Volume 4 2006 Issue 2

INTERNATIONAL JOURNAL OF FRANCHISING LAW

Edited by Martin Mendelsohn

RICHMOND

FEATURE

Franchising: Data Protection and E-Commerce Issues in the United States

By Lee Plave, Partner, DLA Piper Rudnick Gray Cary US LLP, Washington, D.C. and Inna Tsimerman, Corporate Counsel, CS STARS, LLC, an MMC company, Chicago.

While many of the considerations involved in doing business over the Internet are the same as for conducting a business in a regular storefront in the U.S., franchisors must pay particular attention to the collection, storage, and use of personally identifiable information collected online. Heightened scrutiny combined with new and pending federal and state legislation in the United States require that companies make information privacy and security a priority and be prepared to deal with any security breaches that occur.

1. Sites that provide information

1.1. What information must be displayed by website owners to comply with local laws?

Franchisors that operate information websites must remember to consider several important issues even though data is not collected from website users. Particular considerations related to collection of data on websites are discussed in Section II below.

a. Franchisee Information

There are no specific requirements that apply to the inclusion of information about franchisees in a franchise system on the franchisor's website.

b. Fair Advertising

If franchisors advertise franchise opportunities online, such as by offering franchisee applications online for downloading or printing, franchisors must display a notice, on the page or pages where franchise applications are made available or other franchise opportunity information provided, regarding the fact that the franchising information is not intended as an offer to sell or the solicitation of an offer to buy a franchise.[1]

Even operators of informational websites must ensure that products and services are described truthfully in online ads. The FTC enforces consumer protection laws online under the Federal Trade Commission Act (the "FTC Act" or "Act").[2] Specifically, the Act allows the FTC to act in the interest of all consumers to prevent *deceptive and unfair acts or practices,* principally under Section 5 of the Act.[3] In addition to the prohibition on deceptive and unfair acts or practices, the Act requires that advertising claims be *substantiated,* especially when they concern health, safety, or performance.[4] In evaluating whether the advertisements are fair and substantiated, the advertisement must be evaluated as a whole.

The FTC considers a representation, omission or practice to be *deceptive* if it is likely to:

- Mislead consumers; and
- Affect consumers' behavior or decisions about the product or service.

The FTC considers an act or practice to be *unfair* if the injury it causes, or is likely to cause, is:

- Substantial;
- Not outweighed by other benefits; and
- Not reasonably avoidable.

In addition, if the advertisement makes express or implied claims that are likely to be misleading without certain qualifying information, that additional

qualifying information must also be disclosed. Note, however, that disclosures cannot cure false claims but can only act to qualify or limit a claim, and if a disclosure provides information that contradicts a claim, the disclosure will not act to prevent the ad from being considered deceptive.

Franchisors should consider the following in evaluating whether disclosures are likely to be clear and conspicuous in online advertisements:

- Placement of the disclosure and proximity to the relevant claim:
- Prominence of the disclosure;
- Whether items in other parts of the advertisement distract attention from the disclosure;
- Whether the disclosure needs to be repeated due to length of the advertisement; and
- Whether the language of the disclosure is understandable to the intended audience.

Specifically, to make website advertising disclosures clear and conspicuous, a franchisor should:

- Place them near, or when possible, on the same screen as the related claims; and
- When using hyperlinks to lead to disclosures,
  - make the link obvious;
  - label the link appropriately to convey the importance, nature and relevance of the information to which it leads; and
  - take consumers directly to the disclosure on the click-through page.

Parties that engage in unfair and deceptive trade practices in advertising can be subject to FTC cease and desist orders and fines of up to $11,000 per violation, and civil penalties of up to $11,000.[5]

Note also that states also regulate unfair and deceptive trade practices, and while state laws very, they may also grant private rights of actions to consumers who suffer losses as a result of violations of the these laws, in addition to civil and criminal penalties.

Finally, franchisors should note that the FTC and individual states have issued regulations with regard to unfair and deceptive trade practices for certain specific industries, goods and services. Examples include regulations regarding jewelry, wool and textile products, and "Made in the USA" labelling.

c. Copyright Notices

Franchisors should also keep in mind their copyright rights in their websites and/or materials posted on their website. While copyright protection falls outside the scope of this article, website owners should be cognizant of the protection of their copyrighted designs, documents, graphics and other materials posted on their websites.

Although the use of a copyright notice is no longer required under U.S. law, it is often beneficial. A copyright notice serves to inform the public that the work is protected by copyright. More importantly, in the event that a work is infringed, if a proper notice of copyright appears on the published copy or copies to which a defendant in a copyright infringement suit had access, then generally no weight is given to such a defendant's defense based on innocent infringement in mitigation of actual or statutory damages.

1.2. What is the courts' approach to the liability of website owners for libelous information published on the website? Include consideration both of where the website owner (a) is based overseas; and (b) operates a chat room/forum over which it exercises little control.

Libel occurs when: (i) a false and unprivileged statement that a reasonable reader or listener could understand as asserting a statement of verifiable fact; (ii) a statement that is harmful to someone's reputation; (iii) such a statement is published; (iv) the statement is made as the result of negligence or an intentional act. If the plaintiff is a public figure, he or she must also prove actual malice.[6]

a. Libellous Statement by Website Owners

Libel may arise in a trade context when a business makes untrue negative statements regarding its competitors, causing them reputational injury or loss of business.[7] Such statements may also constitute unfair and deceptive trade practices under U.S. federal and/or state law. Franchisors themselves should take care not to make libelous statements on their websites regarding competitors.

b. Libellous Statements by Third Parties

Libelous statements made by website users on website bulletin boards, message rooms, or chatrooms may also cause problems for franchisors who own or operate those websites. While some courts have said that statements made in the context of an Internet bulletin board or chat room are highly likely to be opinions or hyperbole, courts do consider the remark in

context to determine whether it is likely to be seen as an opinion, even if a controversial opinion.

A recent case gives comfort to website owners who do not actively post libelous or allegedly libelous statements themselves.[8] The plaintiff, Austin, the owner of a travel-related business, accused the owner of one of his business's competitors of posting defamatory content on the competitor's website. Austin filed a defamation lawsuit against the company that *hosted* the competitor's website, claiming that the hosting company was liable in connection with the defamatory content for refusing to take down the alleged defamatory statements.

In *Austin*, the web-hosting company argued that the Communications Decency Act of 1996 (the "CDA") shielded them from liability.[9] The CDA provides, in relevant part, that "[n]o provider or user of an interactive computer service (such as an Internet service provider) shall be treated as the publisher or speaker of any information provided by another information content provider." This so-called "good Samaritan" provision effectively creates a blanket shield from liability for parties that host content, but do not create or post content themselves – even if the content is defamatory or libelous, and even if the host does not monitor content posted on its website. In rejecting Austin's argument, the court found that Congress had spoken directly in the CDA and had encompassed distributors and original publishers alike in the exclusion from liability in such cases with respect to online defamation.[10]

Despite the "good Samaritan" shield, it is important to consider inserting disclaimers of website operator/owner liability and responsibility for postings on website bulletin boards and chatrooms in terms of use or website terms and conditions, and also to state that users are prohibited from posting libelous statements on bulletin boards and chatrooms. If such terms of use are clear and binding on users, they will help to mitigate liability for libelous comments posted online.[11]

The CDA created federal immunity to any state law cause of action that would hold interactive computer services (including e-business sites) liable for content provided by a third party.[12] Specifically, Section 230(c)(1) of the CDA provided that no interactive computer service shall be treated as "the publisher or speaker of any information provided by another information content provider." For example, in *Stoner v. eBay*,[13] an early Section 230 case involving an e-business, 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. Similarly, Section 230 immunity protected Amazon.com from liability for negative comments posted on an Amazon.com website about an author and his books.[14]

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, for errors in stock quotation information, negligence, false advertising, and other tort-based claims related to content.[15]

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, Section 230 contains exceptions for intellectual property claims, violations of federal criminal law, and violations of electronic communications privacy laws. Therefore, when a website operator was notified twice by e-mail that trademark infringing content had been placed on the website, a federal court denied a motion to dismiss a trademark infringement claim brought against the ISP, concluding that the CDA does not "automatically immunize ISPs from all intellectual property infringement claims."[16]

While Section 230 is a very important legal defense protecting online service providers from tort liability for third party content, some recent decisions suggest that some courts may be reluctant to apply its reasoning in every instance.[17] Accordingly, caution is still in order. In fact, a California state court of appeals declined to follow the U.S. Court of Appeals for the Ninth Circuit and several California state courts of appeals, and[18] ruled instead that Section 230 does not preclude potential liability of an information distributor where the distributor knows or has reason to know that the distributed material is defamatory. The California Supreme Court has agreed to review that decision.[19] The outcome of this case may have a significant effect on claims that may be brought against California e-businesses for content torts.

