

This article first appeared in Business Law International, January 2002 (Issue 1), co-published by the International Bar Association, Sweet & Maxwell and the West Group. Lapointe Rosenstein would like to thank the International Bar Association, Sweet & Maxwell and the West Group for their consent to the posting of this article on this website.

The continuing impact of the internet on international franchising¹

Bruno Floriani & Michael K. Lindsey

I. Introduction

As the internet becomes progressively more ubiquitous in people's lives,² it is having impacts throughout society and business. This is increasingly true in the world of franchising, which was initially lukewarm to the internet but has rapidly turned to it as a means of facilitating business. A shift of this nature and magnitude necessarily causes a rethinking of franchisor strategy, from the territorial protections granted to franchisees to the ways in which franchisor trademarks are used.

The internet is also causing a rethinking of the law, its substance and its application. Traditional legal concepts are being applied to a medium never contemplated at the time of their establishment, and new laws are being adopted at a dizzying pace.³ Franchisors venturing onto the internet must be aware of these laws and how profoundly their operations can be affected by them. This paper will survey some of the areas of greatest concern to franchising generated by this new digital age.

II. E-commerce strategies for franchise systems

A. Background

Most businesses today have had some experience with or exposure to the world of the internet. While the business community has traveled some distance from the boundless enthusiasm of the first pioneers who embraced online business activities to the more sober approach prevailing today, the internet as a business medium remains in a fairly early stage of development. However, planning for the long-term success of most businesses today requires the development and implementation of some e-commerce strategy to expand, or even simply maintain, market share.

While developing and implementing a successful e-commerce strategy remains challenging, the failures of those e-commerce pioneers have been the source of some important lessons. Perhaps the most important of these lessons is that very few

¹ The authors gratefully acknowledge the contributions of Melissa DeVita, an associate with Paul, Hastings, Janofsky & Walker LLP in Los Angeles, in the preparation of this paper.

² America Online members are averaging almost 70 minutes on the service daily. Wired News Report, "Monster Sues Former Prez", <http://www.wired.com/news/business/0.1367.42288.00.html> (March 8, 2001).

³ In California alone, 85 bills related to or referencing the internet were reported to have been introduced in the first three months of 2001–2002 legislative session, and 258 internet-related bills reported to have been introduced in the last legislative session, compared to five in 1994. See <http://www.leginfo.ca.gov/cgi-bin/postquery> (visited March 23, 2001). See also Hallye Jordan, "California Lawmakers Take On Net", Silicon Valley News, <http://www.mercurycenter.com/svtech/front/docs/state081100.htm> (visited August 10, 2000).

businesses will thrive solely in the online universe, and that a successful “bricks and mortars” component is invaluable. Conversely, most businesses have come to realize that a successful “bricks and mortars” business must have a presence in the online universe to maintain its success in the future. In this context, the customer is king; the customer wants to be able to blend online and real world activities, such as browsing online for comparison purposes, ordering online but taking delivery at a physical store, or even ordering online at a physical store whose inventory of a particular product may be exhausted.⁴

Franchise systems with their multiple retail outlets are particularly well-suited to reap the benefits of a structured e-commerce strategy which builds on the brand name online and leverages its physical stores to reach its online customers.

As a result of evolving market needs, franchisors have been pressed by their franchisees and customers to embrace e-commerce and other uses of the internet. The fear that failure to take timely advantage of the internet and its e-commerce opportunities will result in competitors eroding their market share has caused many franchisors to hastily and haphazardly develop an online presence without properly considering the ramifications and evaluating whether such strategy is best suited to the needs and potential of their franchise system.

On the other hand many franchisees view e-commerce activities conducted by franchisors as an attempt to “cannibalize” their revenues. In order to alleviate franchisee concerns, the old arguments once raised by franchisors as justification for not granting exclusive territories for physical locations are being rehashed; for example, the nearby presence of a store from the same franchise system is far less economically threatening than one from a competing chain. These types of arguments have rarely convinced franchisees, though. Accordingly, e-commerce activities undertaken by franchisors often create competitive concerns within franchise systems which can lead to unanticipated legal and business consequences.

The degree of friction likely to arise from competing interests within a franchise system will depend on the type of use being made of the internet by the franchisor. When the franchisor establishes a web site solely for marketing and promotional activities, which is not enabled to make sales, very little tension is created; however, few benefits may be expected from such a static use of the internet.

Any e-commerce strategy which goes beyond this basic model will necessarily require an examination of the contractual rights of franchisors and their franchisees, as well as any applicable law on this issue. This crucial examination is a necessary starting point in the development of any e-commerce strategy by a franchisor, as it will directly impact upon the nature and scope of the franchisor’s permitted e-commerce activities.

The flip side of the coin is whether the franchisees of a franchise system may themselves develop an e-commerce strategy independently of their franchisor. Once again, this will require a critical review of the contractual rights of the franchisor and its franchisees, as well as applicable legislation, in order to identify the extent and scope of the franchisees’ right to implement an e-commerce strategy. Once this preliminary analysis has been completed, the franchisor will be in a position to establish systemwide policies for use of

⁴ Some chains with smaller stores could allow customers to order online products not carried in stock by local stores and pick them up at the local store the next day. Another example would be HMV, which has given its customers the ability to order hard-to-find music at its web-based kiosks in its Canadian stores.

the internet by its franchisees. The various approaches which may be considered by a franchisor can be generally grouped in the following three broad categories:

- (a) allowing franchisees to use the internet and develop their own independent e-commerce strategy without restriction;
- (b) some regulation of the franchisees' use of the internet or e-commerce as a new advertising medium, subject to the usual rules regarding prior approval of materials used in advertisements and perhaps specific policies regarding internet use in the operations manual; or
- (c) an absolute prohibition against franchisees using the franchised marks as part of any internet or e-commerce activities.

As we will see, the choice of any of the foregoing policy approaches will be dependent upon the interaction, in any given franchise system, between the franchisor's own e-commerce strategy, existing contractual rights which may be enforced by the franchisor or its franchisees and the existing legislative framework in the country or other jurisdiction in which franchises have been or will be granted by the franchisor.

B. Impact of Existing Environment on the Development of an E-Commerce Strategy For a Franchise System

1. Limits on a Franchisor's Use of the Internet or Development of an E-Commerce Strategy

The first area of concern should be the existing franchise agreements: Do they place any contractual limitations on the nature and scope of a franchisor's use of the internet or the development of its e-commerce strategy?

As one might expect for any franchise system that is more than a few years old, the franchise agreement will in all likelihood not specifically address internet use; this is not surprising given that the particular conditions for widespread e-commerce activities (e.g. extent of consumer use of the internet, the cost of implementing e-commerce activities, security issues, etc.) have only materialized in the last few years. The absence of specific references to internet use in a franchise agreement will require a close examination of the grant provisions and the exclusivity provisions, if any, in order to determine the extent of a franchisor's contractual rights.

If no exclusivity was granted to the franchisee for a particular territory, market or distribution channel, it is likely that the franchisor would not face any purely contractual restrictions in its use of the internet and development of its e-commerce strategy. However, as noted below,⁵ this does not paint a complete picture of the situation: courts in the U.S. and elsewhere have not hesitated to examine encroachment issues in light of broadly stated extra-contractual duties that may arise in the context of a franchise relationship. If the existing franchise agreement does contain a grant of exclusivity, regardless of its nature, it will be necessary to identify the scope of such exclusivity. It is not unusual for franchise agreements which contain some sort of exclusive grant to the franchisee also to reserve to the franchisor or its affiliates certain rights intended to reduce the scope of the exclusive rights so granted. For example, the franchisor may reserve the right to sell the same products or provide the same services as its franchisee,

⁵ See text accompanying notes 6–8 below.

in the exclusive territory reserved to the franchisee, using different trademarks or a different distribution channel (e.g. wholesale vs. retail, catalogue vs. store, specialized distribution through franchised outlets vs. mass distribution through department stores, grocery stores, etc.).

Very few exclusivity provisions are drafted so broadly as to prevent a franchisor from developing a “brochure” type of web site, simply advertising products and services but not enabled to make any online sales. Accordingly, the development and implementation of this type of web site by a franchisor would likely not be problematic but, as we will see, may produce little by way of rewards and benefits.

The fundamental question is whether the franchisor can conduct online sales and other e-commerce activities on its web site without encroachment claims from its franchisees and without violating applicable legislation. In order to answer this question, the exact wording of such exclusivity provisions and reservations in favor of the franchisor must be closely examined, together with a review of the existing legislation and case law in relevant jurisdictions. In the United States, and more recently in Canada, courts have shown a remarkable willingness to frame the encroachment issue as a potential breach of the duty of good faith and fair dealing owed by a franchisor to its franchisees, even where the franchise agreement contains provisions reserving rights in favor of the franchisor which would have been considered sufficiently explicit just a few years ago. In two often cited cases⁶ in an off-line context, the courts have entertained claims that franchisors breached the implied covenant of good faith and fair dealing by engaging in activities that might affect franchisees’ revenues, including in circumstances where the agreement contained, in one case, an express reservation for the franchisor to sell, or license others to sell, products under the franchised marks or otherwise through the same or similar delivery systems or other distribution channels and, in the other case, no exclusive territory at all.

In an online context, a United States court went so far as to state that given the parties’ awareness of the internet as a world-wide medium, the burden of negotiating and framing an exception to the license rights should fall on the licensor.⁷ This particular case may be distinguishable in that the licensee was in fact expressly licensed to operate a web site in this case, but it nevertheless highlights the every increasing risks of developing an e-commerce strategy which ignores franchisees.

More recently, certain Drug Emporium franchisees obtained a preliminary injunction from an arbitration panel of the American Arbitration Association⁸ enjoining their franchisor from conducting online sales to customers in their territory. In the Drug Emporium case, the franchisor established a subsidiary which began selling products on the internet within the franchisees’ exclusive territories. The franchisees claimed that the franchise agreement prohibited the franchisor from building any stores within the exclusive territory and that the web site of the franchisor’s subsidiary constituted an “online store” within the territory. The franchisor claimed that the web site did not constitute a store but rather an alternative means of distribution, and also argued that the franchise agreements did not preclude the franchisor from exploiting its own mark on the internet as this was

⁶ *Carvel Corporation v. Baker*, U.S. Dist. LEXIS 17609 (D. Conn. 1997) and *Bus Franchise Guide (CCH)* para. 11.208 (D. Conn. 1997); *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corp., et al.*, 139 F.3d 1396 (11th Cir. 1998) and *Bus. Franchise Guide (CCH)* para. 11.393.

⁷ *Hard Rock Café International, Inc. v. Morton*, 1999 WL 717995 (S.D.N.Y. September 9, 1999)

⁸ *Emporium Drug Mart, Inc. of Shreveport, et al., v. Drug Emporium, Inc. and DrugEmporium.com, Inc.*, September 2, 2000, American Arbitration Association, Dallas, a copy of which may be found online at <http://www.juriscom.net/txt/jurisus/ce/aaa20000902.htm>.

never contemplated when the franchise agreements were signed. Nevertheless, the arbitration panel decided in favor of the franchisees, citing the franchisor's statements on the web site to the effect that it was a "full service online drugstore" and "your neighborhood pharmacy for 20 years" and the franchisor's reference to the web site as a "drugstore" in its filings with the Securities and Exchange Commission. Interestingly, the panel noted that the web site tried to build market share by offering the same products at prices vastly undercutting the franchisees' prices at their physical stores. One could try to marginalize this decision as being rendered in the context of a motion for a preliminary injunction, rather than in the context of a full evidentiary hearing, or as a result of the fact that arbitration decisions are not official precedents followed by the courts, but this decision clearly demonstrates the need for a critical review of the franchisor's and franchisees' respective contractual rights.⁹

What about in other countries? While the case law on this issue is often scarce in other jurisdictions, the few existing court decisions would also suggest that franchisors adopt a prudent approach. In the Province of Quebec, for example, the Court of Appeals found a franchisor in breach of the franchise agreement for opening and operating, in its franchisee's exclusive territory, large surface grocery/department stores which offered products at lower prices and benefited from a better promotional environment than the same products offered by its franchisee in its franchised grocery store.¹⁰ The Court cited the franchisor's obligation of good faith and loyalty towards its franchisees—the franchisor had a duty, in light of competitors opening large surface grocery/department stores, to act in concert with its franchisee so as to minimize the impact of this competition, and could not ignore its franchisees by itself operating the same types of businesses ostensibly to protect the franchise system's market share.

The decision of an Australian court in the case of *Dymocks Holding Pty Ltd v. Top Ryde Booksellers Pty Ltd*¹¹ dealt with a slightly different issue, but also constitutes cause for concern. In this case, Dymocks launched a systemwide web site with its franchisees' participation and written consent, using monies from the advertising funds for such purposes. Letters were exchanged with its franchisees confirming that the web site would be owned by the ad fund. The web site was originally intended to promote new releases and books of the month, with a view to encouraging surfers to buy these books at franchised bookstores whose locations were disclosed on the web site. Unfortunately, the promoted book was often unavailable at the local franchised bookstore and the fallback was that the book could then be bought directly from the franchisor. Having suffered significant losses in the operation of the web site, Dymocks told its franchisees it would take back the ownership of, and itself operate, the web site (including making sales from such web site) and reimburse to franchisees all expenses to date, provided they agreed in writing that they would abandon all claims to the web site. A number of franchisees objected. The court decided that the franchisor could take back the web site but was bound to put the objecting franchisees in the same financial position as they would have been if the original arrangement had been carried out. The court found that the objecting franchisees had suffered and would continue to suffer loss through Dymocks' failure to comply with the original arrangement, firstly through the loss of a prospective

⁹ Another interesting pending case to watch is the suit filed by franchisees of H&R Block in Missouri [No. 99-206379 (Circuit Court of Jackson County Mo., filed April 13, 1999)] in an attempt to have the court prevent their franchisor from offering online tax preparation services, alleging infringement of the protected territories of such franchisees in breach of their franchise agreement.

