posts and transmissions through this website and each of the website's services. You shall have sole responsibility for evaluating and selecting the third parties with whom you interact using this website or any of the website's services.
>
> You agree **NOT** to use the website or any of the website services for or in connection with any of the following activities:
>
> 1. tampering, hacking, modifying or otherwise corrupting the security or functionality of the services, interfering with or disrupting our network or other networks connected to the service, or posting, e-mailing, or otherwise transmitting any data that contains any software viruses, trojan horses and/or any other code, files or programs intended to destroy, disrupt or otherwise impair a computer's functionality or the operation of any service;
> 2. chain letters, pyramid schemes, or spamming;
> 3. posting, e-mailing, or otherwise transmitting any unlawful, harmful, harassing, defamatory, libelous, abusive, threatening, vulgar, sexually explicit, hateful, or otherwise objectionable material of any kind, or any material that is invasive of another's privacy or exploits children under 18 years of age;
> 4. spoofing or otherwise impersonating any person or entity, such as another user or any of our personnel, falsely stating or otherwise misrepresenting your identity or affiliation, or forging any TCP/IP packet header or any part of the header information in any e-mail or other posting;
> 5. using the services for any fraudulent or illegal purpose, or gathering personally identifiable information without prior consent;
> 6. violating any applicable local, state, national, or international law, such as laws governing financial services, export control, gambling and/or money laundering;
> 7. Interfering with another user's enjoyment of the services; or

© 2004 Piper Rudnick LLP. All Rights Reserved.

8. violating any other of our rules or policies.

We reserve the right to terminate service to you, in our sole discretion, with or without notices, if we believe that your conduct fails to conform with this Section or this Agreement, to investigate and to involve and cooperate with law enforcement authorities, and to pursue a civil lawsuit or criminal prosecution for any alleged or actual illegal activities involving this website or any of the services.

Other provisions often included in the website Terms of Use include an indemnity from the user, intellectual property provisions, warranty disclaimers, limitations on liability, dispute resolution, venue selection and general terms similar to those found in any well-drafted agreement. The Terms of Use may prove to be a very important legal strategy for managing the risks applicable to an e-commerce business. Today they are the first line of legal defense for e-commerce websites. As new risks are identified, these website Terms of Use need to be reviewed and when appropriate revised and updated to deal with the new risks.

One risk, for example, that the Terms of Use needs to recognize is the possibility of errors. Pricing goofs happen every day on the web and are a fact of e-business.[246] One way of addressing this risk is by providing that the e-commerce provider does not warrant the accuracy, usefulness, reliability, timeliness, legality or completeness of any of the information or materials provided on or through the site, and does not warrant that the site will operate error-free, or that defects, errors or omissions will be corrected, or that the site is completely secure. Nevertheless, more care is needed to guard against online errors because the consequences of those errors are available worldwide instantaneously and may result in substantial loss. Risk management related to errors in e-commerce applications requires heightened scrutiny.

---

[246] A. Oreskovic, *The Price Isn't Right*, The Industry Standard, June 4, 2001, at 70-71.

© 2004 Piper Rudnick LLP. All Rights Reserved.

DISCLAIMERS

The specific disclaimers for a website will vary based on the information content at that website and the nature of e-commerce business offered from that site.

One common disclaimer is to expressly state on the website that visitors' use of the materials on the website is at their own risk and that materials provided on the website are provided "AS IS," without any warranties as to the availability of the site or the accuracy of the materials provided. This type of disclaimer of liability is most important when providing information over a website upon which visitors may rely. The disclaimer seeks to minimize detrimental reliance by cautioning the user not to rely blindly on the information.[247]

In addition, it is appropriate to disclaim any responsibility for third-party material accessible from a website via links to other websites.[248] With respect to links, it may also be prudent to state that a company does not intend links on the website to be referrals or endorsements of the linked entities or any products or services provided by the linked entities.

Disclaimers can be drafted to deal with specific identifiable risks. These disclaimers are part of an overall strategy to manage risks. Merely placing disclaimers on the home page of a multi-page site may not be sufficient, however, since visitors can access various parts of the website directly and different parts of a website may need different disclaimers based on factors such as the content, the jurisdiction to which the portion of the site is directed, etc. It is also prudent in designing a website to provide a prominent link to website disclaimers and terms of use at the bottom of each web page to emphasize their applicability to all of the content, guard against possible deep-linking while at the same time making sure that each page from the site that is printed out by the visitor includes a reference to the disclaimers and terms of use.

Disclaimers are not, however, sufficient to protect against initial interest confusion because of a domain name.[249] Domain names are said to be like external labels. The initial interest confusion results from the external label prior to the customer reading the disclaimer.

---

[247] For example, websites that provide financial information often state that they are not responsible for the accuracy of the information contained in the site. Similarly, sometimes there are errors in the prices posted.

[248] *See, e.g., Voice-Tel Enters., Inc. v. JOBA, Inc*., 258 F. Supp.2d 1353 (N.D. Ga. 2003), in which a central claim related to a hyperlink on a franchisee's website. According to the court, the franchisee was unaware of the fact that the linked site was taken down and replaced, at the same address, by a site that was pornographic in nature. The court also noted that the franchisee removed the hyperlink once notified to do so by the franchisor. *Id*. at 1364. While the franchisor did not prevail in terminating the franchise agreement due to alleged (but according to the court, unproven) material impairment of the marks, the case illustrates how inattention to hyperlinks can cause difficulties in business relationships from the perspective of the linking party (the franchisee-defendant) and others (*e.g.*, the franchisor-plaintiff-trademark owner).

[249] *Ford Motor Company v. Ford Financial Solutions, Inc.*, 103 F. Supp.2d 1126 (N.D. Iowa 2000).

© 2004 Piper Rudnick LLP. All Rights Reserved.

CONSUMER LAWS

There are numerous advertising and consumer protection federal and state statutes applicable to e-commerce. Compliance can be particularly vexing for e-commerce companies because the state and federal requirements may differ.

On the federal level, the Federal Trade Commission has asserted its jurisdiction over any company providing goods or services online in the event the company fails to adhere to the false advertising and truth-in-advertising regulations that govern other media. The FTC has brought enforcement actions against companies who have committed fraud over the internet and for making false, deceptive or unsubstantiated claims in internet advertisements.[250] Cyveillance, an online monitoring firm, estimates that 10 percent to 20 percent of all items sold in online auctions are bogus.[251] The SEC has also been active.[252]

Fraud is a problem on the internet. The federal government has opened an Internet Fraud Complaint Center (which has since been renamed the Internet Crime Complaint Center, or "IC3"). Almost half of the complaints received by IC3 concern online auction fraud.[253] The second largest category concerns products ordered but never received. The next largest categories of internet fraud reported are securities/commodities fraud, credit card fraud and identity theft.[254]

---

[250] The FTC has brought more than 250 law enforcement actions challenging deceptive practices on the Internet. *See Federal Trade Commission Advertising Enforcement* revised by Lesley Fair, FTC, February 1, 2003. The FTC has been particularly aggressive in this area. *See, e.g., FTC v. 1268957 Ontario Inc.*, No. 01-CV-0423 (N.D. Ga. Feb. 13, 2001) (injunction obtained where company allegedly defrauded consumers into registering variations on their own domain names with the defendant); *FTC v. Carlos Pereira*, No. CV-99-1367-A (E.D. Va. Feb. 2, 2001) (injunction against internet mousetrapper and pagejacker). *See generally* the FTC's website, at *http://www.ftc.gov*.

[251] *Online Bidders, Beware*, Bus. Week, Aug. 16, 1999, at 6.

[252] *See, e.g., Federal Agency Sues PacketSwitch.com*, The Internet Newsletter, July 2001 (reporting on SEC lawsuit filed against PacketSwitch.com, alleging that the company cheated investors out of more than $3.7 million by claiming to own a new technology for broadcasting movies over the internet, when the technology was allegedly a widely available product).

[253] *See* B. Krebs, *Web Auction Fraud Tops List of 2001 Complaints*, The Washington Post, Apr. 11, 2002, at C5. eBay, Inc. obtained a court ruling that it is not liable for the sale of various bootleg and other infringing sound recordings sold through auctions on its Website. In *Stoner v. eBay, Inc.*, 2000 WL 1705637 (Cal. Sup. Ct. 2000), the California Superior Court determined that eBay was not liable for such fraudulent sales as the result of the immunity granted to interactive service providers under the Federal Communications Decency Act, 47 U.S.C. § 230.

[254] N. Knox, *Online Auctions Top List of Internet Fraud*, USA Today, Aug. 29, 2000,at 1A, 5A. *See also* L. Anderson, *They've Got Your Number*, The Industry Standard, June 4, 2001 at 74 (noting that credit card theft on the Internet is a real and pervasive problem). In the wake of the events of September 11, 2001, Congressional hearings were conducted on November 8, 2001, focusing on identity theft arising from the

(footnote continued to next page)

© 2004 Piper Rudnick LLP. All Rights Reserved.

Foreign advertising laws may also prove difficult to comply with.[255] Further, the European Union seeks to apply the laws of a consumer's jurisdiction to e-commerce transactions. For example, in France products and services must be offered in the French language and agreements must be in the French language to be enforceable. There are significant issues regarding dispute resolution for a consumer's right to cancel and what consumer laws shall apply to e-commerce transactions.

As one court observed, what makes the internet "uniquely challenging" is that "the Internet in effect allows one to speak in more than one place at the same time," thus possibly subjecting the same speech to scrutiny in more than one jurisdiction at the same time.[256]

(footnote continued from previous page)

misuse of social security numbers (SSN's) in general, and in particular SSN's assigned to persons who have died.

[255] Among other things, some countries have laws banning certain content. For example, both France and Germany ban the sale of certain Nazi memorabilia, and have taken action to block the sale of such items by companies located outside France and Germany. After a complaint was filed alleging that it was a violation of French law for Yahoo!, Inc. to allow French citizens access to the auction of Nazi memorabilia on a Yahoo.com consumer-to-consumer auction site, a French court ordered Yahoo!, Inc. to implement certain screening measures to prevent French citizens from accessing auction pages that offer such items for sale. Kristi Essick, *Yahoo Told to Block Nazi Goods From French*, The Standard (Nov. 20, 2000). Yahoo, Inc. responded by removing the objectionable items from the auction portion of its website, but has since refused to implement the judge's order to implement screening measures. Kristi Essick, *Yahoo Defies Court Ruling Over Nazi Memorabilia*, The Standard (Feb. 21, 2001).

On November 7, 2001 the U.S. District Court for the Northern District of California ordered that the First Amendment precludes enforcement within the United States of a French order intended to regulate the contents of speech on the Yahoo.com website in *Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitime*, 2001 U.S. Dist. LEXIS 18378 (at slip op. *19-20) (N.D. Cal. Nov. 7, 2001), *summary judgment granted*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); *reversed*, 2004 U.S. App. LEXIS 17869 (9th Cir. 2004) (U.S. court lacked personal jurisdiction over French defendant). In *La Ligue Contre*, the district court noted that "[w]hat *is* at issue here is whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation." (emphasis provided) The district court concluded that "this Court may not enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders." *Id.* at slip op. *19. The French court has ignored the California federal court ruling, and set January 7, 2003 for the criminal trial against Yahoo!, Inc. and its former president. Steven Bonisteel, *French Court Picks 2003 Date For Yahoo's 'Nazi' Trial*, Newsbytes (May 7, 2002) (available at *http://www.newsbytes.com/news/02/176439.html*). The trial ultimately resulted in an acquittal.

[256] *Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitime*, 2001 U.S. Dist. LEXIS 18378 (at slip op *19) (N.D. Cal. 2001), *summary judgment granted*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); *reversed*, 2004 U.S. App. LEXIS 17869 (9th Cir. 2004) (U.S. court lacked personal jurisdiction over French defendant).

© 2004 Piper Rudnick LLP. All Rights Reserved.

DIRECT SALE REGULATIONS

There are federal and state laws, which apply to the direct sale of products to consumers. These laws are applicable when products are sold directly to consumers through websites.

The Federal Trade Commission's Mail and Telephone Order Merchandise Rule applies to any product sale which the consumer orders by telephone or mail. This Rule does not apply to orders made on a C.O.D. basis. However, the FTC has expressly stated that this Rule does apply to sales through the internet because the order information is transmitted over the telephone infrastructure.

This Rule specifies the procedure that must be followed in stating shipping times and performing order fulfillment. The Rule requires companies to notify consumers if an order cannot be shipped on time. If the company cannot meet the revised shipping date, the Rule requires that the consumer be notified a second time, and unless the consumer expressly consents to the new delay, the company must cancel the order. Many e-commerce companies are believed to have violated or to be violating the Mail Order Rule.[257] In July 2000, the FTC fined a number of well-known e-tailers for promising Christmas delivery dates in 1999 they could not meet.[258] By the end of the 2001 holiday shopping season, online retailers were more responsive, yet not all were able to meet customers' expectations for service; in fact, one survey reportedly found that only 30% of online sellers responded to customer service requests in under six hours, and as many as half did not respond for over 24 hours.[259] Online retailers that have made significant investments in consumer service functions fared better; Land's End, which reportedly had over 2,500 sales representatives to help answer questions online, was among the best online sellers during the 2001 holiday shopping season.[260]

Another FTC Rule that may apply is the FTC's Telemarketing Sales Rule. The FTC has indicated that if a consumer visits a company's website in response to an e-mail advertising campaign, then the Telemarketing Sales Rule may be applicable. For any company that sends

---

[257] Stephen Caswell, *E-Tail Failures Could Trigger Federal Legal Action*, E-Commerce Times (Dec. 29, 1999). *See, e.g. United States v. Macys.com, Inc.*, (D. Del. July 26, 2000) ($350,000 civil penalty for violation of the Mail Order Rule during 1999).

[258] The FTC reached settlements with CDnow, Inc., KBkids.com LLC, Macys.com, Inc., Franklin W. Bishop d/b/a Minidiscnow.com, The Original Honey Baked Ham Company of Georgia, Inc., Patriot Computer Corp., and Toysrus.com, Inc., who agreed to change their procedures and pay, collectively, $1.5 million in civil penalties. *See* FTC Press Release dated July 26, 2000 (available at *http://www.ftc.gov/opa/2000/07/toolate.htm*).

[259] Susan Stellin, *Online Customer Service Found Lacking*, The New York Times, Jan. 3, 2002, at C4.

[260] *Id*. and Bus. Week e-Biz, Oct. 23, 2000 ("The ultimate winners in e-commerce will be the companies that focus on what happens after the order button is pushed…. You're not in the game unless you have phone operators, e-mail response, online chat, or easy-to-use online self-help.").

© 2004 Piper Rudnick LLP. All Rights Reserved.

e-mail or direct mailers, or that advertises specific products on its website, it is prudent to comply with the FTC's Telemarketing Sales Rule.

This Rule requires a company to disclose, before the purchase is completed, the cost and quantity, material restrictions, limitations or conditions, any no-refund policy, and certain information related with any contests or sweepstakes.

If the e-mail or direct mailer is advertising any prize-based promotion, then the company must disclose: (1) the odds of winning, (2) that consumers do not have to purchase any products to enter and win; (3) how consumers can enter without paying any money or purchasing any products; and (4) any material costs or conditions to receive or redeem a prize.

California has enacted a statute,[261] for example, that applies to vendors conducting business through the internet or any other electronic means of communication where the transactions involve a buyer in California. This statute requires, among other obligations, the e-commerce purveyor to disclose its refund and return policies, the legal name and address of the seller, and how to communicate with the seller by e-mail. These state laws need to be considered fully in the operation of an e-business.

---

[261] California Bus. and Prof. Code § 17538.

© 2004 Piper Rudnick LLP. All Rights Reserved.

WARRANTY DISCLOSURES AND DISCLAIMERS

There are many different state and federal warranty statutes and regulations which may apply depending on the nature of the products and services sold over the internet. The federal statutes and regulations include the Magnuson-Moss Warranty Act, 15 USC §§ 2301-2312, the Pre-Sale Availability of Warranty Rule, 16 C.F.R. § 702, and the Disclosure of Written Consumer Product Warranty Terms and Conditions Rule, 16 C.F.R. § 701. The state statutes include the Uniform Commercial Code and various consumer protection statutes.

The manner in which these statutes are complied with will differ in the online environment. One approach is to display any warranty information and disclaimers in close proximity to the product description and/or image on the site. Another approach is to place a prominently displayed button labeled "Product Warranty Information—Please Read Before Purchasing" next to the product which would link the consumer to a page displaying any warranty information. A third approach is to automatically display the terms of the warranty or disclaimer on a pop-up screen which consumers must click through if they select the button indicating that they desire to buy the product, *e.g.*, click here for warranty information to lead to the full text of the warranty.

The preferred strategy to meet the warranty requirements of conspicuousness is to display all written warranties applicable to products and all express disclaimers of implied warranties on a splash screen appearing after the customer decides to buy a product. This display should be separate from any other terms of sale, and customers should acknowledge that they have read it by clicking on the screen.

© 2004 Piper Rudnick LLP. All Rights Reserved.