It is also worth noting that Section 230(c)(1) protects interactive computer services against content torts only, and likely does not apply to liability for negligence for conduct such as hacking.

1.3. Where the franchisor is providing confirmation of franchisees on its website, what franchisee information does it need to provide?

As noted above, there are no laws in the U.S. governing this area, other than the general requirement that franchise advertising must be truthful and consistent with a franchisor's disclosure document.[20] Many states consider franchisor websites to be advertising even though the Internet is akin to a national publication, which is exempted from most states' advertising requirements under exemptions that apply to out-of-state publications.[21] However, there is a general exemption available for internet advertising in many states as also discussed above.

Notably, the guidelines for preparing a disclosure document that were issued by the North American Securities Administrators Association (NASAA)[22] as well as the "FTC Franchise Rule," promulgated by the Federal Trade Commission,[23] require the disclosure of certain information about a franchisor's current and former franchisees. These records are available through commercial and state government sources, and sometimes this information is available online or electronically. As a practical matter, neither franchisors nor franchisees should have any expectation that their basic business contact information will be kept from discovery online.

1.4. What are the considerations on linking to another web owner's site?

Linking is the fundamental navigational technology that has made the web 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.

a. Linking Generally

Linking is most problematic when IMG ("IMaGe") links are used. An IMG link instructs a visiting browser to supplement the text on the page with an image contained in a separate image file. To the end-user, the integration of the two pieces of content (text and graphic) is seamless, despite the fact that they were taken from two different sources. The user may not know that the image was not created or stored locally.[24] Thus, the resulting page arguably creates a new derivative work that is based on those preexisting images or text in the linked page. If the owner of the linked website has not given permission for the link, and therefore for the creation of the derivative work, there may be an argument for copyright infringement by the linked website owner.

Note also that those who provide the means to infringe on another's copyright with the express purpose of encouraging infringement or with clear knowledge that the tool will be used to violate another's copyright may be found guilty of contributory copyright infringement. Therefore, franchisors should take care not to link to sites that distribute or contribute to the distribution of copyrighted material illegally.

Franchisors should also beware of creating consumer confusion by linking to third party websites. Since franchisors are generally unable to control the content of third party websites, it is prudent to disclaim liability for the content of third party websites within the franchisor's website terms and conditions. Franchisors might also consider including pop-up windows to notify website users who click on a hyperlink that they are being linked to the website of a third party that the franchisor does not own or control, and whose terms and conditions, and privacy policies, may differ from those of the franchisor.

Linking to sites containing materials, which infringe a third party's intellectual property rights, could subject the linking party to a contributory infringement claim[25] or direct infringement.[26] There is also a potential controversy concerning a claim by a company that it has a patent on the use of hyperlinks on the web.[27]

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 link 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.

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 likely needed and appropriate. 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.[28]

Companies are increasingly adopting policies prohibiting customers from creating or establishing links with their site. eBay, for example, recently prohibited its 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 with which they do not want to be associated. It remains to be seen whether courts will generally 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.

b. Deep Linking

Deep linking was challenged by Ticketmaster Corp. in *Ticketmaster Corp. v. Microsoft Corp.*[29] 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.[30] However, another Ticketmaster case has suggested that deep linking may be difficult to stop legally. The *Ticketmaster Corp. v. Tickets.com, Inc.*[31] litigation also focused on deep linking. In that case, the district court declined to enjoin Tickets.com from deep linking to the ticket-purchasing pages of the Ticketmaster website. The law today in the U.S. remains unclear on deep linking. The propriety of deep linking will depend on the specific facts in question. Under these circumstances, a prudent policy would be to link only to a website's homepage, rather than an internal page, unless the website operator's consent has first been obtained, especially where there may be 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 bypassing disclaimers, disclosures and website use agreements. Some website terms of use specifically prohibit deep linking.[32]

c. Framing

A frame is a window on a website through which pages from another website can be viewed. Frames are used to subdivide web pages. As with certain IMG links, frames can mislead the viewer of a site as to the creator of its content. Moreover, because of their capacity to present data from several different sources as part of one unified display, frames can easily result in the juxtaposition of unrelated, even antithetical, pieces of content, causing obvious confusion. Consequently, framing third-party information into another web page raises issues of copyright infringement (derivative works), as with linking. Franchisors should take care not to use frames in a way that cause confusion as to ownership of or association with third party sites.

1.5. What are the legal considerations when using metatags?

Metatags are hidden codes in which a website owner lists selected keywords describing the site's contents. The end user typically does not see those keywords, but search engines may use them to rank the site's relevance to particular topics.[33] 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,*[34] 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.*,[35] 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*,[36] the court reached the opposite conclusion, noting that while the alleged infringing site used meta-tags that included the plaintiff's 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 plaintiff's 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."[37] 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."[38]

In *Playboy Enters., Inc. v. Welles*,[39] 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.[40]

In an earlier decision, *New Kids on the Block v. News Am. Publishing, Inc.*,[41] 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.[42]

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."[43]

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 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.[44]

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,[45] search engine diversions, page jacking, spamdexing, pixel-tagging, cyber-stuffing[46] and mousetrapping.[47] 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.

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.

2. What are the local privacy law requirements in relation to collecting data?

Fair Practices and the FTC. Business groups in the U.S. have developed industry standards to protect the privacy of consumer information collected over the Internet and stored in databases. These standards, as well as enforcement efforts undertaken by the FTC, lead to the general conclusion that for most companies, there are four "core principles" guiding data collection: notice, choice, access, and security.

In its seminal report to Congress, the FTC wrote that "[t]hese core principles require that consumers be given notice of an entity's information practices; that consumers be given choice with respect to the use and dissemination of information collected from or about them; that consumers be given access to information about them collected and stored by an entity; and that the data collector take appropriate steps to ensure the security and integrity of any information collected."[48]

As an example of industry-led efforts, the Direct Marketing Association adopted online privacy guidelines, an easy-to-use online privacy policy generator, and will expel members who do not follow privacy safeguards set forth in its Ethical Principles. A variety of more specialized self-regulatory initiatives followed. These self-regulatory efforts yielded significant results. In 1999, the Georgetown Internet Privacy study found that 94% of the top 100 websites have posted a privacy policy.[49] Websites posting privacy policies increased significantly.[50] However, an FTC survey in 2000 of major e-commerce Websites found that only about 20% addressed all five of the fair information practices regarding privacy (notice; consumer choice regarding disclosures; right of access to and to correct information stored by the business; maintaining the security of the information; and some right of redress in the event of a violation), even though the FTC also found nearly 90% compliance rate by internet companies with respect to the first fair information practice – posting notice of their privacy practices on their Websites.[51]

Several organizations, such as the Better Business Bureau Online (BBB Online) and TRUSTe, accept applications for a privacy seal that enables consumers to identify Websites that pledge to meet privacy standards. In addition, the Direct Marketing Association and the Online Privacy Alliance have adopted self-regulatory programs and the Direct Marketing Association provides, free of charge, a privacy policy generator on its Website to assist companies in asking the initial questions necessary to develop their own privacy policy.[52]