¹⁰ *Provigo Distribution Inc. v. Supermarché A.R.G. Inc.*, (1998) R.J.Q. 47 (Court of Appeals of Quebec).

¹¹ Supreme Court of New South Wales, Australia (May 15, 2000).

benefit to the advertising fund, and secondly and more importantly, the substantial chance that the objecting franchisees' business would be damaged through unrestrained competition from the Dymocks web site.

In light of the foregoing, it would seem that unless the reservation of rights in favor of the franchisor is explicitly worded, specifically addressing online sales and other e-commerce activities conducted by the franchisor, there is a substantial risk that franchisees would have some sort of legal claim to assert against their franchisor. Even then, as the *Dymocks* case demonstrates, courts may be willing to entertain franchise encroachment claims arising out of the operation of a franchisor-controlled web site.

In recognition of these risks and concerns, some franchisors might resign themselves to adopting an e-commerce strategy only involving online sales in territories not exclusively reserved to any of their franchisees. While this approach is prudent, the practical difficulties may be insurmountable. For example, most exclusive territories consist of a radius around the franchised outlet: firstly, it may be difficult to identify where the customer making the purchase on the Internet is physically located. Even if the customer is asked for an address, how easy will it be to determine whether the customer is located within a particular radius? Secondly, and perhaps more fundamentally, where is the sale made? Some would argue that it is made at the business address where the franchisor's employee accepting the internet order is located, others would claim that it is made at the location of the franchisor's internet server (which is usually located at the premises of franchisor's internet service provider), while others would insist that the sale is made at the customer's location when the internet purchase is made or at the customer's billing or shipping address. These issues have not been resolved by the courts or laws of most jurisdictions and, accordingly, a franchisee who feels he has been wronged in this respect may attempt to make an encroachment claim on the foregoing basis and would likely be able to find case law, with online or offline fact patterns, that would support its claim in at least some respects.¹²

2. Limits on a Franchisee's Use of the Internet or Development of an E-Commerce Strategy

In order fully to understand the parties' respective rights, it is also important to examine whether the franchisor may limit its franchisees' use of the internet and their ability to develop an e-commerce strategy, whether contractually or otherwise through use of applicable law or principles formulated by case law.

Based on the premise that most franchise agreements are vague or ambiguous as to internet use, most franchisors would generally attempt to extend the typical controls and restrictions found in franchise agreements with respect to other facets of the operation of the franchised business by the franchisee. These would include, by way of example, the provisions relating to the grant of the franchise, the usual restrictions on use of the franchised marks, the supervision and control over advertising and promotional activities by franchisees, and the franchisor's ability to modify and add to its operations manual.

A franchisor could claim that the grant provisions limit the license to use the franchised marks and system to the operation of the franchised outlet at or from a particular location. However, this raises the same ambiguities as were mentioned earlier in this paper, namely that the franchisee may place the server at its franchised outlet location

¹² Some of the better known cases are *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*, 939 F. Supp. 1032 (S.D.N.Y. 1996); *Irvine v. Murad Skid Research Laboratories*, Bus. Franchise Guide (CCH) para. 11.727 (1st Cir. 1999); *Jeri-Jo Knitwear, Inc. v. Club Italia, Inc.*, 94 F. Supp. 2d 457 (S.D.N.Y. 2000).

and respond that the online business is being conducted at or from the physical location of the franchised outlet. Given that these issues remain unresolved, it may be prudent to rely instead upon other types of restrictions in connection with the use of the franchised marks, advertising restrictions and implementation of system-wide policies through changes to the operation manuals.

Despite the fact that there may be some creative ways in which to control or limit the franchisees' rights to operate web sites and develop their own e-commerce strategy, some franchisors have been slow to react, partly because of the inherent uncertainties posed by the development of an effective e-commerce strategy and partly because of the perceived costs of implementing such a strategy. With hindsight, this has not always been the most prudent course of action. All that would be needed is for a few franchisees to establish their own web sites to convince most franchisors of the adverse effect on brand uniformity and client frustration at their inability to find the franchisor in the clutter of search results which identify each franchisee's web site as often as the franchisor's web site.

At the opposite end of the spectrum, some franchisors may wish to include an absolute prohibition against their franchisees having an online presence. In our view, this is also unwise, as it could easily be viewed as a failure to keep up with new business methods and consumer trends, thereby creating unrest in the franchise system as well as a sense that the franchise system may be unable to respond to changing market realities.

Quite apart from these business or practical considerations, franchisors may not be legally entitled to impose an absolute restriction against establishment of web sites by franchisees. Europe is a case in point. Firstly, the few decisions on this issue sent mixed signals: the initial decision in the *Fabre* case¹³ prevented a cosmetics company from prohibiting its distributor from selling cosmetics through the Internet from its retail location, based on the reasoning that in the absence of an express reference in the distribution agreement to online distribution of the products, the distributor was free to use the Internet just another means of distributing the products.

However, the court of appeal reversed this decision,¹⁴ holding that internet sales by the distributor were prejudicial to the network of distributors and devalued the image of the marks in general. Its reasoning was not very reassuring to franchisors, though, given that it was based on the fact that the distribution agreement required that these products be sold under certain specific conditions, namely subject to certain technical and health and safety standards, in a physically distinct area of the distributor's store complying with certain specifications and which was to be sufficiently spacious to highlight the various types of *Fabre* products in the best possible conditions from both the aesthetic and informative points of view. The agreement also required that a pharmacist be available to respond to any customer questions at the point of sale. The court of appeal concluded that the sales made by the distributor through the Internet did not satisfy these conditions, but clearly stated that, in the future, it may be possible that internet sales would satisfy these types of conditions. Franchisors are thus left with a seemingly favorable decision which is, however, particularly suited to being distinguished unless the franchise agreement contains express contractual conditions or restrictions concerning the sale of products which are not factually met through online sales.

¹³ *Société P. F. Dermo-Cosmétiques c/ Alain B*, Tribunal de Commerce de Pontoise (Ordonnance de Référé, April 15, 1999), the full text of which may be found online at <http://www.juriscom.net/txt/jurisfr/ce/tcpontoise19990415.htm>.

¹⁴ *Société P. F. Dermo-Cosmétiques c/ Alain B*, Cour d'Appel de Versailles (2 décembre 1999), the full text of which may be found online at <http://www.juriscom.net/txt/jurisfr/ce/caversailles19991202.htm>.

Regardless of the existing case law, the new Block Exemption Vertical Restraints (Regulation EC 2790/1999), which has replaced the Franchise Block Exemption on June 1, 2001 and is being phased in through transitional provisions until December 31, 2001, seems to close the door in this respect. Under the current draft guidelines of the new Block Exemption for Vertical Restraints, the European Commission D.G.I.V. considers sales via the Internet to be passive sales unless the web site is specifically targeted at a given area or customer group. As a result, franchisees must not be restricted from having their own web site as this would amount to a restriction on passive sales contrary to Article 81 of the Treaty of Rome, which prohibits anything which has or may have the effect or preventing, restricting or distorting competition. This position ignores the potentially proactive nature of the Internet and would allow each franchisee to establish its own web site and advertise and sell products on such web site so long as it is not specifically targeted at a given geographical area or customer group. While much was made of the pressure placed on the European Commission to modify the guidelines so as to allow restrictions in franchise agreements that would require franchisees to have their own dedicated pages on a system-wide web site rather than having their own distinct web site, the Commission has not acted upon any such suggestions and it remains unlikely that this change will in fact be made.

In Canada, the franchise legislation in the Provinces of Ontario and Alberta does not currently contain any prohibition on restrictions that may be imposed by a franchisor on its franchisees in respect of their use of the Internet.

Assuming that a franchisor has either decided not to impose, or is legally prevented from imposing, an absolute prohibition on internet use by its franchisees, the franchisor may allow its franchisees to develop web sites for three general types of activities, namely: (i) strictly marketing and promotion activities (*i.e.* simply advertising products and services); (ii) activities facilitated by use of the Internet (including communication and exchange of information); and (iii) activities enabled by, or only possible through use of, the Internet (including online sales and other e-commerce activities). These activities are not mutually exclusive, but bring additional challenges for implementation as a result of the tension they create within a franchise system.

C. Various E-Commerce Strategies For a Franchise System

The types of internet use and e-commerce strategies that could be developed for a franchise system vary greatly in complexity, costs to implement and maintain, and potential rewards and benefits that may be extracted from their use. Some franchisors will choose a particular business model and immediately invest whatever time, resources and effort they can afford to implement that business model. Others will choose a gradual approach, adding functions and capabilities to the franchise system web site over time, as users get familiar and comfortable with the web site.

Certainly one of the things to be mindful of when developing an e-commerce strategy is whether there is a sufficient critical mass of users who will have immediate access and can begin use of the web site almost immediately. For example, franchisees may have to upgrade their computer systems in order to extract the most out of the franchise system web site; some may be reluctant to do so unless they can get a tangible sense of the benefits that can be derived from its use, while others may not have enough computer savvy to use it regularly. In the end, each franchise system must evaluate the best approach for developing and implementing its internet use and e-commerce strategy, taking into account the particular environment in which it is operating and whether it can

convince its franchisees, through use of contractual provisions or otherwise, of the necessity of making the necessary upgrades.

Our view is that the almost infinite variety of business models for internet use and e-commerce strategies for a franchise system can be regrouped to three broad categories: "brochure"-type web sites, intranets and extranets.

1. Brochure-Type Web sites

As the name implies, in this business model the web site is used simply as a brochure or catalogue to advertise the products and services offered by the franchise system. Other features may be added to make the online experience more interesting for customers, such as advertising specials, making coupons available through the Internet and highlighting other marketing and promotional initiatives.

This business model is the simplest and least costly to implement. In fact, when faced with franchisees clamoring for the franchise system to establish some type of presence on the Internet, the initial reflex of most franchisors is to develop and implement this type of web site. Hardly any tension is created with its franchisees, in that these web sites do not directly engage in e-commerce activities, such as selling products and services directly to the customers, but rather drive customers to the "bricks and mortars" franchised outlets operated by the franchisees.

Some franchisors initially implement a brochure or catalogue web site, but subsequently consider the possibility of making online sales through the franchise system web site. If the franchisor decides to ignore its franchisees in making such online sales, there will likely arise strong tensions within the franchise system, pitting the franchisor against its franchisees, with the commercial, and possibly legal, consequences we discussed earlier. Some franchisors have instead sought to include their franchisees in this business model. As mentioned earlier, the franchisor could refer the orders placed by customers to the nearest franchised outlet. An example of how this would be done is asking the customer his or her zip code or postal code at the time of placing of the order, and the customer then being offered the possibility of choosing from the limited number of franchised outlets which are closest to that zip code or postal code.

2. Intranets

Fundamentally, an intranet is the use of web-based internet technology for communication within a company, usually consisting of a secure web site available only to authorized users within the company with exclusive passwords. As such, an intranet is usually intended to facilitate or enable activities within employees of a single organization. However, this term is frequently used to describe web sites available to all members of a particular network, such as a franchise system, even though the members are unrelated companies in the same network. For the purposes of this paper, we will consider web sites available to all franchisees of a franchise system as intranets, rather than extranets.

Intranets are ideally suited for the franchise industry. As we will see, intranet technology provides franchise companies with the opportunity to significantly reduce costs and enhance communication among members of the network.

In the franchise context, there are fundamentally two type of relationships which may be enhanced through use of an intranet, namely the franchisor-franchisee relationship and the employer (whether franchisee or franchisor)-employee relationship.

a. Employer-Employee Relationship

An intranet can provide significant benefits to the employer-employee relationship. For example, an intranet would allow the employees of each franchisee or the franchisor to access employment policies and procedures that are applicable to its organization. It would allow the employer to change those policies and procedures online and advise their employees by e-mail to visit the web site when those changes are made.

An intranet would also permit franchisors and franchisees to conduct web-based training where appropriate. Some franchisors have also used their intranet to distribute newsletters and magazines electronically, keeping employees up to date on developments within the organization, including advancement opportunities.

There are many other uses that could be made of intranets in this regard, including timekeeping, the exercise of choices with respect to pensions and other benefits, etc. While it is beyond the scope of this paper to explore this facet of intranet use in great detail, the human resource component of intranets is often viewed as the one that could provide the most benefits and rewards within an organization on a short term basis.

b. Franchisor-Franchisee Relationship

Once again, an intranet may be used to enhance a franchisor-franchisee relationship in a significant manner, while at the same time reducing costs for the benefit of both franchisors and franchisees. The following are a few examples of the dynamic uses to which intranets may be put:

- *Directory*: In order to facilitate communications by franchisees among themselves, with the franchisor or with suppliers, the web site could contain a directory listing of the telephone number, e-mail and address of key contacts within all of such companies. An obvious advantage is the ability to update the directory at a minimal cost and advise all users by e-mail that changes have been made. The directory listing would be easy to search electronically and could allow franchisees to send an e-mail message to anyone listed in the directory.
- *General Distribution of Information*: An intranet could be used to distribute news, bulletins and any other general information of interest to franchisees. This would save the franchisor the costs of printing and mailing or faxing this information to the franchisees, as well as reduce the time it would otherwise have taken to communicate such information to franchisees.
- *System Documentation*: The intranet could contain all operating manuals, user manuals and other system documentation that would otherwise have to be printed and mailed or faxed to franchisees. Electronic storage of system documentation accessible through the web site offers several other significant advantages: easy updating, consistency of documentation available to all, and ease of searching which simplifies obtaining access to relevant information.
- *Reporting*: An intranet could allow franchisees to file with the franchisor online sales reports, royalty reports and other financial, operating and miscellaneous information required pursuant to the franchise agreement. The availability and transmission of sales, royalty, financial and operating reports in real time could be of significant benefit to franchisors.
- *Forums*: A bulletin board may be set up on the web site for franchisees to post questions, give and receive advice and share opportunities and information. Many

franchisees have found this to be a uniquely helpful function of an intranet, giving them the ability to benefit from experiences of other franchisees quickly and efficiently.