ACCEPTANCE OF CREDIT CARDS

The Industry Standard has reported that 98 percent of online transactions in the U.S. are still paid for by credit card, but that alternatives – particularly person-to-person systems and micropayments – are gaining traction.[262] Current laws governing creditors and merchants who accept credit card payments will be applied to e-commerce transactions, just as they have been applied to telephone catalog sales involving credit cards. Purchase of products over the internet, in which consumers submit their orders with a credit card number, is analogous to a catalogue purchase over the telephone.

VISA and MasterCard have co-developed a Secure Electronics Transactions (SET) encryption protocol to conduct secure consumer credit transactions, using the internet as a front-end to existing computer verification networks.[263] There are also other developments to improve security of e-commerce transactions, such as through the use of "smart cards" and verification through "digital signatures." The whole area of security promises to improve greatly in coming years. Increased pressure on improving security has resulted from the increase of cybercrimes and the threat of cyberterrorism. VISA has announced ten new guidelines that require merchants to have security measures in place and Deloitte & Touche has released what they call "a worldwide benchmark for e-commerce security."[264] In a regulatory arena, a Maine subsidiary of Verizon was cited for not installing an anti-worm patch to protect its network.[265]

Digital signatures use public key encryption algorithms to verify the identity of a signatory. They are a more sophisticated form of a pin code which is harder to steal than a pin code.

Credit card fraud is a significant problem in e-commerce.[266] Even though only 5% of the credit card purchases are online purchases, 50% of all credit card fraud occurs online.[267]

---

262 *What's In Store Online*, The Industry Standard at 73 (June 4, 2001).

263 A March 2002 study on Online Payment Security by Cyveillance, Inc. found that despite credit card association policies, most e-merchants do not employ the industry standard security protocol to encrypt sensitive information transmitted during e-commerce transactions.

264 Deloitte Unveils Benchmark for E-Commerce Security, Electronic Accountant (Aug. 14, 2000).

265 *Failure to Deploy Anti-Worm Patch Was Not Reasonable Under Performance Standards*, 8 Electronic Commerce L. Rep. (BNA) 23, at 588 (June 11, 2003) (reporting on decision of Maine Public Utilities Commission).

266 Credit-card fraud is one of the top three complaints categorized by the Federal Bureau of Investigation and the National White Collar Crime Center in their annual report on internet fraud. In fact, credit card fraud comprised 11.6% of complaints lodged in 2002 with the Internet Fraud Complaint Center, up 23.4% from 2001. The average loss among the 62% of complainants that reported a dollar loss was $120. IFCC 2002 Internet Fraud Report at 5-7 (2003) (available at *http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf*).

© 2004 Piper Rudnick LLP. All Rights Reserved.

Expedia.com disclosed that it expects to lose as much as $6 million on fraudulent airline ticket purchases. These loses result mainly from credit card thieves using stolen credit cards to buy e-tickets that were picked up at the airport. By indicating that they will pick the e-tickets up at the airport they avoid a common red-flag in credit card fraud – different billing and ship to addresses.[268]

Credit card transactions over the internet are classified as "card not present" transactions when transactions happen without obtaining a signature. E-merchants must bear the risk of fraud in these sales.[269] Under current credit card rules, the e-merchants must cover the costs of any charge that the consumer says was unauthorized. This allocation of liability makes merchants with online fulfillment capabilities particularly vulnerable.[270] Many e-merchants outsource the payment process so that payment actually occurs in a separate domain. Outsourced payment processing is more likely to be secure and in accordance with the industry standard security protocol.

(footnote continued from previous page)

[267] J. Sapsford, *Survey Says Online Fraud is Increasing as More Merchants Take Steps To Fight it*, The Wall Street Journal, Nov. 3, 2000, at A2, A6 ("Sapsford"). eBay has adopted a number of programs that have greatly reduced its credit card fraud. These include customer ratings, payment escrows, fraud reimbursement, identify verification and insurance! eBay's fraud experience is about 0.1, which is approximately nine times less than credit cards generally. R. Hof, *The People's Company*, Bus. Week, Dec. 3, 2001, e.biz Section, at EB 15-16.

[268] Bus. Week, Apr. 3, 2000, e.biz Section, at EB60.

[269] Sapsford at A6.

[270] K. Caldwell, *ePayments: Is the Credit Card System, Failing eCommerce? Is a Solution in Sight*, The Public Policy Report, Vol. 3, No. 5 (May 2001).

© 2004 Piper Rudnick LLP. All Rights Reserved.

LIABILITY FOR ACTS OF HACKERS

Websites have become targets for hackers. Recently, a number of e-commerce businesses have been victimized by denial of service hacker attacks, worms and computer viruses. The most common types of attack involve the hacker visibly altering a website[271] or stealing a site's customers' credit card information and other private personal information. Cyber extortion also appears to becoming a more common problem. A business that can reasonably foresee the acts in which hackers may engage, but which fails to take reasonable precautions to prevent those acts could be held liable for the consequences. Companies must stay current and alert as to both the activities of hackers and the methods for guarding against their attacks. Security is a moving standard and is relative to the risks posed.[272] Hackers are continually getting smarter and are harder to catch. Following the bombing of the Chinese embassy in Belgrade, Yugoslavia during the U.S. military action in that country, cyberattacks successfully took down websites at the Defense Department and the White House.[273] Hackers, as well as disgruntled customers, suppliers, and employees (or spouses of any of the foregoing) may potentially launch cyberattacks. For example, a teenager admitted changing the text and images on several websites simply in order to mock the site owners.[274] This vulnerability needs to be appreciated and addressed as a matter of risk management. Hackers are continually getting smarter and are harder to catch. Computer security is expected to become more complicated as websites are programmed to collaborate with each other without human assistance.[275]

Businesses should monitor their website to ensure the content has not been altered. It may also be beneficial to increase the monitoring of other websites for trademark and copyright infringements in order to counter the activities of hackers, pranksters, pirates and infringers. In some e-commerce websites warnings such as the following have been posted: CAUTION: ANY ATTEMPT BY ANY PERSON TO DELIBERATELY DAMAGE THIS WEBSITE OR UNDERMINE ITS OPERATION IS A VIOLATION OF CRIMINAL AND CIVIL LAWS

---

271 *Teenage Hacker Admits Defacing Sites*, The Washington Post, Mar. 3, 2000, at E10 (admitted changing the text and images to mock the sites' owners).

272 *See, e.g., Microsoft, IBM Set Web Security Rules*, The Wall Street Journal, Apr. 11, 2002, at B6 (WS-Security, specification for secure web sites, announced); *see also Moulton v. VC3*, 2000 U.S. LEXIS 19916 (N.D. Ga. 2000) (explaining that a network's security is relative to the risks posed; a network might be secure for one risk, and insecure as to another). In L. Anderson, *They've Got Your Number*, The Industry Standard, June 4, 2001, at 74, the author states that 85% of e-commerce and government sites polled experienced a security breach in the past year and 13% reported that customer's credit card numbers were rendered accessible.

273 D. Frank and D. Brown, *Agencies Batten Down*, Federal Computer Week, June 7, 1999, at 1, 64).

274 *Teenager Hacker Admits Defacing Sites*, The Washington Post, Mar. 3, 2000, at E10

275 *Microsoft, IBM Set Web Security Sales*, The Wall Street Journal, Apr. 11, 2002, at B6.

© 2004 Piper Rudnick LLP. All Rights Reserved.

AND SHOULD SUCH AN ATTEMPT BE MADE COMPANY RESERVES THE RIGHT TO SEEK DAMAGES FROM SUCH PERSON TO THE FULL EXTENT PERMITTED BY LAW.

The primary Federal statutes dealing with computer crimes are the Computer Fraud and Abuse Act, 18 U.S.C. §1030, and the National Information Infrastructure Protection Act of 1996, Public Law 104-294. The laws make it a crime to knowingly or intentionally transmit damaging materials to a computer. This statute also provides a private right of action where the amount of damages from a single act is more than $5,000.[276] The minimum threshold damage amount is measured based on a single act or event, though the economic damages may relate to multiple computers and individuals that are damaged. The criminal statutes applicable to hackers may be applied to extraterritorial matters where the detrimental effect of the hacking occurs within the United States.[277]

Added concerns have been raised concerning a scheme known as "phishing." Phishing is a form of computer hacking that employs fake e-mail messages containing links to Website addresses to induce unsuspecting consumers to visit those sites and divulge personal information, on the assumption that they are verifying information or otherwise communicating with a legitimate company. Phishing scams increased significantly in the first half of 2004, and over 40% of phishing attacks come from outside the United States.[278] In a common phishing scheme, an e-mail containing a company logo or other company branding is sent to a person who transacts business with that company, asking them to visit a web page that is designed to look official, if not nearly identical, to the legitimate company's website. At the unauthorized site, the customer is asked to provide confidential information, such as his or her name, address, account information, personal information (e.g., social security numbers, birthdays), and similar detail – all of which can help the hackers steal account and identity information. While all online e-businesses are vulnerable to phishing, and while phishing attacks have been increasing dramatically, financial companies and their customers have thus far been among the most prevalent targets of these scams.[279]

---

[276] *See, e.g.*, *Ingenix, Inc. v. Lagalante*, 2002 U.S. Dist. LEXIS 5795 (E.D. La. March 28, 2002); *In re America Online, Inc. Version 5.0 Software Litigation*, 168 F. Supp. 1359 (S.D. Fla. 2001); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp.2d 1121 (W.D. Wash. 2000); *Your-Net Dating, Inc. v. Mitchell*, 88 F. Supp.2d 870 (N.D. Ill. 2000).

[277] *See United States v. Ivanov*, 175 F. Supp.2d 367 (D. Conn. 2001). Ivanov, a Russian hacker, hacked into the Online Information Bureau's computer systems in Connecticut, including OIB's merchant account database, and demand $10,000 for his assistance in making the systems more secure. He allegedly obtained the key root passwords that allowed him to control OIB's entire network.

[278] Ian Martinez, *As Phishing Scams Multiply, Officials Focus on Enforcement*, 5 Washington Internet Daily 140, July 22, 2004, at 2.

[279] *U.N. Aims to Bring Spam 'Epidemic' to End*, A.P. Report, published on nytimes.com at http://www.nytimes.com/aponline/international/AP-UN-Spam-Summit.html.

© 2004 Piper Rudnick LLP. All Rights Reserved.

SPYWARE

Spyware and other forms of monitoring software have proven quite controversial[280] and are proliferating.[281] There are nearly 1000 forms of spyware, including adware and key loggers.[282] Spyware is defined as "small programs that install themselves on computers to serve up advertising, monitor web surfing and other computer activities and carry out orders."[283] Key logging is the use of spyware to monitor a user's keystrokes and capture sensitive data.

The Federal Trade Commission conducted a workshop to examine "the issues surrounding the distribution and effects of spyware that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge."[284] The FTC expressed special interest in the issues relating to spyware disseminated through peer-to-peer software because of the widespread use of peer-to-peer file-sharing software among young people who may download it to their families' computers without their parents' knowledge.[285] Many popular file-sharing programs such as Kazaa and Morpheus come bundled with adware that serve up pop-up ads or other marketing tools as a way to subsidize costs.

WhenU.com is one of the best known adware vendors. WhenU distributes the SaveNow program used to generate contextual pop-up ads as the user is using the Internet. WhenU has a fee relationship with its advertisers, but a free relationship with the consumers who install the SaveNow adware on their computers.[286] WhenU's software to deliver ads has been installed 100 million times and uninstalled 80 million times. WhenU's contextual pop-up advertising has been

---

280 D. Bank, "What's That Sneaking Into Your Computer?" Technology, The Journal Report, The Wall Street Journal (April 26, 2004) at R1 ("Bank").

281 E. Kumler, "Spyware's Victims Spread", *How To With PCWorld.Com*, at http://tech.msn.com/howto/article_205-3.armx?GT1=3190 (last visited April 20, 2004).

282 Bank at R6.

283 *Id.* at R1.

284 Federal Trade Commission, Announcement for a Public Workshop on "Monitoring Software on Your PC: Spyware, Adware, and Other Software," April 19, 2004.

285 *Id.*

286 *See, e.g., 1-800 Contacts, Inc. v. WhenU.com, Inc.*, 2003 WL 22999270 (S.D.N.Y. Dec. 22, 2003).

© 2004 Piper Rudnick LLP. All Rights Reserved.

challenged in court.[287] In *1-800 Contacts, Inc. v. WhenU.com*,[288] the district court found that WhenU's use of "www.1800contacts.com" address to generate pop-up ads violated the "1-800 Contacts" trademark owner's rights and violated the Lanham Act. The ruling is on appeal.

One state has already enacted an anti-spyware statute.[289] This Utah anti-spyware statute has been challenged in court by WhenU.com on constitutional grounds.[290]

---

[287] *See, e.g.*, *1-800 Contacts, Inc. v. WhenU.com, Inc.*, 2003 WL 22999270 (S.D.N.Y. Dec. 22, 2003); *U-Haul International, Inc. v. WhenU.com, Inc.*, 279 F.Supp.2d 723 (E.D. Va. 2003); *Wells Fargo & Co. v. WhenU.com, Inc.*, 293 F.Supp.2d 734 (E.D. Mich. 2003).

[288] 2003 WL 22999270 (S.D.N.Y. Dec. 22, 2003).

[289] The Utah anti-spyware statute was approved during the 2004 session of the Utah legislature (H.B. 323).

[290] *WhenU.com, Inc. v. Utah*, Utah Dist. Ct. No. 040907578, complaint filed April 12, 2004 (asserting the anti-spyware statute violates the U.S. Constitution and Utah Constitution).

© 2004 Piper Rudnick LLP. All Rights Reserved.

INTERNET USAGE POLICY

Security is a very serious issue for e-commerce businesses. Employees, especially disgruntled employees, represent a serious security risk that needs to be appreciated. Former employees are considered to be the number one threat to corporate information. *Business Week* notes that 53 percent of companies have adopted an internet-usage policy. Internet usage policies seek compliance with the copyright law, protection from computer viruses and hackers, and other business objectives. They address various policy, security and potential liability concerns, including the right to monitor employees in connection with their use of the internet.[291]

Usually, these policies will provide that internet access is limited to official business. Other provisions might include a prohibition against introduction of viruses or other disabling codes, or malicious tampering with any computer system. Policies may also prohibit employees from discussing or posting messages about company business or about a competitor or competitor's products in chat rooms, bulletin boards or newsrooms. The prohibitions respecting statements about competitors or competitor products also apply to company Intranets to prevent these chat rooms from being a treasure trove of evidence in litigation with a competitor.

Monitoring is necessary because a company can be held liable for its employees' activities on the internet including unauthorized distribution of copyrighted materials as well as sending or even viewing of obscene and harassing communications.[292] One employer's usage policy indicated that the employer would "audit, inspect, and/or monitor employees' use of the internet, including all file transfers, all websites visited, and all e-mail messages deemed appropriate."[293] Furthermore, an employer may need to access the files and e-mails of an employee for the purpose of responding to law enforcement investigations, court orders or other governmental actions. Some states and collective bargaining agreements may require the written consent of the employee for the employer to engage in such monitoring. It is prudent to obtain the written consent from employees acknowledging the employer's right to engage in such monitoring.[294] In *Muick v. Glenayre Electronics*,[295] the U.S. Court of Appeals for the Seventh

---

[291] *See generally* Charles Frayer, Note, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 Bus. Law. 793 (Feb. 2002)

[292] *Garrity v. John Hancock Mutual Life Insur. Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) (employee termination upheld where employees received and forwarded sexually explicit e-mails in the office, in violation of company policy; employees had no reasonable expectation of privacy when sending e-mails that they anticipated would be forwarded to additional parties; but even if there was an expectation of privacy, it would be overridden by the employer's legitimate and statutory obligation to protect employees from harassment and a hostile environment).

[293] *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000).

[294] Some states have attempted to outlaw employer's review of their employees' e-mails. A recent attempt to do that in California failed to survive Gov. Gray Davis' veto. In his veto message, the Governor observed that: "As I previously have, when considering this issue, I start from the common-sense presumption that employees in today's wired economy understand that computers provided for business purposes are company property and

(footnote continued to next page)

© 2004 Piper Rudnick LLP. All Rights Reserved.

Circuit encouraged employers to reserve the right to inspect workplace computers as a matter of prudent risk management.[296] Other strategies to address employee risks include strict background checks for employees and training so that employees are aware of the security risks applicable to their internet practices.

Policies seek to protect the company in litigation and other disputes. Some policies also deal with e-mail etiquette and best practices. Internet usage policies are another means companies use to manage the new set of risks applicable to the internet.

(footnote continued from previous page)

that their use may be monitored and controlled. Under current law, employers are potentially liable if the employer's agents or employees use the employer's computers for improper purposes, such as sexual harassment, defamation and the like. It therefore follows that any employer has a legitimate need to monitor, either on a spot basis or at regular intervals, such company property, including e-mail traffic and computer files stored on either employer-owned hard drives, diskettes or CD ROMs." While he expressed support for a different version of the bill, Governor Davis' comments are nonetheless notable (a copy of the veto message can be found at *http://info.sen.ca.gov/pub/bill/sen/sb_0101-0150/sb_147_vt_20011005.html*). *Cf. Fischer v. Mt. Olive Lutheran Church, Inc.*, No. 01-C-0158-C (W.D. Wis. Mar. 28, 2002) (employer cannot access e-mails stored by employee in on-line Hotmail account without employee's permission).

[295] 280 F.3d 741 (7th Cir. 2002).