Companies that make self-regulatory promises are required to keep them. The FTC and State Attorneys General in the U.S. treat material violations of promises made in privacy policies as deceptive trade practices. Furthermore, there is a possibility that class lawsuits could be brought by consumers against websites that violate their own privacy policies in a way that causes harm to consumers. In recent years, the FTC has begun to expand the range of deceptive trade practice enforcement actions it brings to promises regarding the security of personal information a company collects,[53] and failures to provide adequate notice to data subjects regarding major changes in privacy practices.[54]

E-businesses should develop privacy policies with input from operations, marketing and legal personnel and write privacy policies so that internet users can understand them. E-businesses should treat the words in their privacy policy seriously and only make promises that they are prepared to keep consistently. For example, unequivocal promises, such as that a company will never disclose Personally Identifiable Information ("PII") to third parties, are inadvisable because disclosures almost invariably occur to carry out or enforce transactions, in responding to lawful legal process from law enforcement or civil litigants, in the event of bankruptcy or liquidation of a company's assets. Thus, privacy policies should leave room for these and similar sorts of disclosures. Furthermore, human and computer errors can result in the disclosure of PII. Finally, e-businesses should be wary of making ambitious promises regarding data security. Companies that make such promises but do not live up to the Gramm-Leach-Bliley Act ("GLB") safeguards procedures for data security have been targets of FTC enforcement of two regulations – the Standards for Safeguarding Customer Information Rule ("Safeguards Rule")[55] and the Privacy of Consumer Financial Information Rule ("Privacy Rule"),[56] in cases where the companies make disclosures, whether or not those disclosures were made inadvertently.[57]

Privacy policies should be integrated by reference in website terms of use, including its limitations on liability, dispute resolution and governing law provisions.[58] Otherwise, privacy policies are likely to be treated as contractual commitments without any limitation on liability or other contractual protection. Links to the privacy policy should be located in

conspicuous font or point size on the home page of an e-business size and near the point of information collection on a website (for example, near a form).

While self-regulation continues to be the most important guide for e-business privacy practices, government regulation has become a factor as well. A few examples illustrate the point:

Fair Credit Reporting Act. The Fair Credit Reporting Act ("FCRA"),[59] which was enacted in 1970 and which took effect April 25, 1971, imposes requirements that apply to the collection of data from consumers. The protections of the FCRA have been interpreted in a FTC Staff Advisory Opinion to cover persons seeking to become independent contractors.[60] Among other things, the FCRA imposes on companies that collect and use consumer reports various requirements pertaining to data collection, accuracy and correction of data maintained in these records, the dissemination of these records, as well as standard for security of the information. The law applies to consumer reporting agencies that assemble and disseminate reports, companies that use of consumer reports to make decisions about credit, employment, insurance, and other matters. Users – the companies that in effect "buy" credit reports, are also subject to requirements limiting the use of that information to only specific permitted purposes, so long as they disclose certain information about that use to consumers. The FTC has been active in bringing cases where it believes that there have been violations of the FCRA, including, most recently, a consent decree reached with ChoicePoint, Inc., in which the company agreed to pay a $10 million civil penalty as well as $5 million in consumer redress.[61]

Regulation of Children's Online Privacy. Because data regarding children is widely viewed as sensitive, children's online privacy is regulated at the federal level under a parental consent opt-in regime. The Children's Online Privacy Protection Act ("COPPA")[62] was enacted in 1998 with the support of industry. COPPA regulates sites directed at children or that know that they are collecting Personally Identifiable Information ("PII") online from a child or providing an online forum through which children may communicate. The FTC's Final Rule implementing COPPA[63] applies to the collection of personal information online from children under the age of 13.

COPPA requires sites, or portions of sites, that are "directed" at children under the age of 13 or that know that they collecting PII from children to: (1) provide clear, prominent and understandable notice of what PII they collect online from children, how it will be used, and how it will be disclosed; (2) obtain "verifiable consent" from a parent of a child for the collection, use and disclosure of the child's PII; (3) provide parents with the ability to opt-out of further collection, retention or use of their child's PII; (4) provide parents with a reasonable means to review information that is collected from children; and (5) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of PII online collected from children.[64] The FTC's Rule implementing COPPA adopted a sliding-scale approach for providing verifiable parental consent, and the FTC recently proposed making this approach permanent. It allows websites to use an e-mail-plus mechanism to obtain consent for internal uses (as opposed to disclosures) of covered data.

COPPA's requirements are burdensome, so that e-businesses should consider whether the costs and burdens of compliance with COPPA are worthwhile or should be avoided by refraining from targeting sites or portions of sites at children under 13 and from collecting age information from visitors. For example, children may sign up for sweepstakes used as an incentive for registrations. They may also be discovered to be younger children during customer support telephone calls, which is material because actual knowledge that the user is less than 13 years old also requires compliance with COPPA. 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 a letter from former FTC Chairman Tim Muris to Rep. Edward J. Markey.[65]

State Privacy 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 any personally identifiable information over the internet from California consumers who visit their site.[66] This law applies to Website operators and online services located both outside and inside California. All Website operators in the U.S. that collect PII need to consider their privacy policies in light of California's online privacy law.

The law's requirements are not burdensome. They require that posted privacy policies: (1) identify the categories of personally identifiable information collected and the categories of third-parties with which the Website operator may share that information; (2) explain, if consumer may review and make changes to personally identifiable information the site collects, how the consumer may do so; (3) describe how the website operator notifies consumers of changes to the privacy policy; and (4) note the date when the current version of the privacy policy took effect. Most privacy policies cover the first and second of these elements, but may not cover the third and fourth elements. The law also

requires that privacy policies be posted "conspicuously" through one of a variety of methods, including a clearly visible hyperlink labelled privacy on an e-business' home page. Companies have a thirty-day grace period after notice of non-compliance to come into compliance with the notice requirement. In addition, the law prohibits "negligent and material" or "knowing and wilful" misrepresentations in privacy policies. As a practical matter, due to recent reforms in California's unfair competition statute,[67] violations are likely to be enforced only by government officials, not the plaintiff's bar.

Ironically, another California privacy law, Civil Code § 1798.83 (also known by the designation it was given during its consideration by the legislature – "S.B. 27"), that is not specific to online activities, may have a greater effect on online privacy practices. S.B. 27 first requires businesses and non-profits that disclose personal information regarding California consumers to third parties for the third parties' commercial marketing purposes to designate a contact point to receive inquiries regarding privacy practices and compliance with the statute. Designations may be made on a business' or non-profit's Website and should be labelled "Your California Privacy Rights."

Second, S.B. 27 requires businesses and non-profits who receive these inquiries either to provide: (1) a detailed, annual notice of exactly what data elements they disclosed during the previous calendar year and the names of the businesses to whom the data were disclosed; or (2) the opportunity to opt out or opt in to disclosures to third parties (including, in the case of a range of more sensitive data elements, disclosures to affiliates).[68] S.B. 27 allows privacy advocates and the press to obtain detailed information about business' and non-profit's data disclosure practices for third party commercial marketing purposes unless the business or non-profit provides a broad opt-out of disclosures, including in many cases an opt-out of disclosures to affiliates. Violations are enforceable by the plaintiff's bar through private lawsuits for statutory damages. The net effect of S.B. 27 is to give e-businesses a significant incentive to provide an opt-out of disclosures to third parties for their marketing purposes, a requirement that is missing from the state's online privacy law. By the start 2006, 22 other states joined California in adopting laws requiring some form of notice in the case of a data security breach or the disclosure, intentional, inadvertent or otherwise, of PII.[69] Most of these laws apply not only to online data breaches, but also to data breaches that occur in other settings (e.g., it may be argued that these laws apply to the loss of a laptop computer owned by a franchisee's employee containing customers' PII).

Although the chairman of the U.S. House of Representatives committee with jurisdiction over consumer protection issues supports broad privacy regulation, federal privacy regulation of Websites is unlikely in the near to medium term. The Federal Trade Commission, which would be the lead agency charged with enforcing federal requirements, has recommended against regulation of sites that are not directed at children. 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.[70] His successor, Chairwoman Deborah P. Majoras, has not deviated from this position.