- *Training and Support*: Franchisors would be in a position to conduct training for their franchisees or their employees directly through the web site, post-training material and software as well as real-time support for technical or operational matters.
- *Chat Functions*: An intranet could contain “chat” functions which could be used by franchisees to communicate among themselves on topics of relevance while visiting the web site or by franchisors to give support to franchisees in real time as discussed earlier.
- *Software Distribution*: Franchisors could make available through the intranet software fixes, upgrades and new versions of software that is licensed or sublicensed to franchisees by the franchisor. These could be downloaded directly to the franchisees’ computers rather than sending out disks and hoping that the users will install them properly, if at all.

Obviously, each additional function added to the intranet enhances the franchisor-franchisee relationship and should reduce costs and time and effort expended for all involved.

3. Extranets

Essentially, an extranet is the use of web-based internet technology for communication among different companies or between companies and consumers. Typical e-commerce uses of web site extranets break down into two well-known broad categories, namely B2B (business-to-business) and B2C (business-to-consumers). Franchise-specific uses are also possible, such as delivering a UFOC or other disclosure information to potential franchisees.

a. B2B

B2B is used to describe a multitude of activities between companies. However, the single most effective use of B2B to date has been online procurement. In the franchise context, franchisees would be given the ability to order equipment, supplies or other items from the franchisor, when dealing with proprietary products using technology developed by the franchisor, or from third party preferred or approved vendors. This would be achieved through the use of electronic ordering forms and could allow for tracking of the order and making changes during the order and fulfillment process.

Online procurement could also take different forms, such as direct online ordering from a specific seller after viewing an online catalogue, an online marketplace where various sellers could offer the same products to the franchisees, exchanges of products among franchisees, etc. The extranet could also allow franchisees to capitalize on time-sensitive opportunities, such as product close-outs and excess merchandise announcements. As can be seen, extranets offer wonderful opportunities to reduce cost, increase sales and otherwise enhance the relationships in a franchise system.

Another possible use of extranets is to enhance the corporate profile of the franchise system with investors and the media. Web sites could provide press releases, web-casts, management profiles and access to the management team and product and service information. This would normally be done through public relation pages and investor relation pages located on the extranet.

b. B2C

Selling to consumers is perhaps the portion of an e-commerce strategy which is the most difficult to implement, in large part as a result of the tensions which are produced within the franchise system for the reasons discussed earlier in this paper.

There are an almost unlimited number of ways in which sales can be effected through the web site. Some franchisors could decide to make sales directly to customers, subject to the previously mentioned considerations. Other franchisors might decide to refer sales directly to franchisees. Still other franchisors could decide that they would prefer controlling the sales themselves, but pay a reverse royalty to their franchisees in respect of online sales. This reverse royalty could be paid to the franchisee whose franchised outlet is located the closest to the customer's billing or shipping address, or it could be paid into a general account to be later distributed among franchisees in some previously agreed proportion (e.g. based on the number of existing franchisees, or each franchisee's sales as a function of total sales by all franchisees, etc.).

Instead of online sales being made by the franchisor, the franchisor could instead require that franchisees have their own pages on the franchise system web site, or even a "micro-site" within the franchise system web site, from which to advertise particular specials, offer coupons and otherwise make sales to their customers.

Another interesting solution would be the creation of a separate entity for the sole purpose of operating the franchise system web site and conducting e-commerce activities. This entity would be controlled by the franchisor but could allow participation by franchisees in the equity or profits of such entity.

In addition, a higher degree of interactivity on the web site would allow customers to give feedback to franchisees and franchisors for the benefit of the entire franchise system and otherwise allow franchisees to cultivate a relationship with their customers by means other than those which are available conventionally, such as direct e-mail exchanges, real time support for franchisees selling technical products. etc.

As we have seen creative uses of the Internet and e-commerce could bring both high tension but incredible rewards for the members of a franchise system. A critical examination of the issues we have briefly addressed in this paper is essential in order to develop and implement internet use policies and e-commerce strategies that meet the expectations of the members of the franchise system and deliver rewards which will ultimately outweigh the costs of implementation and maintenance.

III. Brand protection and the internet

For any business—and particularly for franchise businesses—a brand is a form of shorthand used to convey the quality, consistency, reliability, service level and distribution style or technique associated with the business' product or service. Through this shorthand customers can sort through the overwhelming volume of information confronting them to pick the product or service that best suits their needs.

Unfortunately, the miraculous new medium of the Internet has proven to be a bruising battleground for brands. The owners of well-recognized brands have been forced to litigate or buy off "cybersquatters", profiteers who register identically worded, slightly changed or even intentionally misspelled domain names. Companies engaged in product development have been chagrined to find that, even before their products are released,

others have registered the product name selected and variations that were being considered. Even political candidates have found domain names registered to other, quicker actors.

The essential problem is that in e-commerce, trademarks and service marks serve as a navigation tool for users of the Internet. Internet users searching the web often type "<http://www.TRADEMARK.com>" in their browser in an attempt to find the TRADEMARK owner's web site. Other times users seeking the site will type "TRADEMARK" into an internet search engine and click on one of the sites resulting from the search. In many instances, however, users are transported to a site owned by someone other than the rightful trademark owner. This section surveys the many unwelcome techniques used to exploit the traffic-drawing power of brands on the Internet and the legal protections against them provided by U.S. and international laws.

A. Trademark Infringement

1. Statutory Background: U.S

The United States federal statutory scheme provides protection of trademarks by prohibiting "any reproduction, counterfeit, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive".¹⁵

The crucial issue under the U.S. statute is likelihood of confusion, determined by a balancing of seven factors: (a) the strength or distinctiveness of the marks; (b) the similarity of the two marks; (c) the similarity of the goods or services the marks identify; (d) the similarity of the marketing methods and channels of distribution used by the two parties; (e) types of good and the degree of care likely to be exercised by the purchaser; (f) the defendant's intent; and (g) evidence of actual confusion.¹⁶

2. Application of Statutory Standards: *Brookfield*

Given the "three dimensional" issues to be resolved in determining trademark infringement, questions arose as to application of these principles in the essentially "flat" universe of the Internet, where only one company can maintain a domain name registration for "TRADEMARK.com." One of the seminal cases to deal with these questions is *Brookfield Communications Inc. v. West Coast Entertainment Corp.*,¹⁷ in which the court found for the plaintiff in determining a likelihood of confusion by defendants' proposed use of its registered domain name. The plaintiff Brookfield Communications had started marketing entertainment industry software under the "MovieBuff" trademark in 1993, and subsequently began using that mark on an entertainment database and then registered the mark with the Patent and Trademark Office in 1998. The defendant West Coast operated 500 video rental stores under the service mark "The Movie Buff's Movie Store", for which it secured a federal service mark registration in 1991. West Coast also registered the domain name "moviebuff.com" in

¹⁵ Lanham Act, 15 U.S.C. § 1114(1).

¹⁶ See *Pizzeria Uno Corp. v. Temple*, 747 F.2d 1522, 1527 (4th Cir. 1984); *AMF, Inc. v. Sleekcraft Boats*, 599 F.2d 341, 348-49 (9th Cir. 1979).

¹⁷ 174 F.3d 1036 (9th Cir. 1999).

1996 but made no significant use of its web site until November 1998, when it announced that it intended to launch a searchable entertainment database at the site.

In response to Brookfield's request for injunctive relief on trademark infringement grounds, West Coast argued that it had priority, having used "The Movie Buff's Movie Store" since 1986. The Ninth Circuit found that "The Movie Buff's Movie Store" was sufficiently different from "moviebuff.com" such that the defendant could not tack its trademark priority onto use of its domain name. The court specifically noted that "registration with Network Solutions does not in itself constitute 'use' for purposes of acquiring trademark priority".

Accordingly, West Coast's first use of "moviebuff.com" was preceded by Brookfield's first use of "MovieBuff". West Coast's registration of the domain name and limited e-mail communications did not constitute first use; its first use was not until November 1998 when it publicly announced the imminent launch of its web site. Under a traditional trademark infringement analysis, the Ninth Circuit determined there existed a similarity between Plaintiff's mark and the domain name which, combined with the competitive overlap of Brookfield's software and West Coast's online database that could perform a similar function, created a likelihood of confusion if defendant West Coast was permitted to use its registered domain name. The court concluded that "the domain name is more than a mere address: like trademarks, second-level domain names communicate information as to source."

3. Limitations

Many U.S. cases decided to date have held that the mere use by a third party of a domain name which is identical or similar to a federally-registered trademark by itself may not constitute trademark infringement. For instance, in *Giacalone v. Network Solutions, Inc.*,¹⁸ the court found that plaintiff's domain name "ty.com" did not infringe on the defendant's registered trademark "ty". The Chicago-based toy manufacturer owned the "ty" registered trademark, but the "ty.com" domain name was held by a web page designer who had registered "ty.com" because his son's name is Ty. The trademark owner alleged trademark infringement, while the domain name owner alleged in its complaint a "reverse domain name hijacking". The court granted an injunction prohibiting the defendant toy manufacturer from interfering with the plaintiff's use of its domain name and ordering it to "take all steps necessary to see that Plaintiff's right to use the domain name 'ty.com' is undisturbed and not suspended or interfered with in any way".

In *CBS, Inc. v. The Network Network Company*,¹⁹ The Network Network (the "Network") sought declaratory judgment against CBS, alleging that Network's use of the Internet domain name "tnn.com" does not infringe any of CBS' rights, while CBS alleged dilution of its trademark. Plaintiff Network was formed in 1986 to provide consulting and training to information technology managers and professionals concerning the establishment and maintenance of computer networks, and registered the Internet domain name "tnn.com" on January 7, 1994. On January 20, 1987, Opryland USA, Inc. registered the service mark "TNN" with the Patent and Trademark Office. The mark is shorthand for "The Nashville Network" ("Nashville"), a wholly owned subsidiary of CBS, which is described in the opinion as a "cable television network that broadcasts country music and

¹⁸ 1996 WL 887734 (N.D. Cal. June 14, 1996).

¹⁹ 54 U.S.P.Q.2d 1150 (C.D. Cal. 2000).

country lifestyle programs". Nashville argued that the Network's choice of domain name had caused a substantial likelihood of confusion for Nashville viewers and customers.

The court concluded there was no genuine risk of confusion and that no infringement occurred because the products involved were not related. Further, there was no evidence Network sought "to trade on Nashville's good name". "There is a difference between inadvertently landing on a web site and being confused. Thousands of Internet users every day take a stab at what they think is the most likely domain name for a particular web site."

Expensive applications of U.S. trademark law are still found. Perhaps the most notorious such application was found in *Etoys, Inc. v. Etoy*,²⁰ in which a California state court issued an injunction in favor of the online toy retailer against the defendant Swiss online conceptual artists, restraining further use of the "etoy.com" domain name by defendant on trademark infringement, dilution and unfair competition grounds. After an international uproar, the case was settled in January 2000, permitting defendant's continued use of the "etoy.com" domain name. The final chapter in this saga was written in March 2001, when the plaintiff toy retailer ceased operations and filed for bankruptcy protection.

On the other hand, the general rule is that there are no intellectual property rights to a gTLD, and first use of a mark is not determinative. In *Image Online Design, Inc. v. CORE Association and Ken Stubbs*,²¹ the United States District Court for the Central District of California did not enjoin the defendants from using plaintiff's alleged service mark ".web" as a generic top level domain ("gTLD") for computer network addresses and in connection with domain name registry services. In *Image Online*, the plaintiff alleged that it had a common law trademark right in the service mark ".web." Plaintiff further alleged that the defendants had attempted to misappropriate the ".web" mark by using the mark for computer network addresses and domain name registry services in the so-called AlterNIC.

Plaintiff Image Online alleged that it provides computer network addressing and domain name registry services using ".web." Image Online also alleged that it offers other services, including registration of Internet domain names, in connection with the gTLD ".web." However, all domain name registration activities involving the gTLD .web are on a preregistration basis only. Furthermore, as ".web" is not a gTLD approved by any internet governed entity such as the Internet Corporation for Assigned Names and Numbers ("ICANN"), no domain names could yet be assigned within this gTLD. The court ruled against Image Online, finding it could not prevail on a trademark claim when it has no trademark rights in ".web", as web is generic and not protectable.

The Fourth Circuit Court of Appeals in *America Online, Inc. v. AT&T Corporation*,²² focused on the generic nature of the phrase "You Have Mail", and found it to be unprotectable as a trademark when used to alert internet users that they have received electronic mail.

On appeal from the lower court's grant of summary judgment in favor of AT&T's non-infringement with respect to the marks "Buddy List", "You Have Mail" and "IM", the Court of Appeals affirmed the ruling as to "You Have Mail" and "IM" based on the

²⁰ L.A.S.C. BC 216606 (1999).