[296] In the *Glenayre Electronics* case, the Seventh Circuit notes that reserving the right to inspect workplace computers is common and is so far from being unreasonable that the failure to do so might well be thought of as irresponsible. Another U.S. Court of Appeals concluded that interception of employees' e-mails was not punishable under the federal Wiretap Act when the defendant reviewed the e-mails not while they were being transmitted but rather while they were stored on an e-mail server. *United States v. Councilman*, 2004 WL 1453032 (1st Cir. June 29, 2004).

© 2004 Piper Rudnick LLP. All Rights Reserved.

CYBER SECURITY

Cyber security has become a critical e-business legal issue. The risks of computer hackers, computer viruses and worms, denial of service attacks, theft, terrorist attacks, sabotage, surveillance and intrusion by competitors and malicious acts by disgruntled employees and many other vulnerabilities are increasing at an alarming exponential rate. Not only are security solutions essential for protecting information and privacy in a networked economy; they are also critical enablers for the development of e-business. Managing the risks from these unprecedented threats to the enterprise has become a vital risk management concern of the company's board of directors and top management, with the result that effective cyber security programs have become a legal necessity. Prudent risk management and due care with respect to cyber security programs are necessary to avoid potential legal liability. Cyber security is a risk management process to protect the confidentiality, integrity and availability of information systems and information content.

The Federal Trade Commission has challenged companies who have allegedly failed to provide adequate information security and misrepresented the level of security protection for consumer information.[297] In these FTC consent orders, the respondent companies were each required to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The FTC required the respondents in these matters to maintain an information security program containing administrative, technical and physical safeguards appropriate to the respondent company's size and complexity, and the nature and scope of its activities.[298] Adequate security means that companies maintain effective security that is commensurate with risk, including the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, impairment, modification or destruction of information. Information security programs ensure the confidentiality, integrity and availability of the company's information systems and information. The FTC prescribed four steps that should be implemented in an information security program.[299] Information security programs should be evaluated with these four steps in mind:

1. Accountability. Companies should designate an employee or employees to coordinate and be accountable for the information security program.[300]

---

[297] *In the Matter of Guess? Inc.*, File No. 0223260 (FTC Aug. 5, 2003); *In the Matter of Microsoft Corp.*, File No. 0123240 (FTC Dec. 24, 2002); *In the Matter of Eli Lilly and Co.*, File No. 0123214 (FTC May 10, 2002).

[298] *Id*.

[299] *Id*.

[300] *Id*.

© 2004 Piper Rudnick LLP. All Rights Reserved.

2. Risk Assessment. Companies should identify material internal and external risks to the security, confidentiality, and integrity of information that could result in the unauthorized disclosure, misuse, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment will include consideration of the risks in each area of relevant operation, including: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.[301]

3. Safeguards. Companies should design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.[302]

4. Maintenance. Companies should evaluate and adjust their information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances the company knows or has reason to know may have a material impact on its information security.[303]

Another FTC cyber security matter is also worth noting. Tower Records was charged by the FTC based on "a security flaw in the Tower website" that allegedly "exposed customers' personal information to other Internet users in violation of Tower's privacy policy representations and federal law."[304] In particular, the FTC charged "that the security flaw was easy to prevent and fix, but that Tower failed to implement appropriate checks and controls in the process of writing and revising its Web applications; adopt and implement policies and procedures to test the security of its website; and appropriate training and oversight for its employees."[305] In settling the FTC's charges against Tower, the FTC noted: "Companies must have reasonable procedures in place to make sure that changes do not create new vulnerabilities."[306] The FTC settlement requires Tower to establish and maintain a comprehensive information security program that must be certified as meeting or exceeding the standards in the consent order by an independent professional within six months, and every other

---

[301] *Id.*

[302] *Id.*

[303] *Id.*

[304] Federal Trade Commission Press Release dated April 21, 2004, subject: "Tower Records Settles FTC Charges".

[305] *Id.*

[306] *Id.* One of the concerns with computer software is that changes to one portion of a program may have consequences in other portions of a program. Changes may have security consequences. These potential consequences need to be appreciated.

© 2004 Piper Rudnick LLP. All Rights Reserved.

year thereafter for a period of ten years.[307] The settlement also contains record-keeping provisions to permit the FTC to monitor compliance.[308]

A recently published checklist developed by the Better Business Bureau, the National Cyber Security Alliance and the Federal Trade Commission recommends a detailed computer security audit twice a year and routine checks throughout the year.[309] The checklist includes the following recommendations:

1. Maintain a password protection program using cryptic passwords that are changed at least every 90 days.

2. Use virus protection software on all computers, ideally software that updates itself each week.

3. Install firewalls at every point where the computer system is connected to other networks.

4. Install software security patches upon release. Check software vendor sites for security patches or use automated patching programs.

5. Back up all computer data at least weekly, including work done on individual computers.

6. Check routinely for suspicious activity reported on firewall, encryption and password logs.

7. Recognize the risks from file-sharing. Consider turning off the file-sharing function and barring employees from installing file-sharing software.

8. Consider using encryption software to protect data even if someone cracks the firewalls.

9. Educate employees on wise e-mail practices and backup procedures, and advise them to disconnect from the Internet when not using it.[310]

---

[307] *Id.*

[308] *Id.*

[309] "Network Security", BNA Electronic Commerce & Law (April 21, 2004) at pp. 382-383.

[310] *Id*

© 2004 Piper Rudnick LLP. All Rights Reserved.

ANONYMITY

Due to the anonymous nature and virtual aspects of online commerce, the potential for abuse in e-commerce is higher than other forms of commerce. The absence of face-to-face contact or actually being able to inspect the goods before they are purchased makes e-commerce more likely to be the subject of abuse. Product returns are more of a problem in e-commerce and need to be fully considered.

In some situations a company may need to determine when it may be dealing with someone (such as a minor) who only has the capacity to enter into voidable contracts. In the case of export control compliance, a company will also want to confirm that it is not dealing with a foreign national, resident of one of the then-current prohibited countries under the U.S. export control laws. In all cases, a company must take steps to be sure that it is not transacting with a party appearing on the annex to Executive Order 13224, issued by President Bush following the September 11, 2001 attacks, blocking transactions with certain suspected terrorist groups and persons.[311]

Many user names are pseudonyms or pen names that often provide users with a distinct online identity and help to preserve their identity. Many believe that this anonymity of the communicant is both important and valuable to the free exchange of ideas and information on the internet. Legislative attempts to prohibit this anonymity on the internet have failed and courts have recognized that the First Amendment to the U.S. Constitution protects individuals' rights to engage in anonymous speech.[312]

Anyone who can gain access to another person's e-mail account, password, or pin number may have the ability to use that information to impersonate the legitimate user. In some e-commerce applications, this creates special risks. For example, spouses have "emptied" their spouse's e-bank accounts and sold all of the stock in their e-brokerage accounts. Some spouses have sought to hold their e-banks and e-brokerages accountable for these "unauthorized" transactions. One investor successfully sued his e-brokerage firm for the losses he incurred because the e-broker did not comply with its margin account requirements when they allowed him to trade on a margin account. The anonymity problem exacerbates these risks.

Parties can be injured by torts that are committed online pseudonymously or anonymously. Tortfeasors have also been know to provide fictitious or incomplete identifying

---

[311] The annex has been supplemented and can be found on the Treasury Department's website at *http://www.treasury.gov/offices/enforcement/ofac/sanctions/terrorism.html*.

[312] *See Buckley v. Amer. Constitutional Law Fund*, 525 U.S. 128 (1999), and *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995). In *Doe v. 2TheMart.com*, No. C01-453Z (W.D. Wash. Apr. 26, 2001) (citing *Seescandy.com*) and *Columbia Insur. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999), the courts applied the same free speech principle to anonymous postings on the internet. In both the *2TheMart* and *Seescandy.com* cases, the courts wrestled with whether to order a third party to comply with a subpoena that sought to reveal the identity of an anonymous poster.

© 2004 Piper Rudnick LLP. All Rights Reserved.

information to their ISP's, domain name registrars, and others.[313] Tracking down the tortfeasor under these circumstances can be quite difficult.[314]

In a unique attempt to uncover the names of parties that allegedly made defamatory and disparaging statements in an internet chat room, one company filed a lawsuit, anonymously, against various anonymous parties (John Does 1 through 5), in an attempt to discover the identities of the posting parties, whom the plaintiff alleged may have been former or current employees that posted information in breach of their fiduciary duties to the company.[315] The company alleged that it had to proceed anonymously, for fear that to do otherwise would cause it irreparable economic harm. The plaintiff sought to enforce the original subpoena, which was issued by the Indiana courts, in Virginia. While the lower court in Virginia concurred, America Online appealed and the case was heard by the Virginia Supreme Court. The Virginia Supreme Court noted that:

> "The ultimate test for permitting a plaintiff to proceed anonymously is whether the plaintiff has a substantial privacy right which outweighs the customary and constitutionally-embedded presumption of openness in judicial proceedings. It is the exceptional case in which a plaintiff may proceed under a fictitious name."[316]

---

[313] *See Felsher v. Univ. of Evansville*, 755 N.E.2d 589, 601 (Ind. 2001) (affirming lower court's issuance of an injunction against defendant's unauthorized use of other persons' names and likenesses in e-mail addresses and websites).

[314] *See Melvin v. Does*, Civ. No. GD99-10264 (Penna. Ct. C.P., Allegheny Cty., Nov. 15, 2000) (allowing discovery to determine identity of anonymous defendant in libel action); *Columbia Insur. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999) (pre-service discovery procedures to identify anonymous online tortfeasor authorized). As of April 27, 2001, Laura Heymann, who handles civil subpoenas for America Online, noted that AOL, with about 29 million subscribers, is handling about 500 civil subpoenas from third parties a year and about 500 criminal subpoenas a month. The principal request sought by these subpoenas is to identify the identity of a person who use an e-mail address. *See also Dendrite Int'l Inc. v. John Doe No. 3*, 2001 N.J.Super. LEXIS 300 (Sup. N.J. App. Div. 2001); *Immunomedics, Inc. v. Jean Doe*, 2001 N.J. Super. LEXIS 299 (Sup.Ct. N.J. App. Div. 2001).

[315] *America Online, Inc. v. Anonymous Publicly Traded Company*, 542 S.E. 2d 377 (Va. 2001), *reversing In re Subpoena Duces Tecum to America Online, Inc*., 52 Va. Cir. 26 (Va. Cir. Ct. 2000). In *Doe v. 2TheMart.com, Inc*., No. C01-453Z (W.D. Wash. Apr. 26, 2001), the court set out a four-part test to be met by a plaintiff seeking to establish the identity of an anonymous poster to a website: "[1] the subpoena seeking the information was issued in good faith and not for any improper purpose, [2] the information sought relates to a core claim or defense, [3] the identifying information is directly and materially relevant to that claim or defense, and [4] information sufficient to establish or to disprove that claim or defense is unavailable from any other source."

[316] *Id.* at slip op. 15 (citations and internal quote marks omitted).

© 2004 Piper Rudnick LLP. All Rights Reserved.

The court concluded that:

> The limited situations in which a plaintiff has been permitted to proceed under a pseudonym involve the presence of some social stigma or the threat of physical harm to the plaintiffs … A common threat throughout these decisions is that the likelihood of the plaintiff suffering some embarrassment or economic harm is not enough by itself to permit anonymity."[317]

Another strategy for dealing with the added risks associated with anonymity is to make the website customer expressly aware of the risk with a cautionary warning. Some terms of service today identify the risks of dealing across national borders, with underage persons, or with people acting under false pretense. These terms also are acknowledging that because user authentication on the internet is difficult that the website does not confirm that users are who they claim to be. Contractually the customer is made responsible for choosing with whom to transact business and for what. eBay provides an identity verification program.[318]

---

[317] *Id.* at slip op. 16 (citations and internal quote marks omitted).

[318] R. Hof, *The People's Company*, Bus. Week, Dec. 3, 2001, e.biz Section, at EB15-16.

© 2004 Piper Rudnick LLP. All Rights Reserved.

EXPORT CONTROLS

One concern with the fact that websites are available to anyone, anywhere with access to the internet is the United States' export control laws. The United States maintains a list of "prohibited" countries. U.S. regulations impose restrictions on transactions with these prohibited countries, and specially designated terrorism sponsoring organizations and narcotics traffickers. All country and entity lists are subject to change by the U.S. Government. End user restrictions apply to individuals and entities identified by the U.S. Government in the Federal Register from time to time. Direct and indirect exports to some of these countries are prohibited. Due to the fact that there are no country borders on the internet, fulfilling this export control prohibition may require a company to block orders placed from within these prohibited countries.

Compliance with the export laws extends beyond the prohibited country to nationals from such prohibited countries. The definition of "export" includes publication on the internet unless steps are taken to restrict foreign access to the internet site. The fact that people deal with anonymity over the internet may make strict compliance very difficult.

The export control laws also need to be considered in connection with electronic distribution. To address these risks many companies use electronic distribution compliance statements affirmatively acknowledging in a click-wrap agreement that the user is not a national of one of the embargoed countries or a party that is listed in the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals and will comply with the United States and other applicable country laws and regulations when either exporting or re-exporting or importing the e-commerce product or any underlying information or technology.

The following example suggests some additional export considerations that may need to be addressed:

> Export Restrictions. This website is controlled and operated by Company from its offices within the United States. Company makes no representation that the Products or other materials accessed through this website are appropriate or available for use in other locations, and access to them from other countries where their contents are illegal is prohibited. Those who choose to access the Products or the website from other locations do so on their own volition and are responsible for compliance with applicable local laws. You may not export or re-export any Product received under this Agreement except in full compliance with all United States laws and regulations. In particular, the Products may not be exported or re-exported into (or to a national or resident of) any country to which the United States embargoes goods, or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders). In addition, you are responsible for complying with any local laws in your country, which may impact your right to import, export or use the Product.

© 2004 Piper Rudnick LLP. All Rights Reserved.

TRUST AND CONFIDENCE

E-business purveyors need to obtain the trust and confidence of their e-customers. Consumers are looking for a trusted e-tailer that will give them the feeling of safety and security the customer is looking for.[319] Because of the nature of the internet and anonymity involved in e-transactions, trust and confidence are critical to obtaining e-customers and e-customer relationships.[320] Power outages and computer failures contribute to a lack of confidence and mistrust. Significant downtime can do unquantifiable damage to a brand name. Likewise, concerns over misuse of personal data collected through e-business transactions online fraud militate against establishing the necessary trust relationship.[321] Concerns have been raised that adware undermines consumer trust.[322]

Legal strategies should be adopted consistent with building the desired trust and confidence. Maintaining appropriate policies will help contribute to establishing a trust relationship. Fair, reasonable and consumer-friendly website terms of use agreements and click-wrap agreements in easy to understand legalese will also help. Easy access to privacy policies, warranty information and support information provides better disclosure and helps build customer trust and confidence. Giving customers the option to encrypt their communications with the e-commerce purveyor will also help. Reliable systems for accrediting e-buyers and e-sellers will promote confidence in their ability to deliver products, quality and payment. Another approach to help build consumer trust are certification and seals of approval programs. These will increase in the future. Consumer confidence in e-business requires adequate security,

---

[319] E. Neuborne, *It's All About Trust*, Bus. Week, Dec. 3, 2001, e.biz Section, at EB10.

[320] A survey of European online shoppers conducted by Forrester Research rated a Website's security of payment and privacy policy ahead of ease of ordering online and cost of delivery – let alone prices themselves – as the top two factors in choosing to buy from an online retailer. *See Santa's Helper's: Retailers are the top performers online*, The Economist, May 15, 2004 at *Survey of E-Commerce* 5-6 (table 3). In an interesting twist, a court noted how important trust and confidence could be to a Website operator. In *Electronics Boutique Holdings Corp. v. Zuccarini*, 56 U.S.P.Q.2d (BNA) 1705 (E.D. Pa. 2000), *motion to set aside denied*, 2001 U.S. Dist. LEXIS 765 (E.D. Pa. 2001), the court noted that Zuccarini's mousetrapping activities to trap visitors based on misspelled domain names had an adverse effect on Electronic Boutique's website business, which was built on user-friendliness and trust, essential components of a successful online business. On September 25, 2001 the FTC filed a complaint against Zuccarini, a purported cyberscammer, alleging three counts violating Section 5 of the FTC Act; *FTC v. Zuccarini*, Civ. 2002 U.S. Dist. LEXIS 13324 (E.D. Pa. April 10, 2002). *See* the discussion of this case in the text under the heading "Domain Names and Cybersquatting," *supra*.

[321] A comprehensive survey conducted by Ipsos-Reid reported that potential online credit card fraud is a major concern for 46% of adults around the world and a moderate concern for 26%. *Online Fraud – Though Victim Percentage is Low, Fear is High*, eMarketer, June 29, 2001. Numerous other reports have shown similar levels of distrust in Internet security.

[322] Michael Totty, *Pesky Pop Up Internet Ads Go Mainstream, as Adware Gains Acceptance*, The Wall St. J., Jun. 22, 2004, at B1.