Other Sector-Specific Laws. In various contexts, sector-specific privacy requirements will affect businesses. Among the most significant of the requirements at the federal level are:

- The *Health Insurance Portability and Accountability Act of 1996* (known as "HIPAA"), which deals with health care information privacy. HIPAA sets standards for electronic health information transactions. HIPAA rules apply not only to medical providers and health 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.[71]
- The *GLB*, which limits when a "financial institution" may disclose non-public information about consumers.[72] 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 law's notice, opt-out, and disclosure requirements.[73]

It is important to note that both HIPAA and GLB require companies to whom these laws apply to require their service providers who use, collect or otherwise process personally identifiable information (subject to these laws) on their behalf to agree in writing to comply with the same data privacy and security requirements as are applicable to the companies themselves.

Data Security Regulation. There are a number of state laws and also pending federal legislation regarding data security. California has taken a leading role in enacting security laws. For example, California "A.B. 1950" requires businesses to implement and maintain reasonable security procedures and practices to protect certain unencrypted "personal information" from unauthorized access, destruction, use, modification, or disclosure; and to contractually required unaffiliated

third parties to which such information is disclosed to also implement and maintain such procedures and practices. "personal information" protected under this law is defined as a person's first and last name (or first initial and last name), in combination with one or more of the following sensitive data elements: (a) a Social Security number ("SSN"); (b) a drivers license number; (c) California Identification Card Number; (c) account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts; or (d) information regarding medical history, or medical diagnosis or treatment by a health care professional.[74]

Most importantly, California has led the way in enacting security breach notification laws.[75] By January 2006, at least 22 states had enacted new security breach notification laws, all generally based on the California law.[76] Generally, these law impose a duty on the party collecting personally identifiable information over the Internet, or on whose behalf information is collected, to notify individuals whose *unencrypted* sensitive personal information has been accessed or acquired without authorization (e.g., through hacking or other means). Notices of security breaches provided to individuals must contain a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person. In addition, in certain cases, notice of the breach must also be given to state enforcement agencies, such as the state Attorney General's office, as well as to consumer reporting agencies. Typically, sensitive personal information is defined as an individual's first and last name (or first initial and last name), in combination with his or her SSN, driver's license or state identification number, or financial account or credit or debit card number (along with the PIN or access code required to access the account). Note that these laws apply only to unencrypted data, therefore, having personal information in an encrypted system may avoid applicability of these laws – and the obligation to comply with their burdensome security breach notification requirements – altogether.

Most laws provide some mechanism for state enforcement of the security breach notification laws, and some states also expressly provide for an individual right of action, permitted injured individuals to sue for damages.

Beginning in the spring of 2005, the U.S. Congress had also introduced legislation to require companies to notify person affected by data security breaches involving their sensitive personal information. This legislation would, presumably, pre-empt conflicting state security breach notification laws.

In addition, both HIPAA and GLB have stringent data security components.

Other Consumer Data Protection and Security Regulation. There are additional federal and state laws that restrict the use of account and identity numbers.

- *Account Number Truncation* – Section 605(g) of the FCRA (as amended by the Fair and Accurate Credit Transactions Act) prohibits any person that accepts credit or debit cards for the transaction of business from printing more than the last *five (5) digits* of the account number or the expiration date of the card on any receipt provided to the cardholder. There are some state laws have enacted more stringent requirements.[77]
- *Restriction on Use and Display of Social Security Numbers* ("SSNs") – There are a number of state laws which prohibit or restrict certain uses or the display of SSNs, which general serve as federal identification numbers for U.S. nationals. Generally, these laws restrict or prohibit the use of SSNs as account numbers, and the ability to request from individuals or display SSNs on the Internet over an unsecure connection or unencrypted transmission.[78]

3.1. To what extent can the franchisor control what activities a franchisee can engage in through its website.

Franchisors and franchisees are generally free to contract on these issues in the United States. Agreements today should expressly contemplate and permit e-business, and it is even more important now to avoid any "exclusive" arrangements that may 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 (with renewal periods included) run from 20 to 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.[79]

3.2. What local legal requirements must be complied with by website owners who wish to sell over the internet?

There are generally few requirements in the U.S. that website owners need to meet in order to sell their

products over the internet, outside of taxation issues, privacy and data protection issues, and related matters. By and large, the sale of goods and services over the Internet are treated very much like the sale of goods and services in the tangible off-line world.

Antitrust Laws. Of course, the standard antitrust rules apply to firms engaged in e-commerce. For example, in *In the Matter of Fair Allocation System, Inc.,* Bus. Franchise Guide (CCH) ¶ 11,525 (FTC Oct. 22, 1998), Chrysler franchisees allegedly attempted to coerce The Chrysler Corporation into restricting the supply of automobiles that were being advertised over the Internet and sold at discount prices by certain dealers. The franchisee organization entered into a consent agreement with the FTC, promising not to engage in any boycotts or to threaten any boycotts of any automobile manufacturers or consumers. In addition, in *ChoiceParts, LLC v. General Motors Corp.,* the developer of an Internet-based system that allegedly would allow automobile dealers and repair shops to efficiently buy and sell automobile parts to and from one another (B2B) charged the "Big Three" automobile manufacturers with Sherman Act Section 1 and 2 violations for jointly denying the plaintiff access to an essential element of competition in the parts locator business-parts data.[80] The plaintiffs alleged that the automobile manufacturers conspired to deny access to the parts data information because, according to the complaint, the manufacturers are attempting to monopolize e-commerce as it relates to the automotive industry. In April 2002, the *ChoiceParts* court declined to grant plaintiffs a "forced license" to the parts data by preliminary injunction. The court ruled that, although the plaintiff's conspiracy allegation had at least some chance of success on the merits, the plaintiffs did not yet have a prevailing case, and acknowledged the potential harm to the auto manufacturers resulting from such a license outweighed the plaintiff's interest in obtaining the injunction.[81] The outcome of the case is still pending.

In the context of the Robinson-Patman Act, part of the U.S. litany of antitrust laws (along with the principal pillars, the Clayton Act and the Sherman Act) there is authority recognizing that, for Robinson-Patman Act purposes, Internet retailers may be in competition with traditional bricks and mortar establishments. *National Ass'n of College Bookstores Inc. v. Cambridge Univ. Press,* 990 F. Supp. 245 (S.D.N.Y. 1997) (Amazon.com competes with college bookstores).

Auto Dealer Laws. In addition to *ChoiceParts,* at least two other cases involved the automobile industry. In *Ford Motor Co. v. Texas Dep't of Transp.,* the Texas Department of Transportation ("TDOT") filed an administrative complaint against Ford, alleging that Ford was violating the Texas Motor Vehicle Commission Code by attempting to sell pre-owned vehicles via the Internet.[82] Using the website, Ford advertised cars that had been previously leased to customers by Ford dealers, sold to car-rental chains, or used by Ford employees. Through the website, a customer could arrange to have a vehicle delivered to a local dealer for inspection and possible purchase at a fixed price set by Ford; Ford would transfer title to the dealer, who would consummate the sale. Texas law prohibited Ford, as an automobile manufacturer, from owning an interest in or acting as an auto dealer. TDOT argued that by marketing used vehicles via the Internet, Ford was essentially acting as a dealer without a license. Ford challenged TDOT's complaint, and filed suit in federal court alleging that the Texas dealer law violated Ford's Constitutional rights, including the dormant Commerce Clause doctrine. The Fifth Circuit affirmed the district court's grant of summary judgment in favour of TDOT, dismissing Ford's Constitutional claims.

Like the *Ford* case, *Alliance of Automobile Manufacturers v. Hull,* also involved a challenge to the constitutionality of a state law regulating automobile manufacturers.[83] Two trade groups whose members manufacture cars challenged an Arizona law intended to prevent automobile manufacturers from unduly competing with their dealer franchisees. The statute at issue would have prevented manufacturers from selling other products and services related to automobile sales, such as financing, after-market accessories, extended warranties, and emergency roadside assistance. The plaintiffs sought a preliminary injunction, alleging that the Arizona law violated the Constitutional rights of their members. In March 2001, the court denied the plaintiff's motion for a preliminary injunction. The case later settled by the parties' agreement to certain changes that were made to the Arizona law.