²¹ 120 F. Supp. 2d 870 (C.D. Cal. 2000). Michael Lindsey and his firm are counsel of record for defendants CORE and Stubbs in this action.

²² 243 F.3d 812 (4th Cir. 2001).

functional use of the words with their ordinary meaning. The Court, however, concluded that whether “Buddy List” was generic could not be decided on summary judgment, and the district court did not give proper weight to the Patent and Trademark Office’s Certificate of Registration for the mark. The Court noted that “AOL’s use of the phrase [‘You Have Mail’], conditioned on whether the mail is present, does not describe AOL’s e-mail service, but rather simply informs subscribers, employing common words to express their commonly used meaning, of the ordinary fact that they have new electronic mail in their mailboxes”. This functional, generic use is not afforded trademark protection and, therefore, no infringement was found.

4. Recent Developments

In a follow-up decision to *Brookfield*, a U.S. District Court in Washington recently noted in *iCARumba, Inc. v. Inter-Industry Conference on Auto Collision Repair*,²³ that the critical question in determining whether there is a likelihood of confusion for an infringement claim under the Lanham Act is the similarity of the trademarks at issue. Defendant Inter-Industry Conference on Auto Collision Repair (“ICACR”), which has protectable rights in various “I-CAR” marks, sought to enjoin plaintiff iCARumba from using the trademarks “ICARUMBA”, “ICARUMBA DRIVING THE REVOLUTION IN CAR CARE”, and “ICARUMBA.COM”. ICACR uses the I-CAR trademarks in a searchable database of auto collision repair shops and related services available at www.i-car.com. iCARumba is in the business of providing online automotive information services and owns the domain name “icarumba.com”. The district court found that there was no likelihood of confusion between iCARumba’s marks and those of defendant, and, although both parties offer related services, the marks are sufficiently distinctive from one another that there is no great likelihood of confusion. Thus, ICACR’s request for an injunction was denied.

Middle ground is often found by the courts. In late December, 2000, the U.S. Ninth Circuit Court of Appeals, in *Nissan Motor Co. v. Nissan Computer Corp.*,²⁴ upheld a lower court’s grant of an injunction that allowed Nissan Computer Corp., a software developer, to keep the domain name “Nissan.com”, but required it to display a prominent disclaimer that the site is not connected with the car manufacturer and to cease running any automobile-related banner ads on its site. Further, the computer company must post the web site address for Nissan Motor Co. on the computer company’s web site so as to avoid any initial interest confusion of consumers who may visit the web site looking for Nissan cars.

Nissan Computer Corporation contended that it principally sells computers and Internet services, not cars, such that the defendant’s principal business is different from that of plaintiff. The court, however, noted that “this case is not suited to a traditional proximity-of-goods analysis. Starting in August 1999, the defendant’s nissan.com web site primarily promoted automobile-related products and services, through third-party advertisements and web links, rather than the defendant’s own computer products. More than 90 per cent of the defendant’s web site advertising revenue is automobile-related.” The appellate court based its decision on the finding that the computer company “altered its web site so as to capitalize on the ‘initial interest confusion’ of consumers who visited the web sites looking for plaintiffs’ products”. “Whether or not a visitor to the defendant’s web site ultimately makes an automobile purchase from an advertiser, the defendant

²³ 57 U.S.P.Q. 2d 1151 (2000).

²⁴ 246 F.3d 675 (9th Cir. 2000), Unpublished Disposition, 2000 WL 1875821 (9th Cir. 2000).

profits from the visitor's initial interest confusion." Such use of "bait and switch" tactics constitutes trademark infringement.

A New York District Court recently found in *Movado Group, Inc. v. Matagorda Ventures, Inc., et al.*, that listing the Movado Concord watch as an item for sale and including it in defendant's web site when defendant did not in fact offer the Concord for sale constituted infringement.²⁵ Movado complained that defendant, a non-authorized seller of Movado watches, operated a web site that listed for sale Movado Concord watches which it did not actually sell. The court opined that, "it seems patent that the only reason the Defendants would include on their web site the brand name of a watch they did not sell is to lure potential customers searching the Internet to their web site. Such action, analogous to the old fashioned 'bait and switch,' is deceptive and confusing as a matter of law."

In a decision that may broaden the scope of trademark owners' claims, a Pennsylvania district court has decided that trademark protection on the Internet may not be limited solely to a company's main field of business. The court decided that *Qwest Communications, Int'l v. Cyber-Quest, Inc.* may proceed because a company has a right to protect its trademark in markets other than its pertinent area of business.²⁶ Plaintiff Qwest is in the business of providing multimedia communications services and products to businesses and residential customers while Defendant Cyber-Quest is in the business of, among other things, providing telecommunications services and products as an information service provider and developer of internet application technology. Plaintiff first used the "Qwest" mark in 1981, and has used it continuously since 1985. The "Qwest" and "Qwest Communications" marks were registered by plaintiff in 1996. The court noted that a finding of competition of products is not necessary for infringement if there is a likelihood of confusion based on confusingly similar products or names. The court stated that "a consumer might suppose that Cyber-Quest is a new Internet services division of Qwest", and thus permitted the case to proceed.

In another decision showing that U.S. courts remain sensitive regarding the protection of marks from infringement, a federal court in California, upon remand by the 9th Circuit Court of Appeals, has enjoined Interstellar Starship Services ("ISS") from using "epix.com" to promote video image processing services, due to the similar nature of Epix Inc.'s business.²⁷ The court did so even though it did not find bad faith by ISS in its current use of the domain name or a likelihood the parties planned to cross-over into one another's line of business. Additionally, the court found the presence of at least eight other valid PTO registrations of "EPIX" or close variations thereof, which lessen the likelihood that consumers strongly associate the mark with defendant. The court noted that "[w]hile [Plaintiff] admitted he was aware that others would covet the name 'epix.com,' that awareness, by itself does not deprive [Plaintiff] of the right to put the name to his own legitimate use". Still, the Court found the past use by ISS of the web site did infringe defendant's trademark in connection with technical services and digital image processing. The Court therefore enjoined ISS from promoting video image processing services on the web site as it had done in the past, since such services are similar to those of EPIX Inc. The Court also went so far as to enjoin ISS from using gray wallpaper for its site, since Epix Inc.'s site uses gray wallpaper, and required a disclaimer notice on each page displaying the epix.com logo.

²⁵ 2000 WL 1855120 (S.D.N.Y., December 19, 2000).

²⁶ 124 F. Supp. 2d 297 (M.D. Pa. 2000).

²⁷ *Interstellar Starship Services v. EPIX Incorporated*, 125 F. Supp. 2d 1269 (Oregon, 2001).

In what may be the most expansive prohibition to date in a domain name lawsuit, a Wisconsin federal court decided on March 2, 2001, that Right Sports, Inc., owner of the domain name "ereferee.com", could not operate its web site or use the word "referee" in any domain name or other computer address.²⁸ Referee Magazine originally requested only that the court stop Right Sports from using its *existing* domain names with "referee" in them. The court's injunction, however, went further than the remedy originally sought by plaintiff to include all uses of the word "referee". Significantly, the parties participated in the ICANN Uniform Dispute Resolution process (UDRP, discussed at length in Section III. F. 4 below), which resulted in a decision in favor of Right Sports. The court ignored the UDRP decision and allowed the case to proceed, with a conclusion opposite to the arbitral result. The next step for U.S. lawmakers or courts will be to address how to deal with such inconsistencies with, and disregard for, the decision of international arbitral tribunals.

5. Recent International Developments

The U.S. is not the only country to apply traditional trademark infringement principles to Internet domain names. For example, a German court has required the owner of the domain name "Gnutella.de" to cease use of the site because of the potential damage it could cause to the image of the Italian producer of the food product Nutella by associating the Italian company with copyright pirates.²⁹ The owner of the domain name "gnutella.de" is Gnutella, a file-sharing service similar to Napster. The German court found Gnutella to have infringed Nutella's trademark by use of its domain name "gnutella.de" by its use of the domain name in connection with its file sharing service. In the wake of the decision, a separate third party owner of "Newtella.de" voluntarily agreed to take that site offline to avoid similar legal action by the Italian maker of Nutella.

Following is a sampling of the results of other non-U.S. trademark/domain name disputes:

Brazil has adopted a regulation that forbids registration of domain names that conflict with "well-known" or "reputed" trademarks by third parties to the extent the marks are used on identical or similar goods.³⁰ Despite this regulation, a Brazilian appeals court refused to restrain the use of "aol.com.br" by a Brazilian internet service provider because the U.S. internet giant AOL had not yet registered any domains in the .br country code domain.³¹

Canadian courts have found that in order to state a claim for injunctive relief, irreparable harm must be shown and that the mere existence of a web site or consumer confusion is insufficient evidence of a loss of goodwill or reputation.³² In the cited case, a British Columbia broadcaster, registrant of the "ITV" trademark and operator of the "itv.ca" web site successfully enjoined use of "itv.net" by a webcaster that argued "ITV" was not sufficiently distinctive to justify infringement protection.

²⁸ *Referee Enterprises v. Planet Ref Inc.*, Case No. 00-CV-1391 (E.D. Wisconsin, filed Oct. 30, 2000). See also Mark K. Anderson, "Ref vs. Ref: Who Decides?", <http://www.wired.com/news/business/0,1367,42248,00.html> (March 9, 2001).

²⁹ Boris Gröndahl, "Nutella finds Gnutella Hard to Swallow", *The Industry Standard*, <http://www.thestandard.com/> (Feb. 28, 2001).

³⁰ Regulations, Annex I, art.2, III, b. at <http://www.unikey.com.br/users/denis/denis21.htm> (visited April 12, 2001).

³¹ Joanna Glasner, "AOL Loses Brazil Ruling", *Wired News*, at <http://www.wired.com/news/politics/0,1283,19918,00.hfm> (May 27, 1999).

³² *ITV Technologies, Inc. v. WIC Television Ltd.*, F.C.J. No. 1803 (F.C.T.D.), Court File No. T-1459-97, November 28, 1997 at <http://www.fja.gc.ca/en/cf/1997/orig/html/1997fca21666.o.en.htm> (visited April 12, 2001).

Bell Actimedia, famous for its yellow pages, successfully enjoined a newly registered owner of “lespagesjaunes.com” in Canada from use of the domain name and any other acts that infringe on Bell Actimedia’s marks.³³

The Draguignan French court proclaimed that it was the duty of the French domain name registrant of “pacanet.com” to conduct due diligence prior to registering the name which infringed a French mark.³⁴

An early French Court decision looked to the fact that defendant’s web site appeared after typing the name of the plaintiff’s commune, Saint Tropez, in a search engine to find infringement, especially in light of the fact that defendant was responsible for designing the commune’s web site at www.nova.fr/saint-tropez yet registered “saint-tropez.com” for itself in the United States.³⁵

The early bird may get the worm in France, where recent case law allows the first registrant of a domain name to prevail against a subsequent registrant who is the legitimate owner of the same trademark for non-competing goods.³⁶

Contrary to some of the earlier cases in Germany, and as evidenced by the “Freundin” or “Girlfriend” case pitting an online dating service against the women’s magazine, the key question for German courts related to infringement has also come to focus on a likelihood of confusion concerning the *actual contents* of the web site, as opposed to mere use of a trademark or trade name in a domain name.³⁷ German Courts also fail to accord greater weight to commercial trade name rights versus non-commercial rights, and have a stated preference for the first to register a legitimate right in the name.³⁸

Similar to the “You Have Mail” U.S. case,³⁹ German Courts do not protect generic words used as trademarks or names in non-competing fields, as evidenced in the Regional Court’s refusal to enjoin a critical medical provider from using the term “emergency” in its domain name as requested by the software game product designer that used the brand name “Emergency”.⁴⁰

A Greek court recently granted United States’ Amazon.com’s request to prohibit the defendant, that hailed itself as “the greatest bookstore of Grecia”, from using the domain names “amazon.gr” and “amazon.com.gr” that it owned, and all related sites because mere use of the name “amazon” sufficiently proves a danger of confusion under the Greek unfair competition law.⁴¹

³³ *Bell Actimedia, Inc v. Andrea Puzo, et al.*, Court File No. T-1839-98, Federal Court of Canada, April 26, 1999 at http://www.fja.gc.ca/en/cf/1999/orig/html/1999fca24841_o.en.htm (visited April 18, 2001).

³⁴ *Affaire Pacanet*, Tribunal de Grande Instance de Draguignan, April 8, 1998 at <http://www.legalis.net/cgi-iddn/certificat.cgi?IDDN.FR.010.0058332.000.R.A.1999.027.41100> (visited April 12, 2001).

³⁵ *Commune de Saint-Tropez c. Eurovirtuel, Quadra Communication et Nova Développement*, Tribunal de Grande Instance de Draguignan, 1ère ch. civile, August 21, 1997 at <http://www.legalis.net/cgi-iddn/certificat.cgi?IDDN.FR.010.0058338.000.R.A.1999.027.41100> (visited April 12, 2000).

³⁶ *Affaire Mutuelles du Mans*, Tribunal de Grand Instance de Paris, September 23, 1999 at <http://www.juriscom.net/jurisfr/mmans.htm> (visited April 12, 2000).

³⁷ *OLG München*, 6 U 4798/97 (“NJW Aktuell”, Heft 27/98, VIII—freundin. de) February 4, 1998 at http://www.netlaw.de/urteile/olgm_2.htm (visited April 12, 2000).

³⁸ *LG Paderborn*, 4 O 228/99, September 1, 1999 at http://www.netlaw.de/urteile/lgpa_1.htm (visited April 12, 2000).

³⁹ See text accompanying note 22, *supra*.