© 2004 Piper Rudnick LLP. All Rights Reserved.

respect for privacy, and protection from unfair deceptive and fraudulent commercial conduct.[323] Another strategy is to develop a user-friendly dispute resolution program that contains a customer protected fee and is largely paid for by the business entity. Legal procedures, if undertaken properly and fairly, can help e-business purveyors create and maintain the necessary trust and confidence to develop a strong e-brand. While trust and confidence are not legal considerations as such, they should serve among the objectives for implementing a well considered legal strategy. Brand names are much more important in e-business. It is the customer experience with the site that creates the brand.[324] E-business and other internet applications will never reach their full potential unless consumers and other users can go online with confidence.[325] For obvious reasons – including the lack of proximity between buyer and seller – trust has emerged as a critical factor in e-business success.[326]

---

[323] *See* "Leadership for the New Millennium: Delivering on Digital Progress and Prosperity," The U.S. Government Working Group on Electronic Commerce, 3rd Annual Report (2000) at 35.

[324] EBay has become a hub for global e-commerce. In 2003, 30 million people bought and sold $20 billion in merchandise through the eBay market. *See* Robert Hof, *The eBay Economy*, Bus. Week 125 (Aug. 25, 2003). EBay works on building a powerful brand. The eBay system includes a feedback system, fraud police, payment processing, polls of customers, services to keep customers happy and a "Voice of the Customer" program.

[325] *Id.* at xii.

[326] E. Neuborne, *It's All About Trust*, Bus. Week, e.biz Section, at EB10 (Dec. 3, 2001). Here the author argues that a trust relationship is more important than price discounts and that companies need to incorporate a trust-mindset into their marketing messages to drive traffic to their sites.

© 2004 Piper Rudnick LLP. All Rights Reserved.

DIGITAL SIGNATURES

Digital signatures are often confused with electronic signatures. The terms tend to be used interchangeably even though there are significant differences. An "electronic signature" may be any symbol or mark originated electronically with an intent to authenticate an action. A "digital signature" employs public key cryptography to ensure the integrity of a document during transmission. Documents sent employing this methodology are sent after being signed and encrypted with a private key that only the signer possesses. The resulting encrypted document is termed a "digital signature".

The recipient of this encrypted document uses a public key to decrypt the document. This public key may be in the possession of multiple parties. Public key cryptography provides the foundation for secure electronic commerce transactions using digital signatures.

The verifier of a digital signature may easily determine if the digitally signed data has been altered since it was signed. Digital signatures also provide non-repudiation protection because digitally signed documents cannot have signatures denied successfully.

Further protection is available through digital certificates. A digital certificate may be used to verify the authenticity of a digital signature. Digital certificates are issued by a certification authority who performs a function similar to a notary public by verifying the identity of the signer.

© 2004 Piper Rudnick LLP. All Rights Reserved.

ADVERTISING LAW

The Internet is rapidly coming of age as an advertising medium. Paid search ads are the fastest growing form of paid advertising. These ads are popular because they are interactive and the metrics provide an effective means for assessing success.[327] Internet advertising spending in 2003 rose 20% to $7.2 billion and by 38% in the fourth quarter of 2003.[328] Web ad spending will grow an estimated 23% in 2004.[329] E-business companies are spending substantially on both online and offline advertising to create a strong e-brand on the internet. In 2003, web advertising began to rebound rising to $3.2 billion in the first six months from $2.8 billion for the first six months in 2002.[330] It is estimated that about 5,700 companies are advertising online, and that about 75% of these are internet firms.[331] In the fourth quarter of 2000 approximately 40% of net ad spending went to banner ads,[332] while approximately 31% of the online ad market was spent on site sponsorships.[333] Recent studies show that streaming-media ads were almost five times more effective than simple banner ads.[334] In 2002, 23% of the internet advertising revenues are related to search results.[335] Animated and search-related ads continued their popularity into

---

[327] A. Bianco, *The Vanishing Mass Market*, Bus. Week, July 12, 2004, at 61, 64-65.

[328] L. Walker, "Yahoo's lst-Quarter Profit, Revenue Rise," The Washington Post, April 8, 2004, at E5 ("Walker").

[329] M. Mangalindan, "After Wave of Disappointments, The Web Lures Back Advertisers," The Wall Street Journal, Feb. 25, 2004, at A1.

[330] M. Mangalindan, *Web Ads on the Rebound*, The Wall Street Journal, Aug. 25, 2003, at B1, B6 ("Mangalindan"). Another example is the automotive industry. In 2003, auto makers spent $9.5 billion in advertising, a 6.2% increase from 2002, but spending on the internet by 44.3%, to just over $110 million. In contrast, spending on network television dropped by 2.1%, to $2.6 billion. L. Geist, *Carmakers bumped ad spending 6.2% in 2003*, Automotive News, Apr. 12, 2004, at 17.

[331] L. Carr, *Metrics: 100 Numbers You Need to Know*, TheStandard.com, Nov. 13, 2000 (citing Arrelevance, Oct. 2000).

[332] *Compare* O'Connell *with Making Online Ads Click*, The Industry Standard, Dec. 18, 2000, at 123.

[333] In the O'Connell article, she also notes that in the fourth quarter of 2000 about 10% of online ad revenues were generated by classified ads, 5% by interstitials (ads that occur between two content pages), 4% from e-mail ads, 2% from key word advertising, and 2% from rich media advertising. O'Connell, *supra*.

[334] *Making Online Ads Click*, The Industry Standard, Dec. 18, 2000, at 122-23.

[335] B. Elgin and T. J. Mullaney, *Search Engines Are Picking Up Steam*, Bus. Week, Mar. 24, 2003, at 86.

© 2004 Piper Rudnick LLP. All Rights Reserved.

2003.[336] Among the fastest growing segments in 2003 were web search ads, consisting of text ads shown beside search results.[337]

Advertising claims on the internet are subject to the same legal requirements as print, television and other forms of advertising. The advertising claims must not be false or misleading. Objective advertising claims must be substantiated and otherwise comply with the Federal Trade Commission (FTC) advertising rules and regulations. Advertisers should review online ads from the perspective of a reasonable consumer, and assume that consumers do not read every word on a printed page.[338] On May 3, 2000, the FTC released a staff working paper "dot com Disclosures: Information About Online Advertising" reiterating that the rules and guides that apply to written ads and printed materials apply to visual text displayed on the internet, with special emphasis on any required disclosures.[339]

The FTC's "dot com Disclosures" paper applies to online sales and advertising. The FTC emphasizes that disclosures are needed to prevent an ad from being misleading and to ensure consumers get the material information they need. The following FTC guidelines will assist in determining whether the disclosures are sufficiently clear and conspicuous on the internet:

(1) The placement of the disclosure in an advertisement. Place disclosures near, and when possible, on the same screen as the triggering claim. Use text or visual cues to encourage consumers to scroll down a Web page when it is necessary to view a disclosure. A scroll bar on the side of a computer screen is not a sufficiently effective visual cue.

(2) The proximity of the disclosure to the claim it is qualifying. Display disclosures prior to purchase, but recognize that placement limited only to the order page may not always work.

(3) The prominence of the disclosure. Prominently display disclosures so they are noticeable to consumers and evaluate the size, color and graphic treatment of the disclosure in relation to other parts of the Web site.

(4) Whether items in other parts of the advertisement distract attention from the disclosure. Review the entire ad to ensure that other elements such as text,

---

[336] Mangalindan at B1, B6.

[337] Walker at E5.

[338] Joseph P. Lavelle and Marc G. Schildkraut, *Dot Com Disclosures*, 2 Internet Law & Business at 203, 206 (Jan. 2001).

[339] *FTC Issues Guide to Warn Business of Agency Rules Applying to Internet Ads*, Antitrust & Trade Regulation Report (BNA) at 447 (May 5, 2000).

© 2004 Piper Rudnick LLP. All Rights Reserved.

graphics, hyperlinks or sounds do not distract consumers' attention from the disclosure.

(5) Whether the advertisement is so lengthy that the disclosure needs to be repeated. Repeat disclosures, as needed, on lengthy Web sites and in connection with repeated claims.

(6) Whether disclosures in audio messages are presented in an adequate volume and cadence. Use audio disclosures when making audio claims, and present them in a volume and cadence so consumers can hear and understand.

(7) The duration of visual disclosures. Display visual disclosures for duration sufficient for consumers to notice, read and understand them.

(8) Whether the language of the disclosure is understandable to the intended audience. Use clear language and syntax so consumers understand the disclosures.

The FTC paper also provides the following guidelines when employing hyperlinks to lead to disclosures.

(1) Make the link obvious.

(2) Label the hyperlink appropriately to convey the importance, nature and relevance of the information it leads to. The hyperlink should give consumers a reason to click on it.

(3) Asterisks or other symbols by themselves may not be effective. Typically, they provide no clues about why the claim is qualified or the nature of the disclosure.

(4) In most cases, simply hyperlinking a single word or phrase in the text of an ad may not be effective.

(5) Use hyperlink styles consistently so that consumers know when a link is available.

(6) Place the hyperlink near relevant information and make it noticeable. Typically, this means the hyperlink is adjacent to the triggering term or other relevant information. Format, color or other graphics treatment also can help to ensure that consumers notice the link.

(7) Take consumers directly to the disclosure on the click-through page.

(8) Assess the effectiveness of the hyperlink by monitoring click-through rates and make changes accordingly. Tools are available to allow advertisers to evaluate the effectiveness of disclosures through hyperlinks. Advertisers also can evaluate the amount of time visitors spend on a certain page, which may indicate whether consumers are reading the disclosures.

© 2004 Piper Rudnick LLP. All Rights Reserved.

(9) Hyperlinked disclosures may be particularly useful if the disclosure is lengthy or if it needs to be repeated (because of multiple triggers, for example).

The FTC has cautioned advertisers on their use of banner ads as teasers. The FTC stated that the following considerations should apply:

(1) Disclose required information in the banner itself or clearly and conspicuously on the Website it links to. In determining whether the disclosure should be placed in the banner itself or on the website the banner links to, advertisers should consider how important the information is to prevent deception, how much information needs to be disclosed, the burden of disclosing it in the banner ad, how much information the consumer may absorb from the ad, and how effective the disclosure would be if it was made on the website.

(2) Use creativity to incorporate or flag required information. Scrolling text or rotating panels in a banner can present an abbreviated version of a required disclosure that indicates that there is additional important information and a more complete disclosure available on the click-through page.

(3) Provide any required disclosures to interactive banners. Some "smart" banner ads allow consumers to interact within the banner, so that they may conduct a transaction without clicking through to a website. If consumers can get complete information about a product or make a purchase within an interactive banner, all required disclosures should be included in the banner.

The FTC cases relating to the internet involve a broad range of deceptive practices, including, deceptive promotion, hidden contract terms, and deception in the collection and use of personal information. The FTC has prosecuted companies that engage in e-commerce for failing to adhere to the false advertising and truth-in-advertising regulations that govern other media. The FTC has focused on deceptive internet health claims, pyramid schemes, credit scams, auctions, business and investment opportunities and technology based scams, including spam, web cramming, hijacking modems and websites. The Food & Drug Administration (FDA) has also been active with respect to deceptive internet advertising regarding drugs and medical cures. Most of the online "auction" scams involve a failure to deliver the merchandise after the consumer "wins" the auction and sends in their money.

In online advertising a company must be careful not to violate the publicity rights of celebrities by appropriating their likenesses without proper authorization. Because of the ease of capturing images on the internet, this is becoming much more of a concern.

Key word advertising has generated litigation. In key word advertising a company can purchase from a search engine the right to display banner ads in response to search results when a certain key word is searched. In some cases, companies have purchased a competitor's trademark as a key word resulting in litigation.

There are many issues that arise in connection with internet advertising. For example, among the factors to be considered are whether the ads be targeted or untargeted? The size,

© 2004 Piper Rudnick LLP. All Rights Reserved.

placement, content and time of delivery of ads are all important. As a general rule, banners, buttons and pop-up windows are more desirable that plain text links which tend not to catch the users attention. Another factor to examine is the prominence of the advertisement – in other words, will the ad be "above the fold" or "below the fold" *(e.g.*, will the ad be immediately visible on the page or will a you have to scroll down to read it).

One form of online advertising – the so-called "pop-up" ad – has long since drawn consumers' ire and, therefore, commercial fire. One observer noted that "[t]here is a consumer revote as forms of advertising get more intrusive."[340] Indeed, pop-up advertising has become so vexing that several major companies now provide software free of charge to block pop-up ads, and Microsoft will include enhanced an pop-up blocking function in the summer 2004 release of Internet Explorer.[341] Microsoft and Time Warner have gone further by refusing to sell pop-up and pop-under ad opportunities on their MSN and AOL systems in the U.S. and in February 2004, Microsoft announced that it would phase out similar ads on its European MSN service.[342]

Pop-up blocking software will apparently not preclude another form of online advertising – the paid video commercial – which loads in the background while the user reads a webpage.[343] With the growth of broadband connections, the video quality of these ads can be almost the same as that of television.[344] While the first batch of these commercials are designed to be unobtrusive and consumer-friendly (*e.g.*, a viewer can close the ad and not view the entire video), that may not be a feature of future such ads, which may face a fate similar to that of pop-up ads.

---

[340] Saul Hansell, *As Consumers Revolt, a Rush to Block Pop-Up Online Ads*, The New York Times, Jan. 19, 2004, at C1, C4 (quoting Rob Kaiser, vice president for narrowband marketing at EarthLink).

[341] *MSN to swat pop-ups in Europe*, c|net news.com (Feb. 13, 2004) (available at *http://news.com.com/2100-1024_3-5158977.html*).

[342] *Id*.

[343] Bob Tedeschi, *E-Commerce Report-Your Web surfing is being interrupted to bring you a paid video commercial. Advertisers think you will stick around*, The New York Times, Jan. 19, 2004, at C7.

[344] *See generally* M. Graven, *The Broadband Lifestyle*, PC Magazine, Sept. 21, 2004, at 105.

© 2004 Piper Rudnick LLP. All Rights Reserved.

SWEEPSTAKES AND PROMOTIONS

Sweepstakes and promotions is one particular advertising area on the internet that deserves special attention. The competition for e-commerce traffic is fierce. Many e-commerce sites seek to increase traffic through contests and sweepstakes. Some of the most popular websites are the sweepstakes sites. Sweepstakes sites are the fastest growing segment of the consumer internet.[345] There is concern over the effect of state lottery laws on online sweepstakes. Sweepstakes pose specific concerns under the lottery laws. Websites need to be aware that such contests are highly regulated by individual states, many of which have different definitions of what constitutes unlawful gaming.

A sweepstakes promoter typically avoids lottery laws by eliminating the consideration element. Very often the promoter will eliminate the purchase or payment requirement and allow consumers to participate free. A contest or game of skill also avoids the lottery laws as long as it is a game of skill because the element of chance is therefore eliminated. Some commentators believe that eliminating the consideration element might be difficult so they recommend that consumers be able to enter through an off-line alternative means such as by postcard or calling a toll-free number. Companies should make sure to offer a free means of entering sweepstakes other than by visiting the website. The foregoing alternative ways of entering the sweepstakes should be considered.

Sweepstakes should be limited to participants who already have internet access before the sweepstakes begins officially, so that the sponsor will be in a position to contend that a participant did not invest in internet services or resources to enter the contest. The sweepstakes should exist in a text version any browser can read so that participants in the contest do not have to use any particular software or browser.

There are a number of states that are very tough on sweepstakes. Companies may want to consider excluding residents of some states from entering. For example, Florida and New York require sponsors of sweepstakes or games of chance where the total value of the prizes exceeds $5,000 to register the promotion in their states and make a deposit or post a bond to cover the value of prizes. Certain states (*e.g.*, Maryland, Massachusetts Michigan, New Mexico, New York and Texas) require disclosure of the number, value and description of the prizes, and certain other states (*e.g.*, Maryland, Massachusetts and New Mexico) require disclosure of the odds of winning.

For all types of promotions, rules serve as a "contract" between the sponsor and participants, and therefore it is important that they contain all the terms and conditions regarding the promotion and be as detailed and clear as possible. Certain terms, such as a description of the prizes, their approximate retail values, odds of winning, and where a winners' list may be

---

[345] M. Williams, *Monkey See*, The Wall Street Journal, Apr. 23, 2001, at R32 (participants are willing to give marketing information for the chance to win big); Timothy Mullaney, *Web Lotto: it ain't pretty*, Bus. Week, May 15, 2000, e.biz Section at EB 122.

© 2004 Piper Rudnick LLP. All Rights Reserved.

obtained, are mandated by law. Other terms including, but not limited to, the methods of entry (including a free method of entry); eligibility requirements such as age, residence and exclusion of parties related to the sponsor; the promotion and dates; and methods of determining winners are also necessary to explain or outline the restrictions concerning participation. Games, internet promotions, and skill contests have additional required disclosures.

These additional disclosure rules applicable to internet promotions are as follows:

(1) Complete the online official entry form and send it electronically by 11:59:59 p.m. [time zone] on [date]. (It is important to include a time and time zone.)

(2) Sponsor is not responsible for malfunctions of electronic equipment, computer hardware or software, or lost, late illegible, incomplete or misdirected entries.

(3) Sponsor is not responsible for problems downloading entries from the website or for any other technical problems related to website entries.

(4) There is a limit on the number of entries (*e.g.*, one entry per email address.)

(5) Sponsor reserves the right to modify, suspend or terminate the sweepstakes in the event that it becomes infected by a computer virus or is otherwise technically impaired. (If the promotion has an alternate method of entry, then sponsor may limit this to internet portion only, if possible.)