In 2001, FTC Commissioner Thomas B. Leary spoke at the 34th Annual International Franchise Association Legal Symposium, expressing concerns about the Constitutionality of limitations on manufacturer's Internet sales activities.[84]

State-Federal Considerations. Because of the impact of the U.S. Constitution's Commerce Clause,[85] there are limits on what states may do to regulate the sale of goods and services in interstate or international commerce, as those powers are intended to be expressly reserved to the federal government under the U.S. system of federalism. There is, however, a classic tension between state governments and the federal government as to where the dividing line is drawn between the proper assertion of state authority over matters such as regulating the quality of certain

items and services sold within its borders, and Congressional authority to regulate interstate and international commerce. These questions are often very factually-specific, and sometimes involve whether a transaction takes place in – as well as impacts – interstate or international commerce. In the Internet age, the degree to which commercial transactions are isolated to just one state is different than was the case just 10–15 years ago.

The FTC voiced concern about the possible effects that state law might have to restrict competition on the Internet. In particular, the FTC was concerned about the effect on interstate commerce from state regulations that are ostensibly intended to protect "bricks and mortar" business from Internet competition. In October 2002, the FTC held a public workshop on the topic, featuring testimony from industry representatives, state and federal officials, academics, and public policy organizations.[86] The Workshop focused on use of the Internet to engage in wine sales, cyber-charter schooling, the sale of contact lenses, auto sales, casket sales, providing online legal services, telemedicine and online pharmaceutical sales, online auctions, online provision of real estate, mortgage and financial services, and retailing.

Online Pharmacies. There are many problems with specialized applications and specialized e-business efforts. For example, online pharmacy sites are subject to prosecution by the U.S. Justice Department for selling drugs without a prescription,[87] without parental consent, without consultations with a doctor, and without a licensed or registered pharmacist dispensing the drugs.[88] In addition, making certain drugs – for example, steroids – available for delivery in the U.S. may violate other federal laws[89] and international conventions.[90] In addition, online pharmacies must comply with HIPAA requirements, including the provision of a specific HIPAA notice of privacy practices to individuals who purchase drugs online.

Licensed Professionals. 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. In many instances, these practices are regulated at the state level, and the effect of local law can be to make sure that online providers are sufficiently able to render service that is consistent with local standards and requirements. However, the converse is that these laws can sometimes be anti-competitive, protecting local practitioners' practices. Striking the proper balance between affording providers access and uphold consumer protection standards is a daunting task that has been under review at the federal level.[91]

Online Gambling. Online gambling sites have been criminally prosecuted under federal law[92] as well as in states where gambling is illegal,[93] even where the server is located in a state or Indian reservation or offshore where gambling is legal. In February 2000, Jay Cohen was convicted by a jury in New York in connection with an internet gambling enterprise that he set up in Antigua.[94] of "conspiracy to violate the Wire Wager Act and seven substantive violations of the Wire Wager Act in connection with his operation of World Sports Exchange." However, despite these legal standards, the popularity, and likely, the profitability, of online gambling – and the difficulties inherent in regulating the Internet – are such that even so-called "blue chip" investment houses such as Fidelity, Goldman Sachs, and Merrill Lynch are reportedly investing in online gambling enterprises.[95]

States have also passed legislation criminalizing the sale of narcotics, beer and alcohol over the internet. In *State of Missouri v. Beer Nuts, Ltd.*,[96] 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.[97] Others have banned online sales of cigarettes to minors.[98] 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.[99] Many of these statutes fail to pass this strict scrutiny test and are not being enforced.[100] 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."[101] 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 labour of its residents."[102]

Wine Sales. Some states had limited or banned wine sales over the Internet, contending that these limits are allowed under the Twenty-First Amendment to the U.S. Constitution (ratified in 1933, the Twenty-First Amendment repealed the Eighteenth Amendment, which when ratified in 1919, established Prohibition) and that they furthered important public policies such as temperance, preventing the sale of alcohol to minors, and facilitating the collection of sales taxes. Some states,

however, had banned only internet wine sales from out-of-state wineries, setting up a conflict between the Commerce Clause of the U.S. Constitution and the Twenty-First Amendment.[103]

In *Granholm v. Heald,* 125 S. Ct. 1885 (2005), the U.S. Supreme Court determined that the New York and Michigan statutes prohibiting or imposing additional burdens on out-of-state wineries from shipping wine directly to in-state consumers but permitting in-state wineries to do so discriminated against interstate commerce. As such, the Supreme Court, in a 5 to 4 decision, affirmed the Sixth Circuit ruling concerning the Michigan statutes and reversed the Second Circuit ruling with respect to the New York statutes. These two cases challenging state laws regulating the sale of wine from out-of-state wineries to consumers in Michigan and New York had been consolidated. The Court found the differential treatment between the in-state and out-of-state wineries to constitute explicit discrimination against interstate commerce, and rejected an argument that the Twenty-first Amendment to the Constitution gave states the absolute authority – notwithstanding the Commerce Clause – to regulate wine sales in their states.[104] In reaching that conclusion, the Court emphatically concluded that the principles underpinning the Commerce Clause trump the language of the Twenty-first Amendment:

> State policies are protected under the Twenty-first Amendment when they treat liquor produced out of state the same as its domestic equivalent. The instant cases, in contrast, involve straightforward attempts to discriminate in favor of local producers. The discrimination is contrary to the Commerce Clause and is not saved by the Twenty-first Amendment.''[105]

In the *Granholm* decision, the Supreme Court also noted that technological improvements, in particular wineries' ability to sell their wares over the Internet, have helped make direct shipments an attractive sales channel. In dictum, the Court also observed that the Federal Trade Commission had identified that State bans on interstate direct shipping represent the single largest regulatory barrier to expanded e-commerce in that line of commerce. In addition to balancing the Commerce Clause and the provisions of the Twenty-first Amendment, the Court also examined the states' arguments that they had a legitimate interest in their regulatory approach – namely, protecting minors who might otherwise purchase wine over the Internet. The Court discounted that argument and observed that ''[e]ven were we to credit the States' largely unsupported claim that direct shipping of wine increases the risk of underage drinking, this would not justify regulations limiting only out-of-state direct shipments.''[106] Ultimately, while the *Granholm* ruling is a very strong message from the Court as to the primacy of federal Commerce Clause power, the impact is to significantly bolster not only e-business in the wine industry, but the broad range of interstate e-business in general.

3.3. Do the legal requirements change in any way where the goods/ services are supplied exclusively on-line?

There are no such standards generally applicable in the United States.

3.4. In what circumstances will the local courts override choice of a foreign law and jurisdiction?

An e-business website is a virtual storefront with worldwide exposure, open for business whenever users from around the world want to shop there. The internet is not limited by any geographic or jurisdictional boundaries and is believed to connect more than 159 countries. The most fundamental legal issue affecting the legal aspects of e-business concerns jurisdiction and choice of law. 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. Merely by virtue of its presence on the World Wide Web, a company's website (and the content on that site) can reach a virtually unlimited audience and thus could become a source of litigation or enforcement actions in many different places. 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.[107] In general, the law with respect to jurisdictional issues involving the internet is evolving and is far from certain.[108] 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, 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 jurisdiction.[109] Courts have found that merely providing an online purchase order form that must be mailed or faxed does not provide enough interactivity for jurisdiction.[110] Similarly, a return e-mail address or 800 telephone number along with a passive website is still not sufficient for jurisdiction.[111] 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 though it was accessible in the state, and observing that the site was even written in German.[112]

The second category of cases requires analysis of the nature and extent of the e-business' activities beyond simply operating 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—where most e-commerce sites will likely find themselves—is at the opposite end of the continuum from passive websites. This category involves conducting 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.[113] 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 the *Zippo* decision, which established this framework, succinctly stated the jurisdiction issue as follows:

> [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 residents of the forum state via its web site, or through sufficient other related contacts.[114]

An Illinois defendant was found subject to jurisdiction in Maryland in a case involving a cyber squatting claim.[115] There, the defendant registered a domain name (*www.cole-tuve.com*) that infringed on the plaintiff's name, in an effort to redirect browsers, who might otherwise have sought the plaintiff's website at *www.coletuve.com,* to the defendant's website. The court found that under the standard enunciated by the U.S. Supreme Court in *Burger King Corp. v Rudzewicz*, 471 U.S. 462 (1985), it was proper to exercise jurisdiction over the defendant if it "purposefully directed its activities toward residents of Maryland."[116] The court concluded that "[f]oreign defendants who intentionally harm residents in the forum state have been held to have intentionally interacted with the state" and that the defendant "intended for the intentional tort to impact the plaintiff in the forum state."[117]

The language and currency designations of a website can provide a strong indication of targeting in U.S. courts. For example, 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.[118] A different outcome based on consistent reasoning was reached in *Euromarket Designs, Inc. v. Crate & Barrel Limited.*[119] 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.