⁴⁰ *LG Hamburg*, 315 O 107/98 June 10, 1998 at http://www.netlaw.de/urteile/lghh_5.htm (visited April 11, 2001).

⁴¹ Provincial Hearing of the Island of Syros, Civil Room, Not 637/1999, commentary to the case by Apóstolos Anthimos, Salonica, at <http://www.dominiuris.com/casos/grecia.htm> (visited April 11, 2001).

Sabena Airlines was unsuccessful in restraining use by an Italian third party of the “sabena.it” domain name.⁴² The court opined that, while the Internet is not clearly regulated by Italian law, domain names appeared more like addresses than trademarks and hence that the Italian registrant had not infringed on Sabena’s registered trademark.

New Zealand’s second largest outdoor advertising company, Oggi Advertising Ltd., was the first Kiwi company to file a domain name lawsuit, and successfully convinced the court to prohibit the defendant from using “oggi” in connection with any internet site and force the defendant to assign the domain name to the advertising company. After the lawsuit was filed, the defendant went so far as to change the registrant information to a fictitious “Mr. Elliot Oggi” and deleted the site details on the “oggi.co.nz” site so that plaintiff could not provide the court with the information that was recorded on the homepage. Still, the court found it appropriate to grant the injunction.⁴³

In Spain, acts related to infringement have resulted in criminal charges against Lynx Telecommunications, a French company which tried to get around the ES-NIC rule that only trademark owners may register a domain using such marks, when it formed a non-profit entity, “Foundation UNI2”, registered the domain name “UNI2.es” and soon thereafter transferred title of the domain name to Lynx. “UNI” has been used as a trademark by the well-known Union Internacional de Limpiezas, SA in Spain for over twenty years. Criminal charges were brought against the defendant for its fraudulent attempt to violate the non-profit codes.⁴⁴

B. Trademark Dilution

1. Statutory Background: U.S

The U.S. Federal Trademark Dilution Act,⁴⁵ adopted in 1996, allows the owner of a “famous mark” to enjoin another person’s use of a trademark or trade name which causes dilution of the “distinctive quality” of the famous mark.⁴⁶ To determine whether a mark is “distinctive and famous”, a court may consider factors including: (i) the degree of inherent or acquired distinctiveness of the mark; (ii) the duration and extent of use of the mark; (iii) the duration and extent of advertising and publicity of the mark; (iv) the geographical extent of the trading area in which the mark is used; (v) the channels of trade for the goods or services with which the mark is used; (vi) the degree of recognition of the mark in the trading areas and channels of trade used by the mark’s owner as well as the person against whom the injunction is sought; (vii) the nature and extent of use of the same or similar marks by third parties; and (viii) whether a federal registration was issued for the mark.⁴⁷

The Act defines dilution as “the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (i) competition

⁴² Sabena S.A., Tribunale Civile de Firenze, Ordinanza del 29/6/2000, <http://www.andreamonti.it/jus/orfi000629.htm> (visited April 18, 2000).

⁴³ *Oggi Advertising Ltd v. McKenzie*, 1998 NZLR Lexis 50 (June 2, 1998).

⁴⁴ Javier A. Maestre, *Los Casos, Espana – CASO UNI2*, at <http://www.dominiuris.com/casos/espanya.htm> (visited April 11, 2001).

⁴⁵ 15 U.S.C. §1125(c)(1) *et seq.*

⁴⁶ The U.S. Federal Trademark Dilution Act does not apply to use of a famous mark in comparative commercial advertising or promotions, noncommercial use of the mark, or news reporting or commentary. 15 U.S.C. §1125(c).

⁴⁷ 15 U.S.C. §1125(c)(1).

between the owner of the famous mark and other parties, or (ii) likelihood of confusion or mistake or to deceive".⁴⁸

2. Application of Statutory Standards

In *Hasbro, Inc. v. Internet Entertainment Group, Ltd.*,⁴⁹ plaintiff Hasbro, manufacturer of game boards and registrant of the "CANDYLAND" trademark, enjoined defendant's internet Entertainment Group from using the "CANDYLAND" name in connection with its Internet site containing sexually explicit material on trademark dilution grounds. Hasbro successfully argued that defendants "have been diluting the value of Hasbro's registered CANDYLAND mark by using the name CANDYLAND to identify a sexually explicit Internet site, and by using the name string 'candyland.com' as an Internet domain name which, when typed into an Internet-connected computer, provided Internet users with access to that site".

Other adult web site operators have received similar treatment in dilution litigation. For example, in *Mattel, Inc. v. Internet Dimensions, Inc.*, defendant registered and used the domain name "barbiesplaypen.com" for a pornographic site.⁵⁰ The court agreed with Mattel that "linking Barbie with pornography will adversely color the public's impressions of Barbie... The Barbie doll has been associated with wholesomeness by generations of preteen girls". In contrast, "the 'models' on the 'barbiesplaypen.com' site, although many have long blonde hair and anatomically improbable dimensions, can in no way be described as engaging in 'wholesome' activities". The court found actual confusion and bad faith intent to profit on the dilution claims. Because the web site clearly "cashes in" on the wholesome Barbie trademark and pairs negative associations with Barbie, it leads to a likelihood of confusion under the tarnishment theory of trademark dilution.

Dilution claims have also been asserted successfully against cybersquatters, profiteers who register as domain names the brands of unrelated parties. For example, in *Panavision International, L.P. v. Toeppen*,⁵¹ defendant Toeppen, a well-known "cyberpirate", registered "panavision.com" as a domain name, and in an attempt to legitimize use of this domain name, set up a web site with aerial views of the town of Pana, Illinois. In response to Toeppen's offer to transfer the domain name to plaintiff for \$13,000, plaintiff sued for dilution of its mark under the federal act and a counterpart state law. The district court granted summary judgment in favor of Panavision, concluding that Toeppen's conduct violated the Federal Trademark Dilution Act and the California anti-dilution statute.

On appeal, the Ninth Circuit acknowledged defendant's argument that his use was non-commercial and therefore non-dilutive, but noted that "his use is not as benign as he suggests. Toeppen's 'business' is to register trademarks as domain names and then sell them to the rightful trademark owners. He 'acts' as a 'spoiler,' preventing Panavision and others from doing business on the Internet under their trademark names unless they pay his fee [citation omitted]. This is a commercial use."

The court noted dilution may be demonstrated by the inconvenience of prospective customers and found that defendant diluted the plaintiff's mark. "Using a company's name or trademark as a domain name is ... the easiest way to locate that company's web

⁴⁸ 15 U.S.C. §1127.

⁴⁹ 40 U.S.P.Q.2d 1479 (W.D. Wash. 1996).

⁵⁰ *Mattel, Inc. v. Internet Dimensions, Inc.*, 55 U.S.P.Q. 1620 (S.D.N.Y. 2000).

⁵¹ 141 F.3d 1316 (9th Cir. 1998).

site. Use of a 'search engine' can turn up hundreds of web sites, and there is nothing equivalent to a phone book or directory assistance for the Internet [citation omitted]. Potential customers of Panavision will be discouraged if they cannot find its web page by typing in "panavision.com", but instead are forced to wade through hundreds of web sites. This dilutes the value of Panavision's trademark."

In *E. & J. Gallo Winery v. Spider Webs, Ltd.*,⁵² a district court found defendant's use of a domain name violated the Texas state version of the Dilution Act. Defendant used the domain name "ernestandjuliogallo.com", which the court found to reference plaintiff's distinctive and famous trademark, to post information about the domain name litigation and the dangers of alcohol. According to the court, such use may place the Gallo winemakers at the risk of losing business and having its business reputation tarnished. Reiterating *Panavision's* sentiment that possession of a domain name mirroring a corporation name is a valuable asset that facilitates communication with a customer base, the court found defendant's registration of the domain name diluted plaintiff's mark.

3. Limitations.

Not all cybersquatting or related practices can be redressed by the Dilution Act. For example, in *Bally Total Fitness Holding Corp. v. Faber*,⁵³ the United States District Court found no trademark dilution on the part of the defendant for his web site entitled "Ballysucks.com". In that case, Bally's, a health club with the registered trademark "Bally", brought trademark infringement, trademark dilution and unfair competition claims against Andrew S. Faber, a web page designer, who used the mark in his internet site which served as a venue for complaints about Bally's health club business.

The court held that, although the health club had a valid protectable mark in "Bally", Faber's use of the trademarked "Bally" in his "Bally sucks" site did not constitute trademark dilution. The court reasoned that given that Faber "was not using the mark to sell his services, or to identify his goods in commerce, that site expressed protected consumer commentary, in that no reasonably prudent Internet user would believe [Faber's] sites were sponsored by the trademark owner".

Northland Insurance Co. v. Baylock,⁵⁴ is another decision allowing the use of domain name protest sites as non-dilutive activity. In *Baylock*, the insurance company sued the registrant of "northlandinsurance.com" for trademark infringement, unfair business practices, violation of the Anticybersquatting Consumer Protection Act, dilution under the Federal Trademark Dilution Act and similar Minnesota State Statute. On the dilution claims, the court recognized Senator Orrin Hatch's comment upon introduction of the bill before it became law that the Dilution Act "[would] not prohibit or threaten non-commercial expression such as parody, satire, editorial or other forms of expression that are not part of a *commercial transaction* [citations omitted]". The court found that the domain name registrant was not operating the site for commercial gain but instead was using it to criticize the insurance company. Thus, the court found no bad faith and denied the requested preliminary injunction.

In *Avery Dennison Corp. v. Sumpton*,⁵⁵ another seminal decision, the U.S. Ninth Circuit Court of Appeals was once again confronted with issues relating to domain name

⁵² 129 F. Supp. 2d 1033 (S.D. Texas 2001).

⁵³ 29 F. Supp. 2d 1161 (C.D. Cal. 1998).

⁵⁴ 115 F. Supp. 2d 1108 (D. Minn. 2000).

⁵⁵ 999 F. Supp. 1337 (C.D. Cal. 1998), rev'd, 189 F.3d 868 (9th Cir. 1999).

registration and trademark dilution. In *Avery Dennison*, defendants acquired some 12,000 domain names, registering common surnames and in essence subletting those names to persons willing to pay a modest price for use of the names as e-mail addresses. Two of those domain names were *avery.net* and *dennison.net*.

Defendants' argument that use of the domain names only for e-mail addresses was a non-trademark use was rejected by the district court: "Defendants' own use is at issue, not that of its licensees. In the hands of the defendants, without a context to limit their intended meaning, the words selected by defendants as domain names connote, and therefore use, all of the common meanings. Defendants' choice to limit the sense to which they license their domain names for use by others does not change the unlimited scope of the meanings held and used by defendants. In the cases of the *Avery* and *Dennison* domain names, these meanings included the meanings attributable to famous trademarks and the defendants' 'use' is within the coverage of the [Federal Trademark Dilution] Act."

The district court noted that the mere registration of the conflicting domain name was sufficient to support a finding of dilution: "It is the registration of the trademark name as a domain name, which denies the holder of the famous trademark from using its trademark name as an Internet domain name, that dilutes the ability to identify goods and services. The sale or license of the domain name to someone else for some other purpose does not eliminate the dilution."

Despite these findings, the district court noted that, in the absence of undisputed evidence that the defendants were merely cybersquatters, plaintiff would be required to pay the defendants \$300 for each domain name relinquished. On appeal, however, the Ninth Circuit reversed the district court's decision and held that plaintiff trademark owner did not establish that its marks were famous and that defendants had not engaged in commercial use of the marks.

In *TCPIP Holding Co., Inc. v. Haar Communications, Inc.*,⁵⁶ the U.S. Second Circuit Court of Appeals held that descriptive marks that have a secondary meaning are not eligible for protection under the Dilution Act.

In *TCPIP*, defendant owned various domain names consisting of variations on Plaintiff's trademark. In vacating the District Court's opinion, the Court of Appeals found that plaintiff failed to show that its mark, "The Children's Place", used in connection with children's retail stores, had sufficient inherent distinctiveness or sufficient fame as required under the Dilution Act. The court focused on the Act's purpose "to protect the owners of famous marks from the kind of dilution permitted by the trademark laws when a junior user used the same mark in a non-confusing way in an unrelated area of commerce".

The *TCPIP* court identified two issues necessary to determine whether a mark is protected under the Act: whether the mark (1) has achieved sufficient consumer recognition to be famous (acquired distinctiveness); and (2) has sufficient inherent distinctiveness to satisfy the Act's requirement of "distinctive quality". Both questions must be affirmatively answered for protection under the Act. Even though the court found *TCPIP*'s mark had achieved a significant degree of consumer recognition, that was not enough to compensate for the mark's lack of inherent distinctiveness. Since the trademark was merely descriptive and enjoyed a secondary meaning, it did not qualify for dilution protection.

⁵⁶ 244 F.3d 88 (2d Cir. 2001).

4. International Developments

Internationally, most countries provide protection for famous or distinctive marks against diluting uses, even where traditional trademark infringement does not exist. Most non-U.S. trademark/domain name disputes surveyed in the preparation of this paper, however, relied upon infringement or unfair competition theories to restrain inappropriate domain name use.