(6) In order for electronic entry to be valid, entrants must click on the "I accept" button the website.

(7) In the event of a dispute regarding the identity of the person submitting an online entry, the entry will be deemed to be submitted by the person in whose name the email account is registered.

(8) By entering, entrants give their express permission to be contacted by sponsor by email. This is required in California and Nevada.

(9) This promotion is offered on to [fill in] and is governed by the laws of the United States, with venue in [country, state], and all claims must be resolved in the United States.

For any type of promotion, changing the rules once the promotion has commenced is dangerous; for example, a change may not only risk running afoul of state laws, but may also violate the "contract" created with entrants. For example, a sweepstakes should not be extended or cancelled nor is it advisable to provide for such possibilities in the rules. Finally, the rules must be available to participants <u>prior</u> to entry in the same way a contract must be read before being signed so the parties understand in advance of committing themselves, what terms and conditions are going to control the relationship.

For online promotions, we recommend having a statement on top of the Official Rules that states: "This Sweepstakes is intended only for residents of [Insert the Country/Countries]

© 2004 Piper Rudnick LLP. All Rights Reserved.

Who Are Located in [Insert the Countries] at time of entry." This statement should be all caps and boldfaced. The official sweepstakes rules in a sweepstakes run by Perfumania and perfumania.com (the "Company") are an example of how some of these additional disclosure rules for the internet may be handled. These rules, in addition to the off line methods of entering, provided that to enter on the internet "visit the website [URL of company website] and follow the on-screen directions to fill out the drawing entry form. . . ." The rules also note that the sweepstakes company is not responsible for electronic transmissions and/or entries that are lost, late, stolen, mutilated, incomplete, illegible, damaged, garbled, destroyed, delayed or misdirected, and any problems or technical malfunctions, errors, omissions, interruptions, deletions, defects, delays in operation of transmission, communication failures, destruction or unauthorized access to, or alteration of, entries. For internet entries, prizes are awarded to the authorized account holder of the e-mail address submitted. The Authorized account holder is defined as the person who is assigned to an e-mail account by an Internet Service Provider. Prize winners may be notified by e-mail or by mail. The sweepstakes company reserves the right to cancel, terminate, modify or suspend the internet portion of the sweepstake if the sweepstake is compromised or becomes technically corrupted, should virus, bugs, non-authorized human intervention or other causes beyond the reasonable control of the Company corrupt or impair the administration, security, fairness, integrity or proper conduct of the sweepstakes. Furthermore, the Company disclaimed any liability for any systems, servers, providers, computer equipment, software, failure of any e-mail or entry to be received by company on account of technical problems or traffic congestion on the internet or at any website, or any combination thereof, including any injury or damage to any participant's or any other person's computer related to or resulting from participation or downloading any materials in this sweepstakes. The Company also provided a warning to hackers. CAUTION: ANY ATTEMPT BY ANY PERSON TO DELIBERATELY DAMAGE ANY WEBSITE OR UNDERMINE OPERATION OF A SWEEPSTAKES IS A VIOLATION OF CRIMINAL AND CIVIL LAWS AND SHOULD SUCH AN ATTEMPT BE MADE COMPANY RESERVES THE RIGHT TO SEEK DAMAGES FROM SUCH PERSON TO THE FULL EXTENT PERMITTED BY LAW.

These rules include a disclaimer of liability for system malfunctions of every kind and the right to cancel the promotion in the event the process is impaired or corrupted.

© 2004 Piper Rudnick LLP. All Rights Reserved.

UNSOLICITED E-MAIL ("SPAM")

On January 1, 2004, the Federal "CAN-SPAM Act of 2003"[346] took effect, establishing a national standard for the regulation of commercial electronic mail and addressing the concerns applicable to "spam."[347] Spam is a bulk message advertising goods or services that is sent to a recipient without his or her prior consent (and without an underlying business relationship from which consent to exchange such communication can be implied). Spam is the electronic equivalent of the "junk mail" that is sent through the U.S. Postal Service and received in homes and offices every day.

The CAN-SPAM Act requires that all commercial e-mail messages include an opt-out, a physical address, and an indication that the e-mail is a solicitation. The law leaves it up to the sender of the e-mail to determine how to indicate that the message is a solicitation. There are no specific labeling requirements (although the FTC is authorized to consider adding such requirements in the future). The labeling requirements required under many state laws are preempted. These opt-out, address and solicitation indication requirements imposed on commercial e-mail do not apply to "transactional or relationship" e-mail messages, such as ongoing commercial relationships that are not primarily solicitations. These requirements do apply to all other commercial electronic mail, which is defined as any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.

The Federal spam law specifically preempts the numerous state laws that have been enacted in recent years. More than 37 states had enacted some form of commercial e-mail prior to the enactment of the Federal spam law.[348] The CAN-SPAM Act preempts many of these state

---

[346] The legislation was entitled the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003," and is commonly known as the "CAN-SPAM Act of 2003."

[347] Use of the term "spam" to refer to unsolicited e-mail is commonly attributed to a comedy routine performed on the British television show "Monty Python's Flying Circus" in the mid-1970's. During the routine, the performers chant "spam, spam, spam, spam, spam, spam, spam" to drown out all the other conversations in the setting of a restaurant. *See http://www.ironworks.com/comedy/python/spam.htm*.

[348] Alaska, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Missouri, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. The original spam laws in California and Washington were stricken by state trial courts, citing the Commerce Clause of the U.S. Constitution, but subsequently, those decisions were reversed and the laws were upheld on appeal. *See Ferguson v. Friendfinder*, unreported (S.F. Super. Ct. June 12, 2000), *reversed*, 94 Cal. App. 4th 1255 (Cal. Ct. App. 2002) (lower court decision available at *http://news.cnet.com/news/0-1005-200-2047482.html?tag=bplst*); and *State of Washington v. Heckel*, 24 P.3d 404, 412-13 (Wash. 2001), *cert. den.*, 122 S. Ct. 467 (2001), *reversing* 2000 WL 979720 (Wash. Super. Ct. 2000) (Washington Supreme Court reversed lower decision that Washington anti-spam law was unduly burdensome on interstate commerce because it focused only those persons who send spam from, or transmit spam to persons in, the State of Washington; case remanded for trial).

(footnote continued to next page)

© 2004 Piper Rudnick LLP. All Rights Reserved.

spam laws, but preserves these state laws and state common law rules "to the extent that" they prohibit falsity or deception in commercial e-mail. Thus, the Federal spam law preempts the California "opt-in" anti-spam statute[349] that had also been scheduled to take effect at the start of 2004 (*i.e.*, when the federal law became effective). State spam laws may still, however, be used to combat deceptive spam.[350]

Among other things, the CAN-SPAM Act also required the FTC to issue a report to Congress on the possibility of establishing a "do not e-mail registry" similar to the highly popular "do not call registry" established in 2003, which, by its one-year anniversary in June 2004, had already amassed a list of over 62 million telephone numbers.[351] The CAN-SPAM Act mandated that the FTC provide Congress with a report "that (1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-Email Registry; (2) includes an explanation of

---

(footnote continued from previous page)

Several state laws that would limit the access of children to online pornography have also been stricken; *see e.g.*, *ACLU v. Johnson*, 194 F. 3d 1149 (10th Cir. 1999); *Psinet Inc. v. Chapman*, 167 F. Supp.2d 878 (W.D. Va. 2001); *Cyberspace Communications Inc. v. Engler*, 55 F. Supp.2d 737, 741 (E.D. Mich. 1999), *aff'd*, 2000 U.S. App. LEXIS 29359 (6th Cir. 2000); and *American Libraries Assoc. v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997). The court in *Cyberspace Communications* observed that although the law in question only attempts to address speech that originates or terminates within Michigan, "virtually all Internet speech is, as stipulated by Defendants available everywhere including Michigan. A New York speaker must [therefore] comply with the [Michigan] Act in order to avoid the risk of prosecution in Michigan even though (s)he does not intend his message to be read in Michigan. A publisher of a web page cannot limit the viewing of his site to everyone in the country except those in Michigan. The Internet has no geographic boundaries. The [Michigan] Act is, as a direct regulation of interstate commerce, a per se violation of the Commerce Clause." *Cyberspace Comm.*, 55 F. Supp.2d at 751. *See also Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitime*, 2001 U.S. Dist. LEXIS 18378 (at slip op. *19) (N.D. Cal. 2001), *summary judgment granted*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); *reversed*, 2004 U.S. App. LEXIS 17869 (9th Cir. 2004) (U.S. court lacked personal jurisdiction over French defendant.

349 In September 2003, California adopted a law (the legislative proposal was known as "S.B. 186") that included an opt-in requirement for unsolicited commercial e-mail. This California law would have applied to any e-mail sent to a person in California even if the sender was unaware that the recipient was located in California. The California law was one of the reasons motivating Congress to complete work on spam legislation so that the CAN-SPAM Act could take effect on January 1, 2004, thereby preempting the California opt-in statute.

350 In a case brought shortly before both the CAN-SPAM Act and S.B. 186 were adopted, the California Attorney General's office won a default judgment for $2.0 million with respect to allegedly deceptive spam. In this action, the Attorney General obtained an injunction as well against masking the e-mail address from which e-mail is sent, including false information about the server from which e-mail is sent, deceptively accepting payment from buyers without meeting statutory requirements for doing so, accessing other persons' computer systems without their permission, and using false or misleading information to register for an e-mail address or domain name. *California v. Willis*, No. 1-02-CV811428 (Cal. Super. Ct. Santa Clara Oct. 24, 2003); *see also* Press Release, Attorney General of California, *Attorney General Lockyer Wins First-Ever Lawsuit Again Spammer; Court Curbs PW Marketing's Business Practices and Requires Firm to Pay $2 Million* (Oct. 24, 2003) (available at *http://caag.state.ca.us/newsalerts/2003/03-130.htm*).

351 Caroline E. Mayer, *In 1 Year, Do-Not-Call List Passes 62 Million*, The Washington Post, June 24, 2004 at E05.

© 2004 Piper Rudnick LLP. All Rights Reserved.

any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a Registry; and (3) includes an explanation of how the Registry would be applied with respect to children with e-mail accounts."[352] The Commission sought public comment, conducted an investigation,[353] and issued its report to Congress on June 15, 2004. The Commission expressed concern that without some means of first authenticating the address of senders, a National Do Not Email Registry would more likely do harm by facilitating spammers' misuse of the registry information to validate e-mail addresses to which they could send unwanted messages. In the Executive Summary of its *Report to Congress*, the FTC explained its view that:

> The Commission therefore strongly believes that implementation of a National Do Not Email Registry would not reduce the volume of spam, particularly given currently available technology to authenticate the origin of email messages. The Commission thus proposes a program to encourage the widespread adoption of email authentication standards that would help law enforcement and ISPs better identify spammers. If, after allowing the private market sufficient time to develop, test, and widely implement an authentication standard, no single standard emerges, the Commission could begin the process of convening a Federal Advisory Committee to help it determine an appropriate email authentication system that could be federally required. If the Commission were to mandate such a standard, after a reasonable period of time following the effective date of such a standard, the Commission will consider studying whether an authentication system combined with enforcement or other mechanisms (e.g., better filters) had substantially reduced the burden of spam. If spam continued to be a substantial problem, if a Registry could significantly reduce it once an authentication system is in place, and if other technological developments removed the security and privacy risks associated with a Registry, the Commission will consider issuing [the draft of a new rule] proposing the creation of a National Do Not Email Registry.[354]

---

[352] Section 9 of the CAN-SPAM Act, 15 U.S.C. § 7708.

[353] In a notice dated March 11, 2004 published in the Federal Register, the FTC asked for public comment on the subject of whether and, if so, how, to implement a national "do not e-mail registry." 69 Fed. Reg. 11,776 (2004). The Commission reported that it received thirteen responses to the request for comments, that it additionally interviewed an additional eighty individuals, and that it sought detailed information on spam from the seven ISP's that together control over 50% of the national market for e-mail. Federal Trade Commission, "*National Do Not Email Registry: A Report to Congress*," June 15, 2004, at i (available at *http://www.ftc.gov/reports/dneregistry/report.pdf*).

[354] Federal Trade Commission, "*National Do Not Email Registry: A Report to Congress*," June 15, 2004 (available at *http://www.ftc.gov/reports/dneregistry/report.pdf*).

© 2004 Piper Rudnick LLP. All Rights Reserved.

The Federal spam law contains civil prohibitions against sending false or misleading header or transmission information in a commercial e-mail message. The law also includes civil prohibitions against using another computer to relate or retransmit commercial e-mail messages for the purpose of disguising its origin and against sending commercial e-mail that includes an originating e-mail address, domain name or Internet protocol address that was obtained by false pretenses or representations. The Federal law also prohibits the use of deceptive subject headings. Indeed, the first prosecution by the government was against the principals of a company alleged to have sent UCE to consumers by "spoofing" the senders, using the names of innocent third parties in the "reply-to" and "from" fields of their e-mails.[355] The FTC brought a related civil action against the same parties, noting that when these e-mails were "undeliverable and bounced back, tens of thousands of undelivered e-mails bounced [back] to unwitting third parties, sometimes getting the third parties mislabeled as spammers, themselves. The spam did not offer consumers the ability to opt-out of receiving future e-mail."[356]

Aggravated violations of the falsification and deception prohibitions in the Federal spam law will be subject to additional remedies when the e-mail addresses are obtained by "harvesting" or through "dictionary attacks". Harvesting is the practice of collecting through an automated means e-mail addresses that are posted on websites or online services. Dictionary attacks occur when e-mail addresses are generated by combining names, letters, or numbers into numerous permutations in the hope of generating functioning e-mail addresses. Aggravated violations will also apply where multiple e-mail accounts are created through automation to transmit otherwise unlawful messages and the relay or retransmission of commercial e-mail from computers that have been accessed without authorization.

The Federal spam law also criminalizes the most egregious spammer tactics. These new criminal prohibitions apply where more than 100 commercial e-mail messages are initiated in a 24-hour period involving: (i) hacking into someone else's computer to send bulk spam; (ii) using "open relays" to send multiple spam with the intent to deceive ISPs or recipients as to the origin of the messages; (iii) falsifying header information in spam; (iv) registering for five or more e-mail accounts or two or more domain names using false information and then sending multiple spam from these accounts; and (v) falsely representing oneself to be the holder of five or more Internet protocol addresses and sending multiple commercial e-mail messages from such addresses.

Most of the criminal violations are misdemeanors; however, violations involving hacking, larger numbers of commercial e-mail messages or falsified registration, or loss or gain aggregating more than $5,000 in a year, or a criminal spam organization are punishable by a three-year felony. Five-year felony penalties are available for violations undertaken in

---

[355] U.S. Justice Department, Press Release, *Department of Justice Announces Arrests of Detroit-Area Men on Violations of the "Can-Spam" Act*, Apr. 29, 2004 (available at *http://www.usdoj.gov/criminal/cybercrime/chungArrest.htm*).

[356] Federal Trade Commission, Press Release, *FTC Announces First Can-Spam Act Cases*, Apr. 29, 2004 (available at *http://www.ftc.gov/opa/2004/04/040429canspam.htm*).

© 2004 Piper Rudnick LLP. All Rights Reserved.

furtherance of another felony and violations by someone with a prior offense involving hacking or criminal spam under Federal or state law.

There have been a number of lawsuits concerning "spam" or mass e-mailings as a marketing tool and, more recently, lawsuits concerning forged spam with a falsely identified sender and return address. The technique of using an assumed identity of another in an online environment is referred to as spoofing.[357]

Internationally, more than a dozen countries also regulate spam in one form or another, including Australia,[358] Austria,[359] Canada,[360] Denmark,[361] England,[362] Finland,[363] Germany,[364] Italy,[365] Norway,[366] Portugal,[367] Spain,[368] and Sweden.[369] The internationalization of spam was

---

[357] In *Felsher v. University of Evansville*, 755 N.E.2d 589 (Ind. 2001), the Indiana Supreme Court confronted a case in which a college professor had created internet websites and e-mail addresses that incorporated the names of officials at the university where the professor was formerly employed. The Court upheld an injunction against the professor's unauthorized use of other persons' names and likenesses in e-mail addresses and websites, observing that doing so was an invasion of the plaintiff's right to privacy. *Id* at 601. See also the note, above, regarding the first prosecution under the CAN-SPAM Act.

[358] Privacy Amendment (Private Sector) Act 2000, No. 155 (2000) (Austl.) (available at *http://scaleplus.law.gov.au/html/comact/10/6269/pdf/155of2000.pdf*).

[359] Telekommunikations Geretz 1997, BGBI.1 Nr. 100/1997 ("Federal Law Relating to Telecommunications;" unofficial transaction available at *http://www.bmv.gv.at/tke/ofbenglish/egesetz/tkge.pdf*).

[360] Personal Information Protection and Electronic Documents Act, R.S.C., ch. 5 (2000) (Can.) (available at *http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp*).

[361] Danish Marketing Practices Act 2000 (Consolidated Act No. 699 of 17 July 2000, § 6(a)) (available at *http://www.euro.cauce.org/en/countries/c_dk.html*).