The issue of transnational jurisdiction is particularly important where there are conflicts of law and an e-business has assets and can be sued in a foreign state. Libel and hate speech cases are a flashpoint in this regard because the First Amendment and 47 U.S.C. § 230 afford protections for intermediaries far greater than those in most other English-speaking jurisdictions. In late 2002, the High Court of Australia ruled in a landmark case, *Dow Jones & Co., Inc. v. Gutnick,*[120] 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.[121]

In the U.S., the law is still evolving on the type of conduct that will result on a finding of sufficient 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.

Companies turn to contracts and terms of use to limit jurisdictional exposure.

Arbitration and Forum Selection/Choice of Law Clauses. 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.[122] Arbitration clauses should expressly provide that class action arbitration is prohibited under the agreement if class action suits are to be avoided.[123] 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.[124] 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.[125] It is also desirable to provide that the arbitration agreement is subject to the Federal Arbitration Act to pre-empt any conflicting state statutes.[126]

Forum Selection/Choice of Law Clauses and Website Disclaimers. Forum selection clauses and choice of law clauses address jurisdictional risk directly and have become a very important risk management strategy. They are commonly used in website terms of service and terms of use agreements.[127] In addition, 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 indicated 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 emphasized and specified the exclusive market served by its e-commerce business.[128] One court expressed concern over the jurisdictional exposure of 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 forum selection clause.[129]

Country-Specific Sites. Some multinational companies are addressing the legal concerns relating to global e-business by setting up separate, country-specific websites that are tailored to comply with the laws in particular 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.[130] 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.

3.5. What is the treatment of electronic signatures and the verification of identity within the local jurisdiction?

Today, information is almost universally used, stored and transmitted in digital form. As early as 1999, over 90% of information generated by companies was in digital form stored on computers.[131]

On June 30, 2000, U.S. President Bill Clinton signed the Millennium Digital Commerce Act, colloquially known as E-SIGN ("E-SIGN"), which has pre-empted almost all contrary federal and state laws placing conditions on the use of electronic signatures, agreements or records.[132] E-SIGN 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 made online transactions and online notices to consumers significantly easier. E-SIGN established 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.[133]

E-SIGN defines the term "electronic signature" be an electronic sound, symbol or process that is "attached to or logically associated with a contract or other record and executed or adopted by a person *with the intent to sign* the record."[134] In order for an electronic signature or an electronic record to have legal effect the parties must have agreed to transact electronically.[135]

In 1999, before E-SIGN was adopted, 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. By then, 49 U.S. states either enacted UETA or were considering some form of electronic signature legislation. However, states that enacted UETA had not done so in a uniform way. Despite the broad consensus on the need for electronic signature legislation, there was previously little uniformity in the approaches considered by state legislatures. E-SIGN was designed to promote uniform legal standards across all the U.S., facilitating interstate electronic commerce. However, state UETA laws are not pre-empted by E-SIGN as long as the version of UETA adopted by the particular state is not inconsistent with E-SIGN.[136]

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 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.[137] 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.[138]

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 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 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,[139] agreed upon, and that 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.

Conclusion

While many of the considerations involved in doing business over the Internet are the same as for conducting a business in a regular storefront in the U.S., franchisors must pay particular attention to the collection, storage, and use of personally identifiable information collected online. Heightened scrutiny combined with new and pending federal and state legislation in the United States require that companies make information privacy and security a priority and be prepared to deal with any security breaches that occur. Franchisors, in particular, must take care to implement policies to address these issues, not only themselves, but also mandate that their franchisees do the same. Special attention should be devoted to establishing system-wide policies that address data collection, storage, and use so that the franchisor and franchisees in a system meet their legal obligations. Additionally, the adoption of system-wide best-practices policies will stave off having one party's failure to adhere to state or federal law result in liability, and well as damage to the name and reputation of all who are associated with the business.

Footnotes

1. This standard was established by the North American Securities Administrators Association (NASAA) on September 9, 2001, when it issued model regulations to be followed by state franchise authorities in exempting internet advertising (reprinted at Bus. Franchise Guide (CCH) ¶ This standard has been followed in the State of Washington (Bus. Franchise Guide (CCH) ¶ 5470.90) and in California (Exemption for Internet Offers), Cal. Code Regs., tit. 10, § 310.100.3 (reprinted at Bus. Franchise Guide (CCH) ¶ 5050.0715), California (Exemption for Internet Advertising), Cal. Code Regs., tit. 10, § 310.156.3 (reprinted at Bus. Franchise Guide (CCH) ¶ 5050.355), Minnesota (whose Commissioner of Commerce issued an order adopting the NASAA policy, reprinted at Bus. Franchise Guide (CCH) ¶ 5230.82), New York, at N.Y. Comp. Code R. & Regs., tit. 13, § 200.12 (reprinted at Bus. Franchise Guide (CCH) ¶ 5320.12), and Washington State (policy statement FPS-6, reprinted at Bus. Franchise Guide (CCH) ¶ 5470.90).

2. 15 U.S.C. §41 et seq. The FTC Act regulations can be found at 16 C.F.R. §305 et seq.

3. See 15 U.S.C. §45.

4. Evidence required to substantiate claims will depend on the product, the claims, and what experts in the field reasonably consider to be necessary.

5. Federal Trade Commission Act, Section 5(l) (15 U.S.C. § 45(l)).

6. See New York Times Co. v. Sullivan, 376 U.S. 254 (1964).

7. These statements, if false, are often found to be libelous per se:
   - Charges any person with crime, or with having been indicted, convicted, or punished for crime;
   - Imputes in an individual the present existence of an infectious, contagious, or loathsome disease;
   - Tends directly to injure an individual in respect to his/her office, profession, trade or business, either by imputing to him/her general disqualification in those respects that the office or other occupation peculiarly requires, or by imputing something with reference to his/her office, profession, trade, or business that has a natural tendency to lessen its profits; or
   - Imputes to an individual impotence or a want of chastity.

8. Austin v. CrystalTech Web Hosting, 2005 WL 3489249 (Ariz. App. Div. 1, December 22, 2005).

9. See 47 U.S.C. § 230.

10. See also Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir., 1997).

11. Factors such as whether terms were clearly and conspicuously posted and whether users consented to be bound by such terms will be considered in determining whether such website terms of use are binding.

12. 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.

13. 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).

14. Schneider v. Amazon.com, Inc., 108 Wash. App. 454 (Wash. Ct. App. 2001).

15. 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 Corp., 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., 347 F.3d 655 (7th Cir. 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 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., 325 F.3d 87 (2d Cir. 2003) (single-publication rule applies in NY, even to internet publication; plaintiff's claim was time barred).

16. Gucci America, Inc. v. Hall, 135 F. Supp.2d 409, 417 (S.D.N.Y. 2001).

17. See, e.g., Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 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).

18. Barrett v. Rosenthal, 9 Cal.Rptr.3d 142, (Cal. App. 1 Dist., 2004).

19. Barrett v. Rosenthal, 87 P.3d 797 (Cal. Sup. Ct. 2004).

20. See, e.g., N.Y. Gen. Bus. Law § 683(11): "Any advertisement in whatever form, including periodicals or on radio or television, shall contain a statement that no offer of such franchise is made except by such offering prospectus, and all such advertising shall be consistent with the representations and information required to be set forth in such prospectus as hereinbefore in this section provided."