An unusual application of dilution principles is found in an Austrian decision concerning the domain name "bundesheer.at".⁵⁷ The word "Bundesheer" is legally used to refer to the Austrian Armed Forces, which argued that use of this term in a domain name operated by an unrelated party could cause confusion and result in a loss of reputation and image by the Armed Forces. The Austrian Supreme Court rejected this argument, noting that no damage to reputation or image was likely because internet users understand that their search engines generate several "hits" for each search term and that the first hit in any search may well be unsuccessful. This rationale is quite inconsistent with the theory of initial interest confusion articulated in the *Brookfield* decision⁵⁸ as well as the *Panavision* court's assessment that dilution could be established by a user's inconvenience in being drawn to an unintended site.⁵⁹

By contrast, the Delhi High Court in India has ruled consistently with U.S. courts and recently ordered the transfer of the domain name "drreddyslab.com" to the pharmaceutical company Dr. Reddy's Laboratories because it was deceptively similar to Reddy's domain name and "may lead to dilution of distinctiveness of the trademark" of Reddy.⁶⁰ Although the vast bulk of trademarks in use today are unlikely to satisfy the famousness or distinctiveness tests for dilution protection, in the appropriate case dilution arguments remain a formidable weapon against domain names seeking to profit from the use of such well-known marks.

C. Special Cases: Stealthing and Metatagging

A *metatag* is a piece of HTML code invisible to a human viewer but designed to describe the contents of a web site to an internet search engine. Similarly, "stealth" use of a trademark is use in a manner not visually perceptible but perceptible by search engines.

In *Playboy Enterprises, Inc. v. AsiaFocus, Int'l Inc.*,⁶¹ the United States District Court found the defendant liable for metatagging, along with other infringing activity. The court reasoned that the Hong Kong-based defendant owner of adult-oriented web sites with domain names "asian-playmates.com" and "playmates-asian.com" infringed upon the plaintiff's registered trademarks "PLAYBOY" and "PLAYMATE". In addition to finding trademark infringement, the court also found dilution resulting from several willful actions by the defendant, including metatagging or embedding the trademarks "PLAYBOY" and "PLAYMATE" in hidden computer source codes, leading a search engine to the defendants' web sites in response to a search for the plaintiff's trademark.

⁵⁷ Decision 4 Ob 198/00x, Austrian Supreme Court, September 13, 2000, at <http://www.jurpc.de/rechtspr/20010054.htm> (visited April 18, 2000).

⁵⁸ See text accompanying note 17, *supra*.

⁵⁹ See text accompanying note 51, *supra*.

⁶⁰ "Indian Court Transfers Domain Name in Favour of Dr. Reddy's Lab", http://asia...Indian_Court_Transfers_Domain_Name_In_Favour_of_Dr_Reddy_s_Lab.htm (March 20, 2001).

⁶¹ 1998 WL 724000 (E.D. Va. 1998).

Playboy Enterprises was also successful in an earlier suit that involved *its* PLAYBOY trademark and metatagging. In *Playboy Enterprises, Inc. v. Calvin Designer Label*,⁶² defendant Calvin Designer Label had registered the domain names “playboyxxx.com” and “playmatelive.com” to operate an adult entertainment web site. These domain names used plaintiff’s trademarks PLAYBOY and PLAYMATE as metatags. The court granted a preliminary injunction on all claims and enjoined the defendants from using in any manner the PLAYBOY and PLAYMATE trademarks, or any other term likely to cause confusion, including PLAYMATELIVE or “playboyxxx.com” and “playmatelive.com”. The court also ruled that defendant could not use any such name as a domain name, directory name, as the name of its web site service, in buried code or metatags on their home page or web pages.

The United States District Court in Massachusetts also supported the trademark owner’s right to be protected from metatag practices. In *Niton Corp. v. Radiation Monitoring Devices, Inc.*,⁶³ defendant’s web site source code contained keyword metatags including the names of products manufactured by plaintiff Niton, as well as language such as “The home page of Niton Corporation”. The court granted Niton’s request for preliminary injunction because of defendant’s metatag practices. The court reasoned that the content and the means employed to attract visitors to the site have been used in such a way as to create a likelihood of confusion that Niton and RMD are affiliated.

Playboy Enterprises was not as fortunate in *Playboy Enterprises, Inc. v. Welles*,⁶⁴ as it was in *AsiaFocus* and *Calvin Designer Label*. In *Welles*, Playboy Enterprises sued Terry Welles, a former “Playmate of the Year”, asserting trademark and unfair competition causes of action. The court held that “although the magazine publisher’s marks were arguably famous, their distinctiveness did not preclude [Welles], who used the title ‘Playmate of the Year’ in her web page heading and ‘Playboy’ and ‘Playmate’ marks as metatags, from the fair use of those terms.” The court reached this decision in part because “Ms. Welles has used PEI’s trademarks to identify herself truthfully as the ‘Playmate of the Year 1981.’”

In *Brookfield Communications Inc. v. West Coast Entertainment Corp.*,⁶⁵ the Ninth Circuit differentiated between permissible and impermissible uses of the term “Movie Buff” for trademark purposes. In this case, discussed earlier,⁶⁶ the court also held that any use of the “MovieBuff” trademark as a metatag would constitute infringement, as it would result in initial interest confusion rather than source confusion. By using the “MovieBuff” mark as a metatag, West Coast would inevitably attract a number of consumers originally looking for Brookfield’s products but who, upon arriving at the West Coast site, might content themselves with West Coast’s offerings because of their similarity to Brookfield’s products.

The court summarized its conclusion by stating, “Using another’s trademark in one’s metatags is much like posting a sign with another’s trademark in front of one’s store.” Accordingly, the Ninth Circuit reversed the district court and remanded with instructions to enter an injunction against West Coast’s use of “MovieBuff” in its domain name or web site metatags.

⁶² 985 F. Supp. 1220 (N.D. Cal. 1997).

⁶³ 27 F. Supp. 2d 102 (D. Mass. 1998).

⁶⁴ 7 F. Supp. 2d 1098 (S.D. Cal. 1998), *aff’d*, 162 F.3d 1169 (9th Cir. 1998).

⁶⁵ 174 F.3d 1036 (9th Cir. 1999).

⁶⁶ See text accompanying note 17, *supra*.

Although descriptive terms can be used in metatags, "MovieBuff" was not such a descriptive term: "'Movie Buff' is a descriptive term routinely used to describe a movie devotee. 'MovieBuff' is not. When 'MovieBuff' is employed, it is used to refer to Brookfield's products and services, rather than to mean 'motion picture enthusiast'. The proper term for 'motion picture enthusiast' is 'Movie Buff,'" which West Coast could use. However, it could not omit the space.

D. Unauthorized Linking

TicketMaster Corp. v. Microsoft Corp.,⁶⁷ involved a complaint by TicketMaster for trademark infringement and dilution arising out of Microsoft's web site "Seattle Sidewalk", which provided a listing of leisure activities in the Seattle area. By clicking on a link, a user could be transferred directly to the TicketMaster web page where tickets could be purchased for many of the activities advertised at the Microsoft site. Although TicketMaster obtained revenues from this linking arrangement, it alleged that because the link was nonconsensual, its trademark rights were infringed and/or diluted. These issues were not resolved as the case was settled.

As of February, 2001, French online employment companies are entangled in litigation involving deep linking.⁶⁸ Keeping in step with U.S. decisions on deep linking, a French court has ordered Keljob, France's largest employment search engine, to stop providing deep links into job offers posted on another job search site owned by an Internet division of media giant Vivendi Universal, based on "parasitic commercial behavior". Another recent French court decision similarly upheld complaints from the owner of the employment site "Cadreemploi" against Keljob's deep linking practices on the Cadreemploi site.⁶⁹

E. Keyed Banner Ads

A banner ad is an advertisement that stretches across the top and sometimes the side or bottom of a web page and contains a link to the sponsor's web site. Using a third party's trademark as a search term to trigger delivery of a competitor's banner ad is a controversial but apparently ongoing practice.

For example, in *Playboy Enterprises, Inc. v. Netscape*,⁷⁰ Playboy Enterprises sued the Internet search engines Netscape and Excite to stop their practice of arranging for certain combinations of advertisements to appear on the results screen when a user selected the word "playboy" or "playmate" as a search term. Playboy Enterprises unsuccessfully alleged that the search engines were improperly selling advertising space, frequently to adult-themed web sites, keyed on the plaintiff's well-known trademarks, and that these practices constitute trademark dilution.

The court found that "the holder of a trademark may not remove a word from the English language merely by acquiring trademark rights in it" and that "trademark dilution

⁶⁷ No. CV 97-3055 (C.D. Cal. 1997).

⁶⁸ *Cadres Online v. Keljob*, Tribunal de Commerce de Paris, docket number unavailable (December 26, 2000); see "Employment Sites Doing Battle Over Deep Linking in French Courts", <http://internetlaw.pf.com/> (February 22, 2001).

⁶⁹ *Cadreemploi.fr v. Keljob*, Tribunal de Grande Instance de Paris, docket number unavailable (January 8, 2001).

⁷⁰ 55 F. Supp. 2d 1070 (C.D. Cal. 1999), *aff'd*, 202 F.3d 278 (9th Cir. 1999).

protection is not intended to serve as a mere fallback position for trademark owners unable to prove trademark infringement". The court also held that there was no necessary likelihood of confusion and that the First Amendment prevented Playboy Enterprises from being granted a monopoly on the use of those words.

Across the Atlantic, Germany has also dealt with the application of its trademark and unfair competition laws to the Internet. In *Estee Lauder v. The Fragrance Counter*,⁷¹ the District Court of Hamburg ordered Internet companies Excite and iBeauty—formerly named the Fragrance Counter Inc.—to stop using certain Estee Lauder trademarks as keywords to trigger banner ads on web sites. The court ruled that Excite's sale to iBeauty of the trademarks Estee Lauder, Clinique, and Origins as keywords amounted to unfair competition under German law. Similar cases are pending in the U.S. and France.

F. Cybersquatting

Special protections have been developed to address the practice of cybersquatting, which involves the registration as domain names of trademarks, typically well known marks, registered to other parties.⁷²

A thoughtful assessment of the damage caused by cybersquatting may be found in the World Intellectual Property Organization's lengthy Final Report on the Internet Domain Name Process, available at the following url: http://wipo2.wipo.int/process/eng/final_report.html. Among other things, the Final Report recommended that the owners of famous or well-known trademarks be exclusively entitled to register those marks as domain names, that a domain name registrant have the burden of justifying any domain whose name is misleadingly similar to any such mark, and that the Internet Corporation for Assigned Names and Numbers (ICANN) adopt a dispute resolution mechanism for allegations of cybersquatting.

The WIPO acknowledged the widespread problem of abusive registration of domain names, a term which it said encompasses practices ranging from cybersquatting, or the deliberate, bad faith abusive registration of a domain name in violation of trademark rights, to warehousing, or the registration of a collection of domain names corresponding to trademarks in anticipation of selling the domain names to the trademark owners. The WIPO also acknowledged that existing remedies for such practices are frequently ineffective, noting that many are resolved outside the court room, at significant cost to the companies and to the consumers who buy their brand of products. Accordingly, the WIPO recommended the adoption of an expedited administrative procedure for the resolution of all cases of abusive registration.

The Final Report also addressed the long-debated subject of increasing the number of generic top-level internet domains (gTLDs) such as .com, .net and .org, which has recently been resolved, for the time being, with the addition of seven new gTLDs.⁷³

⁷¹ *Estee Lauder v. The Fragrance Counter*, District Court of Hamburg (April 2000).

⁷² John Zuccarini earned between \$800,000 and \$1 million annually from registering and selling thousands of domain names, including misspelled celebrity and company names. Joanna Glasner, "Typo-Loving Squatter Squashed", *Wired News*, <http://www.wired.com/news/business/0,1367,39888,00.html> (October 31, 2000).

⁷³ <http://www.icann.org/tlds/> (visited April 3, 2001). The new TLDs include .biz, .info, .pro, .museum, .aero and .coop. During an initial exclusive registration period, trademark holders were permitted to file domain name applications for names exactly matching their registered marks. As a result of continuing international pressure, ICANN anticipates that additional gTLDs will be forthcoming over time.

1. Cybersquatting Under Trademark Analysis

The commercial misappropriation of one's trademark is often alleged when a party seeks protection against a cybersquatter. However, in *Travel Impressions v. Kaufman*,⁷⁴ the court found that where defendant Kaufman was an authorized user of plaintiff's registered trademarks "Travel Impressions" and "Empress", its use of several domain names similar to these marks, including "travelimpressions.com" and "empresstravel.com" did not constitute misappropriation of the plaintiff's marks. Thus, as the challenged domain names had not been activated and would remain inactive throughout the case, the court denied the plaintiff's motion for preliminary injunction.

In *Hard Rock Café Intern., Inc. v. Morton*,⁷⁵ the court had to consider whether cybersquatting was found when a licensee used the licensed mark beyond the scope of its license agreement. In *Hard Rock*, defendant Morton was one of the founders and original owners of the Hard Rock Cafe. He sold his interest in 1996. As part of that sale, he obtained a license to use and exploit the "Hard Rock Hotel" trademark "solely in connection with the development, operation, ownership, management, operation of and promotion of" the Hard Rock Hotel and Casino and "only in the Morton Territories". Morton operated a web site at "www.hardrockhotel.com" that, among other things, supplied the link through which the Tunes Network could sell its compact discs. A person looking for a Tunes Network compact disc would find that the Hard Rock Hotel mark framed the Tunes site. The court ruled that Morton, as licensee, was in breach of the license agreement in which he agreed only to use the mark in connection with the hotel.

In a dispute between California Closet Company, Inc. and its franchisee in Milwaukee, the United States District Court for the Eastern District of Wisconsin considered a challenge by a franchisor that its Milwaukee franchisee was a cybersquatter.⁷⁶ California Closet sought relief against its franchisee after it learned that the franchisee registered the domain name "californiaclosets.com" and was using the company's registered trademarks on its web site in an unauthorized manner. The franchisor grew concerned because the franchisee's web site simultaneously gave the appearance that the company published the site, yet the site requested that visitors call a toll-free telephone number that differed from the one approved for use by the Company. California Closet Company ultimately succeeded in enjoining the franchisee's infringing uses of the Company's trademarks in the franchisee's domain name and web site.