[362] Consumer Protection (Distance Selling) Regulations 2000 (which implements Directive 97/7/EC of the European Parliament and Council of 20 May 1997 on the protection of consumers in respect of distance contracts. 1997 O.J. (L 144) 19-28); and 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, 2000 O.J. (L 178) 1 (which applies in all the EU member states).

[363] *See* excerpt at *http://www.euro.cauce.org/en/countries/c_fi.html*.

[364] Unfair Competition Law and the Federal Civil Code (excerpt available at *http://www.euro.cauce.org/en/countries/c_de.html*).

[365] Attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza (Implementation of Directive 97/7/EC on the Protection of Consumers in respect of Distance Contracts) (excerpt available at *http://www.euro.cauce.org/en/countries/c_it.html).*

© 2004 Piper Rudnick LLP. All Rights Reserved.

confirmed by Business Week, which cited reports that one-quarter of all spam sent worldwide comes from servers in China and Korea.[370]

Commercial e-mail messages sent to recipients in the U.S. must now comply with the CAN-SPAM opt-out, physical address, and solicitation description requirements. By establishing a national standard applicable to commercial e-mail, the Federal statute eliminates most of the problems arising from the patchwork of conflicting state laws that existed prior to its enactment. E-commerce business models using e-mail as part of their business model need to comply with the Federal spam law. "Tell a Friend", "Refer a Friend" and "e-mail this page to a Friend" features, for example, need to be carefully implemented to avoid anti-spam laws. E-mail advertising campaigns must be planned very carefully so as not to inadvertently run afoul of one or more of the Federal, state, or international anti-spam statutes.

(footnote continued from previous page)

366 Act No. 47 of 16 June 1972 relating to the Control of Marketing and Contract Terms and Conditions (The Marketing Control Act) , Section 2.b (available at *http://www.forbrukerombudet.no/html/engelsk/themcact.htm).*

367 *See* report at *http://www.euro.cauce.org/en/countries/c_pt.html*.

368 *See* report at *http://www.euro.cauce.org/en/countries/c_es.html.*

369 *See* report at *http://www.euro.cauce.org/en/countries/c_se.html.*

370 Bruce Einhorn, *Now Spam in Being Outsourced*, Bus. Week, Sept. 13, 2004.

© 2004 Piper Rudnick LLP. All Rights Reserved.

FIRST AMENDMENT

The internet is a communications medium. As the U.S. Supreme Court noted: "through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox" . . . and "[t]hrough the use of Web pages, mail exploders and news groups, the same individual can become a pamphleteer."[371] It has proven almost impossible for the federal government and state governments to enact laws to regulate the content of communications on the internet without violating the free speech guarantees of the First Amendment. The First Amendment has been held to protect a pro-life, anti-abortion website captioned the "Nuremberg Files" on which were published photographs, and other personal information on doctors and others who provided abortion services[372] and a website critical of law enforcement listing names, addresses, birth dates, telephone numbers and other personal information concerning law enforcement personnel and their relatives.[373]

Free speech issues also relate to filtering software which may be viewed as a form of censorship. Business Week notes that 25 percent of the companies use some form of filtering software to block some websites.[374]

There are a variety of user-based software products that allow users to block access to sexually explicit materials on the Web, to prevent minors from giving personal information to strangers by e-mail or in chat rooms, and to keep a log on all online activity that occurs on the home computer.

While the right to communicate anonymously on the internet falls within the scope of the First Amendment's protections, the right to speak anonymously is not absolute.[375] Wrongdoers cannot hide behind an illusory shield of First Amendment rights.[376]

---

[371] *Reno v. ACLU*, 117 S. Ct. 2329, 2344 (1997). In response to the *Reno* case, which deemed unconstitutional the Communications Decency Act of 1996, 47 U.S.C. § 223, Congress passed a new law, entitled the Child Online Protection Act, 47 U.S. C. § 231 (COPA). COPA imposes criminal sanctions for knowingly posting, for commercial purposes, content that is "harmful to minors." 47 U.S.C. § 231(a)(1). The Court found that the federal district court was correct in issuing an injunction against enforcing COPA, because (among other things) the district court had found that other techniques – such as the use of filters – were likely to be more effective at preventing children from viewing harmful materials than enforcement of COPA itself. The Supreme Court therefore returned the case to the district court to determine whether less restrictive means were possible to protect children than restricting content. *Ashcroft v. ACLU*, 542 U.S. ____, 2004 WL 1439998 (June, 29 2004).

[372] *Planned Parenthood of the Columbia/Williamette, Inc. v. American Coalition of Life Activists*, 244 F. 3d 1007 (9th Cir. 2001).

[373] *City of Kirland v. Sheehan*, 2001 WL 1751590 (Wash. Sup. Ct. 2001) (the court determined the website was protected by the First Amendment by requiring the site operator to remove all Social Security numbers from the site on the grounds that there is a compelling interest to keep SSN's private.)

[374] Bus. Week, Aug. 16, 1999, at 6.

© 2004 Piper Rudnick LLP. All Rights Reserved.

(footnote continued from previous page)

[375] *In re Subpoena Dues Tecum to America Online, Inc.*, 2000 WL 1210372 (Va. Fairfax Cir. Ct. 2000), *rev'd by America Online, Inc. v. Anonymously Publicly Traded Company*, 542 S.E. 2d 377 (Va. 2001).

[376] *Id. See also* the discussion in the Domain Name and Cybersmearing sections, above.

© 2004 Piper Rudnick LLP. All Rights Reserved.

SPECIAL APPLICATIONS

There are many problems with specialized applications and specialized e-business efforts. For example, online pharmacy sites[377] have been sued for selling drugs without a prescription, without parental consent, without consultations with a doctor, and without a licensed or registered pharmacist dispensing the drugs.

Issues also arise with other licensed professionals. Concerns may arise relating to the unauthorized practice of law in jurisdictions where lawyers are not licensed and the same goes for doctors engaged in telemedicine over the internet and other licensed professionals.

Online gambling[378] sites have been criminally prosecuted in states where gambling is illegal,[379] even where the server is located in a state or Indian reservation or off-shore where gambling is legal. States have also passed legislation criminalizing the sale of narcotics, beer and alcohol over the internet. In *State of Missouri v. Beer Nuts, Ltd.*,[380] the Circuit Court determined that by advertising and soliciting orders on its website for microbrewery beers Beer Nuts transacted business in Missouri and was subject to Missouri's Liquor Control Law. Some states are banning internet sales of tobacco directly to consumers in their state.[381] Others have banned online sales of cigarettes to minors.[382] State laws adversely effecting e-business are often challenged based on the Commerce Clause requirement that these statutes meet the strict scrutiny test, when the statute is shown to discriminate against interstate commerce.[383] Many of these

---

377 Jupiter Communications estimates that online prescription sales in the U.S. will hit $970 million in 2003. The Industry Standard, Sept. 20, 1999, at 208.

378 Twenty-five million web gamblers worldwide will produce $1.2 billion in revenues for online gaming sites. The Industry Standard, Sept. 20, 1999, at 208.

379 *New York v. World Interactive Gaming Corp.*, 1999 WL 591995 (N.Y. Sup. Ct. 1999); *Minnesota v. Granite Gate Resorts, Inc.*, 568 N.W. 2d 715 (Ct. App. Minn. 1997).

380 *State of Missouri v. Beer Nuts, Ltd.*, No. 974-2076 (Mo. Cir. Ct. Mar. 31, 1999).

381 D. Streitfield, *Online Tobacco Sales Ignite Fight Over Taxes*, The Washington Post, Aug. 29, 2000, at A1-A8.

382 Internet Law News (Feb. 6, 2000). Massachusetts fined an online cigarette retailer $1.5 million for selling cigarettes to minors noting that specific steps are required to verify age. *See Massachusetts v. S4L Distributing, Inc.*, Mass. Super. Ct. March 29, 2004.

383 In *Santa Fe Natural Tobacco Co. v. Spitzer*, 2001 U.S. Dist. LEXIS 7548 (S.D.N.Y. 2001), the court struck down as an impermissible restraint in violation of the Commerce Clause a state regulation that would have limited the sale of cigarettes to only in-state retailers, *id.* at *54, rather than other sources, such as Indian reservations and "direct sales channels," such as the sales made through the internet, mail order, and telephone sales. *Id.* at *17, n9. The court further concluded that "[u]nder strict scrutiny, defendants must also demonstrate that they have no other means to reduced youth smoking …. [and the] evidence establishes that is possible to reduce youth smoking without banning direct sales …." *Id.* at *70.

© 2004 Piper Rudnick LLP. All Rights Reserved.

statutes fail to pass this strict scrutiny test and are not being enforced.[384] In this regard, the standard was set by the U.S. Supreme Court: "[n]o State may attempt to isolate itself from a problem common to the several States by erecting barriers to the free flow of interstate trade."[385] That conclusion is consistent with the explanation given by the Supreme Court over 70 years ago, when it wrote that "[n]either the power to tax nor the police power may be used by the state of destination with the aim and effect of establishing an economic barrier against competition with the products of another state or the labor of its residents."[386]

---

[384] *See, e.g.*, *Bridenbaugh, Dickerson v. Bailey*, 212 F. Supp. 2d 873 (S.D. Tex. 2002) (Texas ban on direct shipment of wine to consumers in Texas found unconstitutional); *Bolick v. Roberts*, 199 F. Supp. 2d 397 (E. D. Va. 2002) (Virginia ban on out-of-state wine shipments found unconstitutional); *Beskind v. Easley*, 197 F. Supp.2d 464 (W.D.N.C. 2002) (North Carolina ban an out-of-state shipment of wines to residents found unconstitutional); *Sweedenburg v. Kelly*, 358 F.3d 323 (2d Cir. 2004) (N.Y. ban on shipments by out-of-state wineries direct to consumers unconstitutional); *Kendall-Jackson Winery, Ltd. v. Branson*, 82 F. Supp.2d 844 (N.D. Ill.), *aff'd*, 212 F.3d 995 (7th Cir. 2000). In other cases with implications for online sales, *see Craigmiles v. Giles*, No. 00-6281 (6th Cir. Dec. 6, 2002) (rejecting Tennessee law that restricts sale of burial caskets to only state licensed funeral directors); *Ford Motor Co. v. Texas Dept. of Transportation*, 106 F. Supp.2d 905 (W.D. Tex. 2000), *aff'd*, 264 F.3d 463 (5th Cir. 2001) (upholding law banning any party other than a franchised auto dealer from obtaining a state license to sell motor vehicles in Texas, thereby precluding manufacturers from engaging in online auto sales); and *Powers v. Harris*, No. CIV-01-445-F (W.D. Okla. Dec. 12, 2002) (facts substantially similar to *Craigmiles*, above, but here the court upheld the Oklahoma statute). *Cf. Beskind v. Easley*, No. 02-1432 (4th Cir. Apr. 8, 2003) (law banning importation of wine into N.C. other than through regulated three-tiered structure violated dormant Commerce Clause and discriminated against out-of-state wine sellers).

[385] *Chemical Waste Management, Inc. v. Hunt*, 504 U.S. 334, 339-40 (1992) (internal quotations and citations deleted).

[386] *Baldwin v. G.A.F. Seeling, Inc.*, 294 U.S. 511, 527 (1935).

© 2004 Piper Rudnick LLP. All Rights Reserved.

INSURANCE

Conventional insurance does not protect against many e-commerce risks. Insurance companies are developing new insurance products to deal with cyber-liability risks. These policies are evolving. They may be appropriate in some circumstances and will need to be considered as part of a risk management program. Some of these new policies ignore many of the risks created by the internet and e-commerce. Some of these new policies cover liabilities for economic losses and damage to intangible property. There are special anti-hacking policies available. Many of the internet liability policies contain restrictions that severely limit the value of the coverage. Companies should very carefully review any insurance policies for the internet.

© 2004 Piper Rudnick LLP. All Rights Reserved.

SECURITIES LAW

All postings on a company's website need to be reviewed with the securities laws in mind. Company websites are available to the investing public. The accuracy and currency of information posted is quite important from a securities law perspective. It is important that posted information remains current.

Press releases and other public announcements posted on the company's website should be clearly dated to avoid any confusion as to when they were prepared. Links may also create a securities issue in the event that the information is materially false. References to a web site in securities filings may result in the contents of the site being incorporated in these documents. The Securities and Exchange Commission has determined that an embedded hyperlink within a prospectus or any other document required to be filed or delivered under the federal securities laws caused the hyperlink information to be part of the document.[387] Investors may consent to electronic delivery telephonically.

Many press releases posted on by public companies on the web will include a "safe harbor" statement under the Private Securities Litigation Act of 1995, indicating that statements in the press release which are not historical facts are "forward-looking statements" that involve risks and uncertainties, and cross-referencing the company's filings with the Securities and Exchange Commission with respect to the description of specific risk factors. The cautionary language must be substantive and tailored to the specific future projections, estimates and opinions.[388]

Bogus press releases and internet stock rumors have resulted in serious security fraud cyberhoaxes. The Emulex cyberhoax is a recent example.[389]

---

[387] *See* "Use of Electronic Media", Securities Act Release No. 33-7856, Exchange Act Release No. 34-42728, Investment Company Act Release No. 24426, 2000 WL 502290 (S.E.C.) (Apr. 28, 2000).

[388] *See Lindelow v. Hill*, 2001 U.S. Dist. LEXIS 10301 (N.D. Ill. 2001). There the court determined the press release about OneMedPlace.com was false and misleading and not protected by the vague forward-looking statements.

[389] *See generally Hart v. InternetWire, Inc.*, 145 F. Supp 2d 360 (S.D.N.Y. 2001). Bloomburg and Interwire were not liable for Securities Act violations for their republishing the false press release about Emulex.

© 2004 Piper Rudnick LLP. All Rights Reserved.

TAXES

What taxes apply to e-business? Various state, national and international governmental agencies, as well as private companies, are struggling with how to devise a tax structure that will deal with the complex issues related to the taxation of e-business.[390] The Internet Tax Freedom Act (ITFA),[391] enacted in October 1998, imposed a three-year moratorium on a variety of Federal, state and local taxation on e-commerce. The ITFA moratorium expired on October 22, 2001, and was retroactively extended until November 1, 2003.[392] The moratorium was not extended by Congress in 2003, but the issue is likely to be taken up again in the Second Session of the 108th Congress in 2004. The stakes are high: in September 2003 the Multistate Tax Commission estimated that a bill to extend the moratorium would cost state and local governments at least $4 billion in lost tax revenue in 2003 and as much as $8.75 billion by 2006.[393]

The ITFA helped spur the growth of e-commerce. The National Bureau of Economic Research reported that people who live in areas with high sales taxes are "significantly" more likely to buy on the internet than people in areas where local sales tax does not apply.[394] Tax inequities will in all likelihood compel the implementation and imposition of some form of e-commerce tax scheme. The challenge facing tax administrators is to maximize the potential efficiency gains of the internet while still preserving their revenue base, without impeding the development of new technologies.

Online tobacco sales are a major concern of many states. There is about a 30% differential between the cost of cigarettes with taxes sold in a state and those purchased online

---

390 The fundamental approach to sales taxes in the U.S. drives, to a large degree, the debate on whether and, if so how, state sales taxes should or should not be collected on internet sales. The U.S. Supreme Court ruled that some nexus is required in order for a state to impose or collect sales taxes, and consequently, a seller cannot be required to collect sales taxes from a purchaser located in a state where the seller does not have a physical presence. *Quill Corp. v. North Dakota*, 504 U.S. 298 (1992).

391 Pub. L. 105-277, Div. C, Title XI, §§ 1100-1104, Oct. 21, 1998, 112 Stat. 2681-719 (codified at 47 U.S.C. § 151 note).

392 On November 28, 2001, President Bush signed H.R. 1552, the "Internet Tax Nondiscrimination Act," which simply amended the IFTA so that the moratorium would not expire until November 1, 2003.

393 Press Release, Multistate Tax Commission, *Net Tax Moratorium Would Cost Cities, States Up to $9 Billion a Year, Create Blanket Telecom Tax Exemption* (Sept. 24, 2003) (available at http://www.mtc.gov/ITFANewsRel092403-FINAL.pdf).

394 *Tax Dodgers Go Online*, Bus. Week, Apr. 19, 1999, at 30 (also referencing a study indicating that applying existing taxes to Internet sales would reduce online buyers by 25 percent).

© 2004 Piper Rudnick LLP. All Rights Reserved.

without taxes. California[395] and Washington have dunned online cigarette purchasers for the taxes. New York, on the other hand, has banned internet, mail order and telephone orders of cigarette sales directly to consumers in the state,[396] but the enforcement of this statute has been enjoined based on its discriminatory effect on interstate commerce.[397]

A recent study by Ernst & Young found that not only do 45 states impose a sales tax, but that 4,696 cities, 1,602 counties, and 1,113 school districts do as well.[398] These numbers suggest the possible complexity. Collecting taxes on the internet may prove to be insurmountable especially for small e-merchants. While the internet tax moratorium has been extended for two years, the issues of simplification and collection of interstate sales and use taxes is not going away and will once again be in play when the moratorium expires on November 1, 2003.