21. See, e.g., N.Y. Code Regs. and Rules § 200.9 (reprinted at Bus. Franchise Guide (CCH) ¶ 5320.09).

22. Guidelines for the Preparation of a Uniform Franchise Offering Circular, adopted April 25, 1993 (Item 20(B) and 20(E)). Bus. Franchise Guide (CCH) ¶ 5700.

23. 16 C.F.R. § 436.1(a)(16)(iii).

24. In this respect, an IMG link is different from an HREF link; a user following an HREF link is usually aware that he has "changed pages," either from the different appearance of the newly accessed page, or from the change in the URL address display in the web browser.

25. 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).

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

27. 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).

28. 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.

29. No. 97–3055 DDP (C.D. Cal. filed April 28, 1997).

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

31. 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).

32. See, e.g., Cairo v. Crossmedia Services, Inc., 2005 WL 756610 (N.D. Cal. April 1, 2005).

33. Most Internet search engines have reduced or eliminated their reliance on metatags due to the proliferation of inaccurate and misleading uses by opportunistic marketers.

34. 1997 U.S. Dist. LEXIS 14345 (N.D. Cal. 1997).

35. 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.

36. 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).

37. 300 F.3d 808, 814 n.13 (7th Cir. 2002) (as amended, Oct. 18, 2002) (emphasis supplied).

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

39. 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.

40. 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).

41. 971 F.2d 302 (9th Cir. 1992).

42. Id. at 308.

43. 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).

44. 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.

45. 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.

46. 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).

47. 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).

48. Federal Trade Commission, Report to Congress on Privacy Online, June 1998 (available at www.ftc.gov).

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

50. 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.

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

52. See http://www.the-dma.org/privacy/creating.shtml. Our firm has helped The DMA with this effort.

53. See, e.g., In the Matter of Vision I Properties, LLC, doing business as CartManager International, File No. 042–3068 (FTC Apr. 19, 2005); 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).

54. In the Matter of Gateway Learning, FTC File No. 042–3047 (FTC July 7, 2004).

55. 16 C.F.R. Part 314.

56. 16 C.F.R. Part 313.

57. See, e.g., In the Matter of Sunbelt Lending Services, Inc., File No. C-4129 (FTC Jan. 3, 2005); 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).

58. 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.

59. 15 U.S.C. §§ 1681–1681x.

60. See staff advisory opinion from Ronald Isaac, FTC Bureau of Consumer Protection, Credit Practices Division (letter dated Feb. 23, 1998) (available at http://www.ftc.gov/os/statutes/fcra/allison.htm).

61. U.S. v. ChoicePoint Inc., FTC File No. 052–3069 (consent decree) (filed Jan. 30, 2006, N.D. Ga.) (available at http://www.ftc.gov/opa/2006/01/choicepoint.htm).

62. 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, 124 S. Ct. 2783 (2004).

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

64. 15 U.S.C. § 6502(b).

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

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

67. Cal. Bus. & Prof. Code § 17200.

68. Cal. Civ. Code § 1798.83.

69. Arkansas, Ark. Code Ann. §§ 4–110-101; Connecticut, Conn. Gen. Stat. §§ 36a-701; Delaware, Del. Code Ann. tit. 6, §§ 12B-101; Florida, Fla. Stat. § 817.5681; Georgia, Ga Code. Ann. §§ 10–1-910; Illinois, 815 ill. comp. stat. §§ 530/1; Indiana (applies only to state agencies) , Ind. Code §§ 4–1-10–1; Louisiana, La Rev. Stat. Ann §§ 51:3071; Maine, Me. Rev. Stat. Ann. tit. 10, §§ 1346; Minnesota, Minn. Stat. §§ 325E.61; Montana, Mont. Code Ann. §§ 30–14-1701 et seq.; § 33–19-321; Nevada, Nev. Rev. Stat. §§ 603A.010; New Jersey, N.J. Rev. Stat. §§ 56:8–161; New York, N.Y. Gen. Bus. Law § 899-aa; North Carolina, N.C. Gen Stat., § 75–65(a); North Dakota, N.D. Cent. Code § 51–30-02; Ohio, Ohio Rev. Code § 1349.19(B)(1); Pennsylvania, Pa. Cons. Stat. § 3(a); Rhode Island, R.I. Gen. Laws § 11–49.2–7(a); Tennessee, Tenn. Code. Ann. §§ 47–18-2107; Texas, Tex. Bus. & Com. Code § 48.103(b); Washington, Wash. Rev. Code § 19.255.010.

70. 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).

71. 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.

72. 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).

73. 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)).

74. See California Civil Code § 1798.81 et seq. "Personal information" excludes information if both the name and the other data elements are either encrypted or redacted; and publicly available information that is lawfully made available to the general public from federal, state, or local government records.

75. See California Civil Code §§ 1798.82 and 1798.29.

76. These states include: Connecticut, Delaware, Florida, Georgia, Illinois, Minnesota, Nevada, New Jersey, New York, Ohio and Texas.

77. Section 625 of the FCRA generally provides that nothing in the FCRA shall exempt persons from complying with any state laws regarding the collection, distribution or use of any information on consumers, or for the prevention or mitigation of identity theft except to the extent of any inconsistency with the FCRA. However, the FCRA carves out specific exceptions to this general rule, including with respect to truncation of credit and debit card numbers. Specifically, section 625(b)(5)(a) of the FCRA provides that "no requirement or prohibition may be imposed under the laws of any State" with respect to the requirement to truncate credit and debit card numbers and eliminate expiration dates from receipts issued to cardholders (emphasis added). Operators of retail websites should also bear in mind that VISA and MasterCard have issued requirements to all licensed merchants that not more than the last four (4) digits of the consumer's account number be displayed on a receipt. Effective July 1, 2003, for all new terminals, Visa USA mandates that all but the last four (4) digits of the cardholder account number and the entire expiration date, be suppressed on the cardholder copy of all transaction receipts generated from electronic (including cardholder-activated) terminals. Effective April 1, 2005 MasterCard requires all cardholder receipts generated by newly installed, replaced, or relocated ATM and point-of-interaction (POI) terminals, whether attended or unattended, must reflect only the last four digits of the primary account number (PAN). Fill characters that are neither blank spaces nor numeric characters, such as X, *, or #, must replace all preceding digits.

78. See, e.g. Michigan Stats. § 445.81 et seq. and California Civil Code §§ 1798.85–1798.86.

79. A 2001 article explored the details of how franchisors and franchise systems most effectively use the Internet. See L. Plave and K. Miller, International Franchising & E-Commerce: Adapting Franchise Systems

to the Global Electronic Marketplace, 3 J. Franchising and Distrib. L., 4, at 259 (2001).

80. 203 F. Supp. 2d 905 (N.D. Ill. 2002).

81. ChoiceParts, 203 F. Supp. 2d at 924–25.

82. 264 F.3d 493 (5th Cir. 2001).

83. No. 00–1324-PHX-PGR (D. Ariz. 2001),

84. State Auto Dealer Regulation: One Man's Preliminary View, available at http://www.ftc.gov/speeches/leary/learystateautodealer.htm (May 8, 2001).

85. U.S. Const., Art. I, Sec. 8, cl. 3.

86. Federal Trade Commission, Agenda for Public Workshop on Possible Anticompetitive Efforts to Restrict Competition on the Internet (Sept. 30, 2002) (available at http://www.ftc.gov/opa/2002/09/ecomagenda.htm).

87. These practices potentially violate the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301, 353(b)(1).

88. See Press Release, U.S. Drug Enforcement Administration (U.S. Justice Department), International Internet Drug Ring Shattered: E-Traffickers Arrested: Indian/Costa Rican/Canadian Cyber Criminal Alliances Shut Down (April 20, 2005) (available at http://www.usdoj.gov/dea/pubs/pressrel/pr042005.html).