2. International Applications.

Most international courts and dispute resolution bodies similarly favor trademark owners over cybersquatters. For instance, Holland has gone beyond finding cybersquatters liable for trademark infringement. In *Labourchere v. IMG Holland*, the court found a cybersquatter liable for trademark infringement even though trademarks could be registered under other gTLDs than ".com".⁷⁷ The court also recognized that greater commercial value attaches to ".com" domain names than to others.

Two German court opinions have been handed down against cybersquatters, acknowledging that the acquisition of web site domain names that incorporate names of

⁷⁴ Bus. Franchise Guide (CCH) ¶¶ 11,470 and 11,471 (E.D.N.Y. 1997).

⁷⁵ 1999 WL 717995 (S.D. N.Y. Sept. 9, 1999).

⁷⁶ *California Closet Co., Inc. v. Space Organizational Systems, Inc.*, Bus. Franchise Guide (CCH) ¶ 11,150 (E.D. Wis. 1997).

⁷⁷ *Labourchere v. IMG Holland*, President District Court, Amsterdam, May 15, 1997 RudW193.

companies unrelated to the purchaser of the domain names is improper.⁷⁸ German courts may enjoin any person who registers an internet domain name that incorporates the “trade name” of a company when the registrant has no relationship or interest to or in such company.

As part of Norway’s attempt to limit cybersquatting, the Norwegian Registration Service for Internet Domain Names (“NORID”) has a domain name registration policy for “.no” that requires each applicant to sign a statement certifying that “to the best of his or her knowledge, registration or use of the names does not violate any third party’s registered or unregistered rights to the name”. NORID also limits the number of domain names each organization may register under its name at any time to fifteen.⁷⁹

Hong Kong does not have specific laws dedicated to intellectual property related to the Internet, but instead relies on pre-existing trademark, copyright or unfair competition laws. Cybersquatting complaints in Hong Kong may be resolved pursuant to the Domain Dispute Resolution Policy Statement of the Hong Kong Network Information Center (“HKNIC”).⁸⁰

In China, the China Internet Network Information Center (“CNNIC”) manages and operates the Chinese domain name system, but has no power to cancel or transfer domain names absent judgment gained in a civil action.⁸¹ In an attempt to quell “vicious domain name registering”, the Beijing Higher People’s Court in China has instituted tough new rules regulating Internet domain name registration. The rules set forth fines for “anyone who deliberately confuses their domain name with a famous trademark to confuse people”.⁸²

In September 2000, a French Court of Appeals handed down a decision related to distribution rights for trademarked products via the Internet.⁸³ Sony granted France-based Alifax a license to use the term Espace Sony in advertising and marketing operations. In mid-1997, Alifax registered the domain name “espace-sony.com”. In late 1999, Sony informed Alifax it disagreed with Alifax’s use of the Sony trademark online and demanded Alifax stop using the domain name.

The French county court found Alifax’s registration and use of the trademarked domain name in violation of Sony’s intellectual property rights. The license was for shopfront, advertising and marketing materials. The Court of Appeals narrowed the lower court’s ruling, however, finding Alifax did not engage in any intentional wrongdoing, counterfeiting or trademark infringement. Although the Appeals Court upheld the demand that Alifax stop using the domain name, it did not uphold the damage award, instead ordering Sony to pay \$8,200 U.S., and admonished Sony to be more cautious in future distribution contract negotiations.

⁷⁸ See John R. Schmertz and Mike Meier, “The German Courts Find Acquisition of Internet Domains Using Names of Unrelated Companies Improper Since Profit is Sole Motive”, 7 Int’l L. Update 22 (February 2001).

⁷⁹ <http://www.norid.no/name-policy.html/#link1> (visited March 25, 2001).

⁸⁰ The HKNIC’s web site is found at <http://www.hknic.net.hk/hknic/>.

⁸¹ See www.cnnic.net.cn/e-index.shtml. A more thorough discussion of the application of laws regarding Internet domain name issues in Hong Kong and China is found at Yvonne Chua, “Protecting Intellectual Property Rights in the International Marketplace: New International Boundaries”, 621 PLI/Pat 255 (October 2000).

⁸² “China Warns Internet Domain Name Squatters”, <http://dailynews.muzy.com/ll/english/84348.shtml> (August 27, 2000).

⁸³ *S.A.R.L. Alifax v. S.A. Sony France*, <http://www.juriscom.net/txt/jurisfr/ndm/caversailles20000914.pdf> (Versailles Ct. of App. 2000).

3. U.S. Anticybersquatting Consumer Protection Act ("ACPA")⁸⁴

The ACPA, adopted in the fall of 1999, makes cyberpiracy a separate violation of the U.S. Lanham Act. Specifically, any person who has bad faith intent to profit from another's mark (e.g., selling the mark), and registers a domain name that is identical or confusingly similar to a distinctive or famous mark of another, violates the Act.

Bad faith intent may be found in several instances. For instance, bad faith may be found where the registrant intends to divert customers away from the trademark owner's web site to a site found under the domain name that could harm the goodwill associated with the mark by creating a likelihood of confusion as to the source, sponsorship, affiliation or endorsement of the site. Bad faith may also be found if the registrant offered to sell the domain name or has a pattern of offering to sell domain names it has not used to make a bona fide offer of goods or services.

The ACPA makes it easier for courts to have jurisdiction over cybersquatters. Traditionally, the trademark owner had to obtain *in personam* jurisdiction, often over a party who gave false information to the domain name registry.⁸⁵ The ACPA also allows *in rem* actions against the domain name owner if the court cannot get personal jurisdiction over the domain name owner, if the domain name owner gave false information to the registrar, or if the domain name owner has not updated the name's record and, therefore, cannot be located.

Penalties for any such violation include the court-ordered transfer of the domain name, injunctive relief preventing any further such acts, actual damages and lost profits, statutory damages up to \$100,000 per domain name, court costs and attorneys' fees. Hundreds of actions under the Act have been filed across the country, resulting in several reported decisions in favor of trademark owners as well as a general market decline in the asking price generally sought by cybersquatters for turning over their improperly registered domains.

For instance, in *Sporty's Farm L.L.C. v. Sportsman's Market, Inc.*,⁸⁶ the court granted injunctive relief in favor of the trademark owner after setting forth its holding that the ACPA applies even if the domain name was registered before the law took effect. In *Sporty's*, the owner of the internet domain name "sportys.com" brought an action against a catalog company that held the "sporty's" trademark. Sporty's Farm sought a declaration that as owner of the "sporty's.com" domain name, it had the right use that name. Sportsman's Market brought a counterclaim alleging trademark infringement and dilution, and unfair competition under state law. Upon applying the ACPA, the court granted injunctive relief in favor of the trademark owner, holding that "sporty's" trademark was distinctive and that the trademark and domain name were confusingly similar. The court further held that Sporty's Farm, the domain name owner, acted in bad faith because it intended to profit from Sportsman's Market's mark.

The U.S. District Court for the Eastern District of Virginia interpreted the ACPA in *Virtual Works v. Network Solutions*.⁸⁷ Volkswagen sued Virtual Works claiming trademark infringement and dilution due to its use of the "vw.net" domain name. Virtual Works

⁸⁴ 15 U.S.C. § 1125(d) *et seq.*

⁸⁵ Many countries, such as Japan, still require *in personam* jurisdiction. See Ian C. Ballon, "Rethinking Cyberspace Jurisdiction in Intellectual Property Disputes", 21 U. Pa. J. Int'l Econ. L. 481 (Fall 2000). 202 F.3d 489, 502 (2d Cir. 2000).

⁸⁷ No. 99-1289-A (E.D. Va., Feb. 24, 2000).

asserted that Volkswagen was interfering with its right to use its lawfully registered domain name. The court concluded that Volkswagen is the only entity with a legal right to use the initials "VW" and that Virtual Works has never conducted business using those initials. The fact that Volkswagen and Virtual Works offer different products was irrelevant since both parties use the Internet as a facility to provide goods and services. Furthermore, the court concluded that Volkswagen's inability to use the "vw.net" domain name has caused it economic harm and diluted its trademark. Accordingly, the court decided that Virtual Works was a cybersquatter that must turn over its domain name, "vw.net", to Volkswagen.

In late January, 2001, the U.S. Fourth Circuit Court of Appeals affirmed the district court judgment and ordered Virtual Works Inc. to transfer the domain name "vw.net" to Volkswagen under the ACPA.⁸⁸ Virtual Works had registered "vw.net" late in 1996 for use with its Internet business. Certain Volkswagen dealerships contacted Virtual Works two years later in 1998 to inquire about the site. As a result, Virtual Works approached Volkswagen about purchasing the domain name. The court found evidence of "mixed motive" in Virtual Works' registration of the name, which made Virtual Works ineligible for the ACPA's safe harbor available to defendants who have a reasonable belief their domain name use is lawful. The court ordered Virtual Works to transfer the domain name to Volkswagen, especially in light of the fact that Virtual Works was aware of the potential confusion surrounding the vw.net name when it registered it.

Brands for luxury cars have also been protected under the ACPA. For example, a domain name owner who advertised various famous mark domain names for sale, including "PorscheSource.com", has been stopped by Porsche Cars North America, Inc.⁸⁹ A U.S. District Court in California granted Porsche an injunction against defendant's auction, offer for sale, transfer or use of the domain name pending resolution of the lawsuit, based on the court's finding that the majority of the bad faith factors weigh in favor of a finding that the defendant likely acted with a bad faith intent to profit from Porsche's mark.

4. The Internet Corporation for Assigned Names and Numbers ("ICANN")

ICANN is the governing body for domain name registration for the Internet. In order to facilitate the registration and administration of domain names, ICANN adopted a Uniform Domain Name Dispute Resolution Policy (the "Policy"), which may be found at the following url: <http://www.icann.org/udrp/udrp.htm>.

Under the Policy, disputes arising out of cybersquatting, and similar types of abusive domain name registrations, may be resolved through expedited administrative proceedings conducted by ICANN-sanctioned dispute resolution services. Specifically, disagreements involving domain names sponsored by Network Solutions, America Online, and the Name IT Corp., as well as domain names sponsored by ICANN-accredited domain name registrars, are covered by the ICANN dispute resolution policy.

Under the Policy a party which desires to enforce a claim of abusive registration may :

- (a) file a complaint in a court of proper jurisdiction against the domain-name holder (or where appropriate an *in rem* action concerning the domain name); or

⁸⁸ *Virtual Works, Inc. v. Volkswagen of America, Inc.*, 238 F.3d 264 (4th Cir. 2001).

⁸⁹ *Porsche Cars North America, Inc. v. Spencer*, 2000 WL 641209 (E.D. Cal. 2000).

(b) in cases of abusive registration submit a complaint to an approved dispute-resolution service.⁹⁰

In the first decision under the Policy, *World Wrestling Federation Entertainment, Inc. v. Michael Bosman*,⁹¹ the WIPO Arbitration and Mediation Center considered whether respondent Bosman had legitimate rights to the domain name "worldwrestlingfederation.com." The complainant World Wrestling Federation Entertainment, Inc., contended that Bosman registered the domain name in bad faith and it should not be permitted to use its domain name because it is identical to the World Wrestling Federation's service mark and trademark, "World Wrestling Federation".

The Administrative Panel found under Paragraph 4(a) of the Policy that the disputed domain name, "worldwrestlingfederation.com", was identical or confusingly similar to the mark registered by complainant. Secondly, the Panel decided that respondent therefore had no legitimate interests or rights in connection with using that domain name. Finally, the Panel determined that the name was registered in bad faith as respondent offered to sell the mark three days after it was registered. Thus, the Panel decided that registration of the domain name "worldwrestlingfederation.com" be transferred to the World Wrestling Federation.

An Administrative Panel of the WIPO Arbitration and Mediation Center considered another similar case in *Alcoholics Anonymous World Services, Inc. v. Lauren Raymond*.⁹² There the Panel once again considered whether respondent Lauren Raymond had a legitimate right to use the domain name "alcoholicsanonymous.net", despite complainant Alcoholic Anonymous World Services ("AA Services") ownership of the trademark and service mark "Alcoholics Anonymous". AA Services proved each of the three prongs to Paragraph 4(a) of the Policy. The Panel required Raymond to transfer the domain name "alcoholicsanonymous.net" to AA Services, as the domain name was identical or confusingly similar to the Alcoholics Anonymous mark, Raymond had no rights in connection with the domain name, and, she had registered the domain name in bad faith.

In the relatively short time the Policy has been in effect, hundreds of decisions have been issued, affecting domain names as diverse as "bestwestern-hotels.com",⁹³ "juliaroberts.com"⁹⁴ and "absolute-vodka.com".⁹⁵ Although this paper cannot comprehensively analyze each of these decisions,⁹⁶ in general it appears that owners of registered marks have been successful in recovering identical or confusingly similar domain names in the overwhelming majority of cases. By contrast, owners of unregistered marks have had mixed results under the Policy.⁹⁷ The outcomes of cases

⁹⁰ Uniform Domain-Name Dispute Resolution Policy, <http://www.icann.org/udrp/udrp.htm> (visited July 17, 2000).

⁹¹ Case No. WIPO D99-0001, <http://arbitrator.wipo.int/domains/decisions/html/d99-0001.html> (Jan. 14, 2000).

⁹² Case No. WIPO D2000-0007, <http://arbitrator.wipo.int/domains/decisions/html/d2000-0007.html> (Mar. 6, 2000).