Even though the IFTA imposes a moratorium on taxes, it still allows the imposition of a single nondiscriminatory tax on goods and services sold on the internet. As such, the imposition of taxes during this moratorium is not out of the question. In order to collect a sales tax on internet transactions, a state must show that it has sufficient jurisdiction over a company doing business over the internet. Today many pure play e-commerce companies, like Amazon.com and eToys, are paying sales taxes as if their tax exposure is similar to catalogue businesses. They collect sales taxes only in those states in which they have nexus - such as where they are headquartered, have warehouses, or other facilities.[399] Borders.com collects sales taxes where the subsidiary has offices, personnel, warehouses or servers.[400] In fact, notwithstanding the moratorium, many corporations are paying taxes on goods purchased on line just as they would if they purchased the goods from the store.[401] If the taxes and the obligations to collect them are substantially the same as those in transactions effected by mail order, telephone or other remote means some states have been adamant, such as Florida and Tennessee, that they will continue to impose and attempt to collect sales and use taxes from e-commerce businesses. E-business

---

395 In *Santa Fe Natural Tobacco Co., Inc. v. Spitzer*, 2000 WL 1694307 (S.D.N.Y. 2000) it was reported that 78% of the California consumers who purchased cigarettes from out-of-state sellers paid the taxes to California upon demand.

396 D. Streitfield, *Online Tobacco Sales Ignite Fight Over Taxes*, The Washington Post, Aug. 29, 2000, at A1, A8.

397 Santa Fe Natural Tobacco Co., Inc. v. Spitzer, 2000 WL 1694307 (S.D.N.Y. 2000).

398 Alan K. Ota, *States' Internet Tax Strategy*, Congressional Quarterly Weekly, Jan. 15, 2000, at 75.

399 *Net Retailers Face Taxing Question*, The Industry Standard, Dec. 13-20, 1999, at 61.

400 *Id.* at 64.

401 *See* R. Gold, *Taxing Questions*, The Wall Street Journal, Dec. 10, 2001, at R14.

© 2004 Piper Rudnick LLP. All Rights Reserved.

taxation is becoming more likely. Many states are projected to lose billions in online sales taxes in several years.[402]

Many major e-tailers are voluntarily starting to collect sales taxes on online sales.[403] Walmart.com began collecting taxes February 1, 2003 in all 45 states that have a sales tax-based on the purchaser's address. Toysrus.com, along with its Babiesrus.com and Imaginenarium.com units, now collect sales taxes based on the buyer's state except in Wyoming and the District of Columbia, where they have no physical sites.[404] Target.com collects sales tax in states in which it has "Target" retail stores.[405] By collecting sales taxes, these companies are foregoing any effort to totally separate their online and traditional businesses, which frees up these companies to take advantage of synergies, such as allowing e-customers to return goods online purchased to the company's traditional "brick and mortar" stores. The integrated retailers with both e-business and traditional retail stores will be able to take advantage of their retail stores as part of their e-business model.

E-business companies need to carefully monitor tax developments affecting e-commerce, including international taxation policies. In all likelihood there will be major tax developments affecting e-commerce in the coming years, and the likely result will be a more uniform state tax structure throughout the United States. As e-business revenues increase the likelihood of taxation will probably increase, especially if the "brick and mortar" tax base decreases." State and local governments are projected to lose as much as $20 billion dollars in uncollected internet sales taxes by 2002. The National Governors Association is drafting a "voluntary" plan to designate a third party to calculate, collect and remit taxes on both mail order and online remote use taxes.[406]

The EU[407] is introduced a "harmonized" value-added tax ("VAT") on the sale of virtual products which is effective July 1, 2003.[408] The internet tax situation promises to ultimately be a

---

402 *The State of Net Tax Loss*, The Industry Standard, Aug. 21, 2000,at 132.

403 L. Grant, *Some Big Websites Collecting Sales Tax*, *USA TODAY*, Mar. 13, 2003, at 2B.

404 *Id.*

405 *Id.*

406 *See also* Norm Alster, *Illinois Joins Suits to Collect Taxes on Internet Sales*, The New York Times, Feb. 22, 2003; Jones, *Should States Tax E-Commerce and, if so, How?*, 4 J. Internet Law 12, at 21 (June 2001); Beck, *Get a Grip! Regulating cyberspace won't be easy*, Business Law Today at 14 (May/June 2001).

407 The current EU proposal will require any foreign company that sells goods and services into the EU to register in at least one EU country and pay a VAT to that country's taxing authority for online sales anywhere in the EU. The country will, under the proposal, redistribute the VAT to the appropriate country. Pressure to pay the VAT will increase at online sales increase because companies paying the tax will be competitively disadvantaged in comparison to companies who are not paying these VAT taxes.

© 2004 Piper Rudnick LLP. All Rights Reserved.

complex mess both within and without the United States. One of the toughest problems will be determining whether there is sufficient "nexus" for tax purposes.[409] The tax problem concerns the collecting the taxes and remitting them to the proper taxing authorities.[410]

(footnote continued from previous page)

[408] As of April 2002, the EU proposal would require any foreign company that sells goods and services into the EU to register in at least one EU country and pay a VAT to that country's taxing authority for online sales anywhere in the EU. The country collecting the tax would, under the proposal, redistribute the VAT to other appropriate countries. Pressure to pay the VAT will increase because companies paying the tax will be competitively disadvantaged in comparison to companies that are not paying these VAT taxes.

[409] A. Oreskovic, *Giving It To The Government*, The Industry Standard, June 4, 2001, at 74-75.

[410] *Id.* at 75.

© 2004 Piper Rudnick LLP. All Rights Reserved.

CUSTOMS DUTIES AND FOREIGN TAXES

Currently there is a moratorium on customs duties on e-commerce transmissions. The World Trade Organization has commenced a work program covering global e-commerce, and the issue of customs duties on e-commerce transactions is being considered as part of this WTO work program.

Global e-commerce is likely to become quite complex if countries impose customs duties on e-commerce transmissions. Many countries are in the process of considering imposing taxes on information products and services delivered to customers in their countries.

A permanent establishment is deemed to have been established wherever a server is located "if the business of an enterprise is wholly or partly carried on through the equipment.[411] Tax planning with respect to server locations is thus desirable. A website does not create permanent establishment because it does not constitute a fixed place of business. A website hosting arrangement also does not result in a permanent establishment as long as the site does not own the equipment.

---

[411] Organization of Economic Cooperation and Development Committee Model Tax Convention. *See* 6 Electronic Commerce & Law Report (BNA) at 51 (Jan. 17, 2001).

© 2004 Piper Rudnick LLP. All Rights Reserved.

E-BUSINESS OUTSOURCING

Many companies are relying upon e-business infrastructure outsourcing to attain the guarantee of application availability, flexibility and scalability in a timely and cost-effective manner. Scalability and security are two major issues today that are promoting the outsourcing of e-commerce applications. Scalability is needed to address the phenomenal growth and surges in internet traffic. Security is required to guard against hackers, viruses, industrial espionage, denial of service attacks and fraud.

E-business applications need to be available 24 x 7. Some companies are outsourcing their e-business applications to protect against the damaging effects of downtime on e-customer satisfaction, reputation of the e-commerce business and revenues. Many of the e-commerce outsourcing companies will provide the critical infrastructure for web-based e-commerce applications. They may provide the necessary turnkey infrastructure, permit acceleration of e-business application deployment, minimize downtime, and lower the total cost of ownership.

There are many contractual issues that need to be addressed in these e-business outsourcing relationships. Probably the most important is the Service Level Agreement ("SLA"). The SLA is the contractual mechanism for providing accountability in the outsourcing relationship and for measuring performance.

One form of e-business outsourcing is through the use of Application Service Providers (ASP's).[412] The ASP model is becoming increasingly more popular. They provide remote access to computing, software, communications and data storage resources enabling their licensed customers to perform operations using the functionality provided by specific application software or a bundle of application software products. The ASP application software is accessible through the internet or other communications networks. Today's ASP's provide access to browser-based, Web-enabled application software. The application software may be third-party software licensed by the ASP, software licensed or developed by the customer, or proprietary software developed by or for the ASP or a combination of any of the foregoing. Of course, each one of these situations presents different contractual and intellectual property concerns.

The Gartner Group believes the ASP market is poised for significant growth. The Gartner Group estimates that ASP revenues for 2000 will exceed $3.5 billion and grow to more than $25 billion by 2004.[413] End users outsource a wide variety of applications to ASP's. Among these applications hosted e-commerce and IT outsourcing services are expected to increase dramatically.

---

[412] Others are the Managed Service Provider ("MSP") that manages IT operations for multiple businesses and a Wireless Application Service Provider ("WASP") that enables users to access services from a variety of wireless devices.

[413] "*Apps on Tap*", E-Commerce ASP's, Fortune Technology Guide, Vol. 142, No. 12 at 217-220 (Winter 2001).

© 2004 Piper Rudnick LLP. All Rights Reserved.

ASP's provide significant advantages to customers. Essentially the ASP allows customers to rent software and retain a third party to operate it. The ASP relationship allows the customer to access expensive software at lower cost than if the customer had to acquire the necessary software license and the related hardware, software and communications infrastructure. It also allows the customer to take advantage of the ASP's IT workforce. Typically ASP's charge customers an up front fee and monthly service fees, which includes all installations, upgrades and maintenance. The ASP manages the application software. As between the customer and the ASP, the ASP is responsible for keeping the applications current, and delivering end-user performance and uptime. The ASP also manages, hosts, implements, integrates and supports software applications for their customers. The ASP usually is responsible for providing the scalability to permit the customer to increase its bandwidth, telecommunications and computing processing requirements to meet the customer's needs. This flexibility is becoming increasingly more important in the fast-changing internet environment.

The use of ASP models along with the maturity of network infrastructures and evolution of e-business have raised the service expectations. As the result of these heightened expectations service level agreements are becoming increasingly more important. These service level agreements define the responsibilities of the ASP and the users of the service. The "Service Level Agreement" identifies and defines the services provided as well as the supported products, measurement criteria, reporting criteria, performance and standards for the ASP Service.[414]

ASP transactions may involve various service schedules or agreements relating to implementation, software development, training, support and other services in addition to the agreement for ASP services. It is important to stress that the basic ASP agreement is for ASP services related to the application software functionality and not a license to use the application software itself.

The basic ASP agreement may be thought of as a combination of a web hosting agreement and an online service bureau agreement. ASP models are just evolving. Since ASP's are relatively new, many of the paradigms for ASP's are based on similar, but more traditional outsourcing agreements and other agreements for managing IT services. One commentator refers to the ASP model as in some ways being analogous to the main frame computing "time-share" model.[415] The concerns traditionally dealt in connection with service bureau agreements apply to ASP agreements today – maintaining the confidentiality of customer data, security, reliability, remedies, disaster recovery, redundancy, scalability, termination grounds and issues, dispute resolution, availability and access, transfer of the application software upon termination from the ASP to the customer or from the ASP to another ASP, service levels, payment terms, cancellation fees, and other issues that are common to many agreements relating to information

---

[414] *See* ASP White Paper.

[415] D. Loundy, *All the Rage, and a Significant Concern: Application Service Provider Agreements*, Cyberspace Lawyer at 10 (May 2000).

© 2004 Piper Rudnick LLP. All Rights Reserved.

technology. Many ASP arrangements also involve implementation, project management, milestones and acceptance testing as well as intellectual property issues.

As noted above, Service Level Agreements have become increasingly more important in ASP arrangements. They are considered to be the best method for ASP service arrangements to work to the satisfaction of all parties.

© 2004 Piper Rudnick LLP. All Rights Reserved.

TORT LIABILITY

The Federal Communications Decency Act (CDA), 47 U.S.C. § 230, creates federal immunity to any state law cause of action that would hold computer service providers liable for information originating with a third party.[416] Section 230 of the CDA provides that no interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. In *Stoner v. eBay*,[417] the California Superior Court held that the federal immunity created by Section 230 precludes courts from holding computer service providers liable for information originating with a third party or otherwise entertaining claims that would place a computer service provider in a publisher's role. As such, eBay was granted summary judgment in the *Stoner v. eBay, Inc*. case where the plaintiffs had sought to hold eBay liable for the sale of various bootleg and infringing sound recordings through auctions on eBay's website.

Section 230 immunity also protected Amazon.com respecting negative comments posted on an Amazon.com website about an author and his books.[418]

Section 230 has also been used to provide interactive service providers with immunity for third-party defamatory statements posted on bulletin boards, chat rooms and other places, errors in stock quotation information, negligence and other tort claims.[419]

---

[416] For a discussion of the approach to ISP liability in Canada, *see* Adrian Denegar, *ISP Liability for Third-Party Defamation in Canada: Adopting a US-Style Regulatory Scheme*, J. Internet Law (Dec. 2001) at 18.

[417] *Stoner v. eBay, Inc*., 2000 WL 1705637 (Cal. Sup. Ct. 2000); *See also Gentry v. eBay, Inc.*, 99 Cal. App. 4th 816 (Cal. Ct. App., 4th App. Dist. 2002) (eBay not liable for forged autographed sport items sold on auction site); *Green v. America Online, Inc*., 318 F.3d 465 (3rd Cir. 2003) (AOL not liable for virus transmission); *Batzel v. Smith*, 333 F.3d (9th Cir. 2003) (operator of listserv on website not liable); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003) (online dating service not liable for identity theft).

[418] *Schneider v. Amazon.com, Inc.*, 108 Wash. App. 454 (Wash. Ct. App. 2001).

[419] *See Zeran v. America Online, Inc*., 129 F.3d 327 (4th Cir. 1997). *See also Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003) (identity theft); *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003); *Doe v. GTE Corporation*, 347 F.3d 655 (7th Cir. 2003); *Noah v. AOL Time Warner, Inc.*, 261 F.Supp.2d 532 (E.D. Va. 2003) (civil rights claims); *Barrett v. Fonorow*, 343 Ill. App. 3d 1184 (Ill. Ct. App., 2d Dist., 2003); *Barrett v. Rosenthal*, 112 Cal. App. 4th 749 (Cal. Ct. App., 1st App. Dist. 2003); *Green v. America Online, Inc*., 318 F.3d 465 (3d Cir. 2003); *Ben Ezra, Weinstein and Co. v. America Online, Inc.*, 206 F.3d 980 (10th Cir. 2000); *Blumenthal v. Drudge*, 992 F.Supp. 44 (D.D.C. 1998); *Doe v. America Online, Inc*., 783 So. 2d 1010 (Fla. Sup. Ct. 2001). *But see Gucci America, Inc. v. Hall*, 135 F. Supp.2d 409, 421 (S.D.N.Y. 2001) (distinguishing *Zeran*) (Mindspring not protected under Section 230 under established law respecting printer-publisher liability and contributory infringement under the Lanham Act); and *Barrett v. Rosenthal*, No. A096451 (Cal. App. Dep't Super. Ct. Oct. 15, 2003) (specifically declining to follow *Zeran*, court refused to grant immunity under § 230 to a defendant who re-sent (distributed) and posted (published) allegedly defamatory e-mails). *Cf. Doe v. GTE Corp.*, No. 02-4323 (7th Cir. Oct. 21, 2003) (in dictum, Judge Easterbrook cast doubt on the *Zeran* line of cases and applying § 203(c)(2) as grounds for dismissal of a claim by persons who were depicted in hidden video footage displayed on a website that defendants hosted). In contrast, a German court found the local

(footnote continued to next page)

© 2004 Piper Rudnick LLP. All Rights Reserved.

Section 230 does not protect the website with respect to information the e-commerce company develops or creates itself or participating in such development or creation. In addition, where a website operator was twice notified by e-mail that infringing content had been placed on the website, at least one federal court has denied a motion to dismiss a trademark infringement claim brought against the ISP itself, concluding that the CDA does not "automatically immunize ISPs from all intellectual property infringement claims." *Gucci America, Inc. v. Hall*, 135 F. Supp.2d 409, 417 (S.D.N.Y. 2001).

While Section 230 is very important legal defense to protect online service providers, certain decisions suggest that some courts may find it hard to apply that reasoning in every instance.[420] Accordingly, caution is still in order.

(footnote continued from previous page)

provider of the Microsoft Network liable for content posted by a private party, reasoning that the provider facilitated the objectionable activity by hosting the forum in which the message was posted. *Graf v. Microsoft GmbH*, OLGZ Cologne No. 15 U 221/01 (28 May 2002) (reported in 7 Electronic Commerce L. Rep. (BNA) 23, at 560-61 (June 5, 2002). A similar result was reported in Australia, where the High Court of Australia ruled in *Dow Jones & Co., Inc. v. Gutnick*, 194 A.L.R. 433 (Canberra, Australia 10 Dec. 2002), that a plaintiff can maintain an action against the publisher of the *Barron's Online* website alleging defamation. *See also Australian High Court Rejects Single Publication Rule for Internet Defamation*, 7 Electronic Commerce L. Rep. (BNA) 48, at p. 1226 (Dec. 18, 2002). *Cf. Van Buskirk v. The New York Times Co.*, No. 00-9220 (2d Cir. Apr. 2, 2003) (single-publication rule applies in New York, even to internet publication, and accordingly the plaintiff's claim was time barred).

[420] *See, e.g., Doe v. GTE Corp.*, No. 02-4323 (7th Cir. Oct. 21, 2003) (casting doubt on the *Zeran* line of cases (in dictum)); *Gucci America, Inc. v. Hall*, 135 F. Supp.2d 409, 417 (S.D.N.Y. 2001) (CDA does not provide a from liability for IP infringements); *Gucci America, Inc. v. Hall*, 135 F. Supp.2d 409, 421 (S.D.N.Y. 2001) (distinguishing *Zeran*); *Blumenthal v. Drudge*, 992 F.Supp. 44, 51-52 (D.D.C. 1998) (acknowledging its preference for a different outcome, the court declined to find liability for allegedly defamatory online posting); *Barrett v. Rosenthal*, No. A096451 (Cal. App. Dep't Super. Ct. Oct. 15, 2003) (specifically declining to follow *Zeran*).