89. See, e.g., The Controlled Substances Act, 21 U.S.C. §§ 822, 829, 841, 958.

90. See, e.g., The United Nations Convention Against Illicit Traffic in Narcotics and Psychotropic Substances of 1988 (available at http://www.unodc.org/pdf/convention_1988_en.pdf).

91. In September 2000, the Federal Trade Commission conducted a Public Workshop on the subject of Health Care and Competition Law and Policy. See generally http://www.ftc.gov/ogc/healthcare/index.htm. This was neither the first nor the last such effort. See, e.g., U.S. Dep't of Health & Human Services, Telemedicine Report to Congress 2001 (available at http://telehealth.hrsa.gov/pubs/report2001/2001repo.pdf).

92. The Federal Wire Wager Act, 18 U.S.C. § 1084.

93. 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).

94. See Press Release, U.S. Attorney for the Southern District of New York, Jay Cohen Convicted of Operating an Off-Shore Sports Betting Business that Accepted Bets from Americans Over the Internet, (Feb. 28, 2000), at http://www.usdoj.gov/criminal/cybercrime/cohen.htm.

95. See Matt Richtel, Wall St. Bets on Gambling on the Web, The New York Times, Dec. 25, 2005, at A1.

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

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

98. 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.

99. 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.

100. 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).

101. Chemical Waste Management, Inc. v. Hunt, 504 U.S. 334, 339–40 (1992) (internal quotations and citations deleted).

102. Baldwin v. G.A.F. Seeling, Inc., 294 U.S. 511, 527 (1935).

103. In relevant part, the Twenty-first Amendment provides that: "[t]he transportation or importation into any State, Territory, or possession of the United States for delivery or use therein of intoxicating liquors, in violation of the laws thereof, is hereby prohibited." U.S. Const. amend. XXI, § 2.

104. 125 S. Ct. 1885, at 1905.

105. Id. (emphasis omitted).

106. Id. at 1905–06.

107. 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.

108. 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).

109. 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."

110. 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).

111. See, e.g., Poly-America, L.P. v. Shrink Wrap Int'l, Inc., 2004 U.S. Dist. LEXIS 7875 (N.D. Tex. Apr. 23, 2004) (the only interactive feature on the defendant's website allowed a user to send an e-mail to the operator; that was deemed insufficient to support a finding of personal jurisdiction).

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

113. 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 defendants but indicated that in the event the French defendants seek to enforce their judgment in the United States, the Constitutional issues raised in the district court could be dispositive), rev'd en banc, 2006 U.S. App. LEXIS 668 (9th Cir. Jan. 12, 2006) (in an unusual decision, the appellate court dismissed the case, inter alia, for lack of ripeness but a majority of the en banc panel found that there was personal jurisdiction over the French parties because there were three contacts with California: (1) they sent a cease and desist letter to Yahoo!; (2) they served process on Yahoo! to commence the French lawsuit; and (3) they served two interim court orders on Yahoo!). Id. at pp. 6–8.

114. Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 454 (3d Cir. 2003). See also Jennings v. AC Hydraulics A/S, 383 F.3d 546 (7th Cir. 2004); Lakin v. Prudential Securities, Inc., 348 F.3d 704 (8th Cir. 2003) (adopting modified Zippo standard); 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); Revell v. Lidov, 317 F.3d 467 (5th Cir. 2002) (adopting Zippo standard); 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); Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997); 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 at *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).

115. Cole-Tuve, Inc. v. Am. Mach. Tools Corp., 342 F. Supp.2d 362 (D. Md. 2004).

116. Id at 366.

117. Id. at 366, 368.

118. Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d at 454.

119. 96 F. Supp. 2d 284 (N.D. Ill. 2000).

120. 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 Electronic Commerce & 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. A contrary result was reached in a U.S. court, in Realuyo v. Villa Abrille, 2003 U.S. Dist. LEXIS 11529 (S.D.N.Y. July 8, 2003), aff'd, 2004 U.S. App. LEXIS 5771 (2d Cir. Mar. 29, 2004), in which the court refused to exercise jurisdiction over the defendant in a defamation suit against a Philippine news service, where the "sheer availability of the article on [the defendant's] website, where

it can be downloaded in New York at no cost'' was deemed insufficient to sustain jurisdiction.

121. 194 A.L.R. 433 at ¶ 44 (emphasis added).

122. 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).

123. See Green Tree Financial Corp. v. Bazzle, 123 S. Ct. 2402 (2003).

124. 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.

125. 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).

126. See Discover Bank v. The Superior Court of Los Angeles County, 105 Cal. App. 4th 326 (Cal. Ct. App., 2d Dist., Jan. 14, 2003).

127. 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 Caspi v. The Microsoft Network, 323 N. J. Super. 118, 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999).

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

129. Stomp, Inc. v. Neat O, LLC, 61 F. Supp.2d 1074, 1080–81 (C.D. Cal. 1999).

130. For example in Quebec v. Products Metalliques CMP, Province of Quebec, District of Beauharnois, Localite de Salaberry-de-Valleyfield, No. 760–61-031078–026, Dec. 8, 2004, the Court of Quebec ruled that Quebec-based company violated the provincial Charter of the French Language by failing to provide a French version of just a portion of its website, even though the company claimed that 80–90% of its customers transacted business in English. The company was fined Cdn$500.

131. See In re Bristol-Myers Squibb Securities Litigation, 205 F.R.D. 437, 2002 U.S. Dist. LEXIS 13808 (D.N.J. Feb. 4, 2002).

132. 15 U.S.C. § 7001, et seq. Most of the provisions of E-SIGN took effect on October 1, 2000.

133. In June 2001, the FTC and Commerce Department issued a report to the Congress, as required under Section 105(b) of E-SIGN. 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.'' See, , 15 U.S.C. § 7001(c). If a law or statute requires that information relating to a transaction be made available to a consumer in writing, then certain requirements must be satisfied in order for the electronic record to be considered sufficient to meet the ''written'' requirement. The requirements of Section 7001(c) consist of the following:

1. That the consumer affirmatively consented to the use of electronic records, and has not withdrawn that consent;
2. Prior to consenting, the consumer has been provided with a clear and conspicuous statement:
   (a) informing the consumer of:
      (i) any right to have a paper record; and
      (ii) the right to withdraw consent to use electronic records and any conditions, consequences of such a withdrawal;
   (b) informing the consumer of whether consent applies:
      (i) only to the particular transaction; or
      (ii) identified categories of records;
   (c) describing procedures that the consumer may use to withdraw consent and update his or her contact information; and
   (d) informing the consumer:
      (i) how, after consent, consumer may request and obtain paper copy of electronic record; and
      (ii) whether fee will be charged;
3. The consumer:
   (a) is provided with statement of hardware and software requirements for access to and retention of electronic records, prior to consenting;
   (b) consents electronically, or confirms consent electronically, in a manner that reasonably demonstrates that consumer can access information in the electronic form that will be used to provide the information subject to consent; and
4. After receiving the consent of the consumer, if there is a change in the hardware and software requirements for access to and retention of electronic records that creates material risk that consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the party providing and relying on the electronic record:
   (a) provides the consumer with statement of:
      (i) revised hardware and software requirements for access to and retention of electronic records; and

(ii) right to withdraw consent without imposition of fees or consequences; and

(b) again complies with the requirements set forth in Item (3) above.

134. 15 U.S.C. § 7006(5) (emphasis added).

135. See, e.g., 15 U.S.C. § 7001(b)(2).

136. 15 U.S.C. § 7002(a).

137. 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.

138. 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).

139. 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 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).

Lee Plave and Inna Tsimerman

Lee Plave is a partner in the Washington, D.C. and Northern Virginia office of DLA Piper Rudnick Gray Cary US LLP. Inna Tsimerman is corporate counsel with CS STARS, LLC, an MMC company, CS STARS' Chicago, Illinois office.

Volume 4 2006 Issue 2

INTERNATIONAL JOURNAL OF FRANCHISING LAW

Edited by Martin Mendelsohn

RICHMOND