© 2004 Piper Rudnick LLP. All Rights Reserved.

CRIMINAL LIABILITY

Companies need to avoid criminal liability for "aiding and abetting" criminal offenses on their websites. Violations of federal criminal laws are an exception to online service providers' legal immunity under 47 U.S.C. § 230(c)(1) for content posted on a website by third parties. Under some circumstances, a website's operator could face some risk of criminal prosecution if, after receiving notice or knowledge of illegal material on that website, the illegal material is not removed. Among the potential criminal areas of concern are: (1) counterfeiting; (2) explosives; (3) firearms; (4) drugs; (5) criminal threats; (6) suicide; (7) gambling; and (8) pornography.

Crimes can occur on the internet. For example, it is possible for websites to be used to counterfeit instruments; provide instructions on how to make explosives to cause public disturbances; engage in the business of selling firearms without a license; offer for sale drug paraphernalia; send criminal threats to persons; give away medical equipment and advice to enable terminally ill persons to commit suicide; promote gambling; engage in the sharing of copyrighted computer files and programs,[421] and distribute child pornography. Another example might involve users offering to sell illegal counterfeiting devices in a chat room, instructing others how to make illegal explosives on a personal home page, or sending criminal threats to other users via e-mail. A company's policies should be directed to avoiding liability for "aiding and abetting" such potential criminal activities on its enterprise computer network.

An outstanding compendium of information concerning laws in this area, prosecutor's guidelines, prosecution summaries by statute, and cybercrime in general can be found on the U.S. Justice Department's website, at *http://*www.*cybercrime.gov*. Even before the tragic events of September 11, 2001, and the subsequent legislative responses, there were many federal laws that touch upon these matters, including, among others:

- Child Sexual Exploitation and Pornography, 18 U.S.C. Ch. 110
- Computer Fraud and Abuse Act, 18 U.S.C. § 1030
- Criminal Copyright Infringement, 17 U.S.C. § 506(A) and 18 U.S.C. § 2319
- Economic Espionage Age, 18 U.S.C. §§ 1831-39
- Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*

---

[421] Under the No Electronic Theft Act of 1997, Congress made it clear that copyright infringement prosecutions could be conducted even if the infringer does not immediately or directly obtain monetary payment for the pirated work. 17 U.S.C. §§ 101, 506(a)(1). The law makes it a crime to willfully infringe a copyright "by the production or distribution, including electronic means, during any 180-day period, of 1 or more copies of phonorecords or more copyrighted works, which have a total retail value of more than $1000." 17 U.S.C. § 506(a)(2).

© 2004 Piper Rudnick LLP. All Rights Reserved.

- Export Administration Act, 50 App. U.S.C. § 2410
- Fraud in Connection with Identification Documents and Information, 18 U.S.C. § 1028
- Gathering, Transmitting, or Losing Defense Information, 18 U.S.C. § 793
- Government Confidential Information Act, 18 U.S.C. § 1905
- International Emergency Economic Powers Act, 50 U.S.C. § 1705(B)
- Mail Fraud and Wire Fraud, 18 U.S.C. §§ 1341, 1343
- National Stolen Property Act, 18 U.S.C. §§ 2314-15
- Racketeer Influenced Corrupt Organizations Act, 18 U.S.C. § 1961 *et seq.*
- Securities Fraud, 15 U.S.C. §§ 77Q(A) and 78J(B)
- Trafficking in Counterfeit Goods and Services, 18 U.S.C. § 2320
- Trafficking in Counterfeit Labels and Computer Program Documentation and Packaging, 18 U.S.C. § 2318

Shortly after the events of September 11, 2001, Congress passed, and the President signed, the "USA PATRIOT Act of 2001" (Public Law No: 107-56). The PATRIOT Act, as it is called, is a wide-ranging bill that among other things significantly enhanced the U.S. Government's authority with respect to surveillance, intelligence-gathering, and other law enforcement functions.

The issue of cybercrime has also garnered international attention. Even before September 11, 2001, The Council of Europe had considering adopting a "cyber-crime convention" that would be the first international treaty to address criminal law and procedure in connection with actions taken that threaten the integrity and security of computer systems, networks, data, and other technologies. The Convention on Cybercrime was adopted on November 23, 2001 and has been signed by 31 member states of the Council of Europe and four other nations (Canada, Japan, South Africa, and the U.S.); the ratification and accession process is underway. Council of Europe, *Convention on Cybercrime*, ETS 185 (Nov. 23, 2001) (copy available at *http://conventions.coe.int/Treaty/EN/cadreprincipal.htm*).

Internet fraud also remains a serious concern. The FBI and National White Collar Crime Center report, in their 2002 Internet Fraud Report, that they received 75,063 complaints in 2002,

© 2004 Piper Rudnick LLP. All Rights Reserved.

with a total dollar loss from fraud of $54 million, up from $17 million in 2001, with a median loss per complainant of $299.[422]

[422] IFCC 2002 Internet Fraud Report (2003) (available at *http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf*).

© 2004 Piper Rudnick LLP. All Rights Reserved.

AMERICANS WITH DISABILITIES ACT COMPLIANCE

Title III of the Americans with Disabilities Act ("ADA"), that is applicable to public accommodations and services operated by private entities, provides that "[n]o individual shall be discriminated against on the basis of disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation by any person who owns, leases (or leases to), or operates a place of public accommodation."[423] The question is whether the "place of public accommodation" only applies to physical places, and not to virtual places like web sites.

In *Access Now, Inc v. Southwest Airlines Co.*[424] the court addressed the question of whether Southwest's Virtual ticket counters violated the ADA by being inaccessible to blind persons. In the complaint the plaintiff asserted that of the 10 million visually impaired persons in the United States, about 1.5 million of these persons use the internet. The court noted that there are various assistive technologies that are available to assist the visually impaired on the internet, such as voice-dictation software, voice navigation software and magnification software. The court dismissed the complaint finding that "Southwest.com" was not "a place of public accommodation" and therefore not within the scope of Title III of the ADA. In so ruling, the court determined it is the role of Congress, not the court, to specifically expand the ADA's definition of public accommodation beyond physical, concrete places of public accommodation to include "virtual" places of public accommodation. Notwithstanding this ruling there is other authority defining the "place of public place of accommodation" suggesting that the Southwest ruling may not be the final answer to whether the ADA applies to publicly-available websites.

In *Doe v. Mutual of Omaha Ins. Co.*,[425] Chief Judge Posner of Seventh Circuit, writing for the court, stated that "[t]he core meaning of [the public accommodation section], plainly enough, is that the owner or operator of a store, hotel, restaurant, dentist's office, travel agency, theatre, web site, or other space, . . ., that is open to the public cannot exclude disabled persons from entering the facility and, once in, from using the facility in the same way that the non-disabled do (emphasis added)."[426] The Justice Department has also stated that the ADA's accessibility requirements apply to web sites. In addition, the National Federation of the Blind filed suit against American Online claiming that AOL's internet service violated the ADA because AOL's service was not compatible with assistive software that enables the blind to use the internet. The National Federation of the Blind agreed to withdraw the law suite after AOL agreed to undertake

---

[423] 42 U.S.C. § 12182.

[424] 227 F. Supp. 2d 1312 (S.D. Fla. 2002).

[425] 179 F.3d 557 (7th Cir.), *reh'g en banc denied*, 1999 U.S. App. LEXIS 18360 (7th Cir. 1999), *cert. denied*, 528 U.S. 1106 (2000); *see also Carparts Distribution Center, Inc. v. Automotive Wholesaler's Ass'n of New England, Inc.*, 37 F. 3d 12 (1st Cir. 1994) (Title III of ADA is not limited to actual physical structures).

[426] 179 F.3d at 559.

© 2004 Piper Rudnick LLP. All Rights Reserved.

actions to ensure the accessibility of its internet services to the blind. We believe it is likely that ADA compliance will become a serious concern in the years ahead. E-business sites should undertake steps to ensure they are accessible to persons with disabilities.

The Federal Government has adopted new government-wide regulations under Section 508 of the Rehabilitation Act Amendments requiring agencies buying electronic and information technology to ensure that the technology, including commercially available software and web-based intranet and internet applications, is accessible to persons with disabilities. This Federal regulation will undoubtedly contribute to commercially available assistive technologies for disabled persons. The availability of these technologies and technical solutions in our view will increase the public, legal and competitive pressures on e-business companies to become ADA-compliant.

© 2004 Piper Rudnick LLP. All Rights Reserved.

APPENDIX

NOTICE AND PROCEDURE FOR MAKING CLAIMS OF COPYRIGHT INFRINGEMENT

Pursuant to Title 17, United States Code, Section 512(c)(2), all notifications of claimed copyright infringement on the _____**[*COMPANY*]** system or Site should be sent ONLY to our Designated Agent.

NOTE: THE FOLLOWING INFORMATION IS PROVIDED SOLELY FOR NOTIFYING THE SERVICE PROVIDERS REFERENCED BELOW THAT *YOUR* COPYRIGHTED MATERIAL MAY HAVE BEEN INFRINGED.

WE CAUTION YOU THAT UNDER FEDERAL LAW, IF YOU KNOWINGLY MISREPRESENT THAT ONLINE MATERIAL IS INFRINGING, YOU MAY BE SUBJECT TO HEAVY CIVIL PENALTIES. THESE INCLUDE MONETARY DAMAGES, COURT COSTS, AND ATTORNEYS FEES INCURRED BY US, BY ANY COPYRIGHT OWNER, OR BY ANY COPYRIGHT OWNER'S LICENSEE THAT IS INJURED AS A RESULT OF OUR RELYING UPON YOUR MISREPRESENTATION. YOU MAY ALSO BE SUBJECT TO CRIMINAL PROSECUTION FOR PERJURY.

DO NOT SEND ANY INQUIRIES UNRELATED TO COPYRIGHT INFRINGEMENT (*e.g.* REQUESTS FOR TECHNICAL ASSISTANCE OR CUSTOMER SERVICE, REPORTS OF E-MAIL ABUSE, *etc.*) TO THE CONTACT LISTED BELOW. YOU WILL *NOT* RECEIVE A RESPONSE IF SENT TO THAT CONTACT.

Written notification must be submitted to the following Designated Agent:

Service Provider(s):	**[_____, Inc.]**
Name of Agent Designated to Receive Notification of Claimed Infringement:	**[Provide Name of Company's Designated Agent]**
Full Address of Designated Agent to Which Notification Should be Sent:	**[Provide mailing address, including street]**
Telephone Number of Designated Agent:	**[Provide Tel. # direct to agent]**
Facsimile Number of Designated Agent:	**[Provide FAX. # direct to agent]**
Email Address of Designated Agent:	**[Provide e-mail address for agent]**

Under Title 17, United States Code, Section 512(c)(3)(A), the Notification of Claimed Infringement must include the following:

- An electronic or physical signature of the owner or of the person authorized to act on behalf of the owner of the copyright interest;
- Identification of the copyrighted work (or works) that you claim has been infringed;
- A description of the material that you claim is infringing, and the location where the original or an authorized copy of the copyrighted work exists (for example, the URL of the page of the web

© 2004 Piper Rudnick LLP. All Rights Reserved.

site where it is lawfully posted; the name, edition and pages of a book from which an excerpt was copied, etc.);

- A clear description of where the infringing material is located on our web site, including as applicable its URL, so that we can locate the material;

- Your address, telephone number, and e-mail address;

- A statement that you have a good-faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law; and

- A statement by you, made under penalty of perjury, that the above information in your notice is accurate and that you are the copyright owner or authorized to act on the copyright owner's behalf.

© 2004 Piper Rudnick LLP. All Rights Reserved.

ABOUT THE AUTHORS

© 2004 Piper Rudnick LLP. All Rights Reserved.

J. T. WESTERMEIER

http://www.piperrudnick.com/jay_westermeier

J. T. ("Jay") Westermeier is a partner in Piper Rudnick LLP's Reston office. He has been involved in all aspects of information technology law, including intellectual property, technology licensing and other forms of technology contracts, business strategy and risk management, domestic and international distribution, corporate, litigation, arbitration and mediation. He represents emerging and established software, internet, electronic commerce and other information technology companies as well as information technology users and suppliers.

He is the only lawyer to ever receive the Distinguished Information Sciences Award, the highest award presented annually by the Association of Information Technology Professionals. He is a past president of The Computer Law Association, the world's largest association of its kind with members in 62 countries. He also served as the Chairman of the American Bar Association's committee on professionalism of computer specialists under the Science and Technology Section, Co-Chair of the D.C. Bar's Computer and Telecommunications Section and Director of the D.C. Computer Law Forum. He was appointed by the Governor of Virginia and approved by the Virginia Assembly to serve a four year term on the Council on Information Management for the Commonwealth of Virginia. He is also a Fellow of the American Bar Foundation and listed in Best Lawyers in America (2003-2004), Euromoney's "Guide to the World's Leading Technology, Media, and Telecommunications Lawyers" (in publication), Euromoney's "Guide to the World's Leading Information Technology Lawyers," Mondaq's "Guide to the World's Leading E-Commerce and Internet Advisors," and Law Business Research Limited's "An International Who's Who of e-Commerce Lawyers – 2nd Edition."

He serves on the advisory boards for *The Computer Law Reporter*, *E-Commerce Law & Strategy*, BNA's *Computer Technology Law*, *Commercial Law Advisor*, *Intellectual Property Counselor*, *Internet Law and Business*, and *Information Strategy*: *The Executive's Journal*. He is a USA correspondent for *Computer and Law International*. He is also on the advisory board for The Computer Law Association and the World Organization of Law and Computer Science. He founded the Georgetown University Law Center Advanced Computer and Internet Law Institute and co-founded the Virginia Bar CLE Foundation's Virginia Information Technology Legal Institute. He has edited several books on computer law, published more than 100 articles on legal issues related to information technology and has lectured at conferences, seminars and programs all over the world on numerous computer and internet-related legal topics. He is a 2001 recipient of the Burton Award for Legal Excellence.

He is a member of the Virginia, D.C. and Maryland bars and numerous courts. He litigates cases in state and federal courts. He has been a member of the American Arbitration Association's National Technology Panel of commercial arbitrators and mediators. He is also a member of the CPR Institute for Dispute Resolution Technology panel of distinguished neutrals and served on its panel of distinguished neutrals for Year 2000 disputes.

Education: George Washington University (LLM 1978); American University (J.D. 1974) (Articles Editor, Law Review); George Washington University (M.B.A. 1969); United States Military Academy (B.S. 1963). Certificate of Data Processing (CDP) awarded by the Institute for the Certification of Computer Professionals. For more information, his direct telephone number is 703.773.4216 and e-mail address is *jay.westermeier@piperrudnick.com*.

© 2004 Piper Rudnick LLP. All Rights Reserved.

LEE J. PLAVE

http://www.piperrudnick.com/lee_plave

Lee J. Plave is a partner in the Franchise and Distribution Practice Group as well as the Business and Technology Practice Groups of Piper Rudnick LLP in its Washington, D.C. office. He has had extensive experience counseling manufacturers, distributors, and franchisors with respect to the application of technology to franchise and distribution systems, including matters such as the development and implementation of e-commerce strategies, system-wide internet roll-out policies and procedures, cybersquatting and domain name disputes, consumer complaint and "cybergripe" web sites, unauthorized e-commerce, software and hardware licensing, and issues relating to online and internet services. His practice involves business, technology, franchise, distribution and antitrust matters. Mr. Plave is Chair of Piper Rudnick's Domain Name Practice Group.

He also counsels clients extensively on drafting and negotiating franchise, license, and distribution agreements for international and domestic transactions, and advising clients in all aspects of franchise and distribution law. In addition, Mr. Plave represents clients in matters before the Federal Trade Commission, where he served from 1983-87 in the Enforcement Division of the Commission's Bureau of Consumer Protection before entering private practice.

Mr. Plave serves on the Technology Committee of the American Bar Association Forum on Franchising, as well as on the Information Technology Task Force of the International Franchise Association. He served on the Board of Directors of Temple Beth Ami in Rockville, Maryland from 1997-2003.

Mr. Plave has been named to the *International Who's Who of Business Lawyers* and the *International Who's Who of Franchise Lawyers*. He is also listed among the "100 Legal Eagles" published by *Franchise Times* and was selected by his peers for inclusion in the 2005-2006 edition of *The Best Lawyers in America*.

Mr. Plave is a member of the District of Columbia, New York, and Virginia bars. He is a member of the American Bar Association, District of Columbia Bar Association and International Bar Association. Mr. Plave has published numerous articles and is a frequent lecturer at business and legal conferences, seminars and programs on franchising and distribution, the internet, e-commerce, and other information technology legal topics.

Education: New York Law School (J.D. 1983), *cum laude*; Clark University (B.A. 1980).

For more information, contact Mr. Plave at 703.773.4243 or by e-mail at *lee.plave@piperrudnick.com*.

© 2004 Piper Rudnick LLP. All Rights Reserved.