⁹³ *Best Western International, Inc. v. CITI Services, Inc.*, Case No. NAF FA0003000094299, <http://www.arbforum.com/domains/decisions/94299.htm> (April 12, 2000).

⁹⁴ *Julia Fiona Roberts v. Russell Boyd*, Case No. WIPO D2000-0210, <http://arbitrator.wipo.int/domains/decisions/html/d2000-0210.html> (May 29, 2000).

⁹⁵ Case No. NAF FA 0096606, <http://www.icann.org/udrp/proceedings-list.htm> (February 16, 2001).

⁹⁶ In February 2001 alone, 249 domain name disputes were filed under the Uniform Domain Name Dispute Resolution Policy of ICANN. <http://www.icann.org/udrp/proceedings-list.htm> (visited March 18, 2001).

⁹⁷ See, e.g., *Gordon Sumner p/k/a Sting v. Michael Urvan*, Case No. WIPO D2000-0596, <http://arbitrator.wipo.int/domains/decisions/html/d2000-0596.html> (July 20, 2000). See also Ivan Hoffman, "Bruce and Julia: A Domain Name Case Study", http://www.jurisnotes.com/articles/Domain_Name_Case_Study.htm, in which the author discusses the disparate results in domain name proceedings initiated by entertainers Bruce Springsteen and Julia Roberts.

decided under the Policy have been criticized as unfairly biased toward holders of marks and inappropriately variable depending upon the dispute resolution organization selected to handle the matter and the composition of the panel hearing the dispute.⁹⁸ In any event, because of the speed and efficiency of results obtained under the Policy, this procedure has been adopted by many mark owners as the weapon of choice in combating cybersquatting.

IV. Copyright protection in cyberspace

The Internet contains a vast number of works subject to protection under domestic and international copyright laws, including written materials, music, movies, multimedia works and database information. Because of the nature of the Internet, which permits easy and usually anonymous electronic access to posted materials, it is difficult to police whether anyone has “copied” the material and, if so, to determine where any copy may be stored. Furthermore, it is impossible to complete the electronic transmission of any material on the Internet without “copying” the works because information on the Internet is transmitted through various servers and nodes of the network. Thus, the mere nature of the Internet further complicates Internet copyright issues, which are evolving and to some degree unresolved. This portion of the article will provide a brief survey of the most significant issues surrounding copyrights on the Internet.

A. *Scope of Copyright Protection*

The U.S. Copyright Act protects “original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device”.⁹⁹ A copyright owner has the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies, to perform the work publicly, to display the work publicly and to perform the work by means of digital audio transmission.¹

Exceptions to the exclusive rights are provided under the Copyright Act for fair use of a work for purposes such as criticism, comment, news reporting, teaching or scholarship; reproduction by libraries and archives of one copy of a work for archival preservation and security purposes; and sale of a copy of a work by the owner thereof.² In addition, the owner of a copy of a computer program may make or authorize the making of another copy or adaptation of the program so long as the copy is for archival purposes or is created as an essential step in the utilization of the computer program in conjunction with the machine.³

⁹⁸ Michael Geist, “Fair.com?: An Examination of Systemic Unfairness in the ICANN UDRP”, <http://aix.uottawa.ca/~geistudrp.pdf>. The author of this article has set up a web site permitting users to track the decisions rendered by individual panelists in such cases: <http://www.udrpinfo.com>.

⁹⁹ 17 U.S.C. §102(a).

¹ 17 U.S.C. §106.

² 17 U.S.C. §107–109.

³ 17 U.S.C. §117.

As the ongoing saga of Napster demonstrates, the scope of copyright protection on the Internet is far from settled. A preliminary injunction was issued March 5, 2001, against Napster, the online music swapping service, giving it 72 hours to block song titles of copyrighted works identified by the music industry and various artists.⁴ This is just one step in the battle over Napster's liability for contributory and various copyright infringement of songs.

The pirated music phenomenon may be on its way to resolution for Napster, but for those trying to stop music pirates from bootleg distribution of music in Russia, the fight is an uphill battle. According to some sources, Russian pirates have accounted for well over \$310 million in U.S. losses for bootlegged CDs.⁵ In the online global marketplace, copyright owners still face great difficulty in protecting their works. While most businesses, including franchisors, are unlikely to become involved in practices such as online "music sharing" as Napster fans and international music pirates have, they may well encounter other copyright-related practices that have frustrated others on the Internet.

In the wake of the U.S. Ninth Circuit Appeals Court's decision in February of this year that Napster may be held liable for copyright infringement,⁶ a suit was filed in New York related to copyright ownership of materials duplicated over the Internet. In *Random House, Inc. vs. Rosetta Books LLC*,⁷ Random House alleged that defendant Rosetta Books offers e-books on line for certain popular Random House books without the publisher's permission, thereby infringing the copyright licensed exclusively to Random House. Random House claimed it has, "for the term of the copyright, the exclusive right to publish and sell the works contracted for in book form, which it claims gives it the exclusive right to publish its authors' works in "eBook" formats".

Rosetta Books is a relatively new start-up company that claims to be an electronic publisher of great works. Random House claimed, however, that "[t]he sum total of Rosetta Books' 'publishing' activities to date has entailed the copying in digital form of copyrighted works such as those covered by the [Random House Author] Agreements." Random House feared that Rosetta Books' actions would greatly adversely affect Random House's new e-book business and therefore filed suit to enjoin such alleged infringement which, according to Random House, constituted an attempt to "skim the cream of modern literature in utter disregard of the contractual and copyrights owned in such works by the publishers that introduced, marketed and sold them to the public at great investment".

In a decision issued in July 2001, a federal district court refused to grant Random House the requested injunction against Rosetta Books.⁸ The court held that the exclusive right to "print, publish and sell the work[s] in book form" does not include the right to publish the works in digital form.

As courts attempt to battle online copyright infringement, technology may win the war. In yet another interesting technological development, copyright owners may soon find even more sources of infringement of their copyrights in works on the Internet. IBM Corporation recently announced a new software product that will instantly translate into

⁴ *A&M Records, Inc. v. Napster, Inc.*, 2001 WL 227083 (N.D. Cal. 2001).

⁵ See Farhad Manjoo, "Russian Pirates Rule the CDs", <http://wired.com/news/culture/0,1284,39234,00.html> (October 6, 2000).

⁶ *A&M Records, Inc. v. Napster, Inc.* 239 F. 3d 1004 (9th Cir. Feb. 12, 2001, as amended Apr. 3, 2001).

⁷ *Random House, Inc. v. Rosetta Books LLC*, Case No. 01-01728 (S.D.N.Y., filed Feb. 27, 2001); Complaint at 7ILR (P&F) 4020.

⁸ *Random House, Inc. v. Rosetta Books LLC*, 150 F.Supp.2d 613 (S.D.N.Y. 2001).

another language documents that are sent over the Internet or the contents of a web site.⁹ IBM is likely to face a legal challenge to the software because the translations occur without the copyright holder's consent. This is true especially in light of the ever-expanding internet copyright infringement suits such as recent *Random House* case. Most publishers contract with authors regarding foreign language translation rights. Thus, either the publisher which has obtained a license for such translation rights or the author who has maintained such rights may have a cause of action against internet users who employ such software to translate works themselves. More likely than suits against individual users, however, IBM faces the potential of contributory copyright infringement claims similar to those asserted against Napster.

B. Linking and Framing

A "link" is an electronic address embedded in a web site that "points" to another web site. There are two types of links—"out link" and "in link". An "out link" stores the electronic address of a different web site, permitting a user to move to the new site merely by clicking on the link. An "in link", sometimes referred to as a "frame", also points to another web site but, upon being clicked, in effect pulls text, images or other materials from the other web site into the documents currently being viewed by the user.

The first case to address the technique known as framing was *Washington Post Co. v. TotalNews, Inc.*¹⁰ In *TotalNews*, defendant TotalNews provided links from its web site to more than 1,200 news organizations, identified by name. Upon clicking one of the names, the user viewed the remote site, displayed within the frame of TotalNews' web site, thereby permitting messages from TotalNews' advertisers to remain on the screen. The Washington Post and a number of other news organizations sued TotalNews for copyright infringement and related causes of action. In their complaint, the plaintiffs accused TotalNews of "pirating copyrighted material", republishing it and profiting from the work of others. The case settled shortly after being filed. As part of the settlement agreement, TotalNews agreed to discontinue framing the seven web sites that were at issue in the suit. Thereafter, TotalNews would provide a direct link to the web sites without TotalNews, or its advertisers, tagging along to decorate the site.

On the other hand, the United States District Court for the Central District of California opted not to find copyright infringement in *FutureDontics Inc. v. Applied Anagramics Inc.*¹¹ There the plaintiff operated a dental referral business utilizing the anagrammatic phone number "1-800-DENTIST", while the defendant owned the registered service mark "1-800-DENTIST." Later, the plaintiff decided to establish an Internet web site to promote its dental referral service. Its site consisted of a number of web pages containing graphics and text, which were copyrightable material. The plaintiff registered its copyrighted web pages. Thereafter, defendant Applied Anagramics developed its own web site. Its web site established a link which reproduced FutureDontics' web pages within a frame that includes its logo and information about Applied Anagramics. The court ruled for the defendant by denying plaintiff's preliminary injunction motion because the plaintiff had failed to demonstrate that framing of material from its web site created a derivative work in violation of the its copyrights.

⁹ See "In The News", *Cyberspace Lawyer*, 5 No. 11 Cyberspace Law 22 (February 2001).

¹⁰ 97 Civ. 1190 (S.D.N.Y. 1997).

¹¹ 45 U.S.P.Q.2d 2005 (C.D. Cal. 1998), aff'd, 152 F.3d 925 (9th Cir. 1998).

Subsequent to the copyright action, both FutureDontics and Applied Anagramics were back in court on trademark grounds. In this second round of the parties' dispute, the district court issued a preliminary injunction against FutureDontics, prohibiting promotion of any product "in connection with" the mark Applied Anagramics. The Ninth Circuit Court of Appeals upheld the injunction, noting the threat of irreparable harm to Applied Anagramics and that FutureDontics should be aware it cannot use the plaintiff's mark to promote any dental products without Applied Anagramics' prior approval.¹²

The practice of linking has also received variable treatment by courts. In *The Shetland Times Co., Ltd. v. Wills*,¹³ the plaintiff Shetland Times maintained on its web site articles that had appeared in the print version of its newspaper, accessible by clicking on a headline on the "front page" of the web site. The defendant Shetland News maintained a web site containing the Times' headlines verbatim which, when clicked, linked directly to the full text of the Times' articles, bypassing the Times' front page (and the advertisers who appeared on that front page). In the only order issued in the case before it was settled out of court, the Court of Sessions ruled for the plaintiffs by enjoining the defendants from deep linking. The court determined that the headlines were copyrightable literary works, rejecting the defendant's argument that the headlines were not the product of sufficient skill or effort to be copyrightable, and that copying of the headline constituted copyright infringement, at least in some instances.

A directly contrary result was rendered by a Dutch court.¹⁴ PCM, the publisher of several Dutch daily national newspapers, sought to prevent the online publication of headlines by Krantem.com. Each headline linked to the text of the related article on the newspaper's web site, bypassing the newspapers' home page. The Rotterdam District Court rejected PCM's copyright claims, noting that the web site could rely on the "droit de citation" of the Berne Convention, and observed that PCM had neither implemented technical measures to prevent linking nor sought to mitigate its home page advertising losses by placing ads adjacent to articles on the PCM site.

In *Ticketmaster Corp. v. Tickets.com*,¹⁵ the court considered whether the deep linking involved in this case violated copyright laws. In *Ticketmaster*, defendant Tickets.com's web site allegedly contains deep links to event descriptions on Ticketmaster's web site, bypassing the home page and other pages, and through use of "spiders", systematically copied and extracted event descriptions reformatted on defendant's site. Plaintiff Ticketmaster allege that Tickets.com's deep links to its web site are diluting its value. In a March 27, 2000 minute order, the district court noted that "hyperlinking does not itself involve a violation of the Copyright Act (whatever it might do for other claims) since no copying is involved" and that "deep linking by itself (i.e., without confusion of source) does not necessarily involve unfair competition". On the other hand, the court noted that the practice could involve a breach of contract, as a violation of the "terms of use" at Ticketmaster's site.

An aggressive variation of linking was at issue in *eBay v. Bidder's Edge, Inc.*¹⁶ There a U.S. District Court found that eBay was likely to prevail on the merits of its trespass claim against Bidder's Edge due to potential irreparable harm to eBay. eBay sued Bidder's Edge for infringement of eBay's intellectual property by way of "crawling" on eBay's web site

¹² *FutureDontics, Inc. v. Applied Anagramics, Inc.*, 201 F.3d 444 (9th Cir. 1999).

¹³ Scotland Court of Session (1996).

¹⁴ "Dutch Newspapers Lose Attempt to Ban Links", E&P Online, <http://www.mediainfo.com/ephome/news/newshtml/stories/082400n4.htm> (August 24, 2000).

¹⁵ No. CV 99-7654 (C.D. Cal. 2000).

¹⁶ *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

in contravention of eBay's posted terms of use policy.¹⁷ Bidder's Edge then used the data collected about eBay items on Bidder's Edge's own site. Following the district court's ruling that such conduct was likely to render Bidder's Edge liable for trespass, the parties settled the lawsuit by agreeing to a confidential payment by Bidder's Edge and its promise to cease crawling eBay's site for information.

C. *Digital Millennium Copyright Act*

As a franchisor develops a greater presence on the Internet, the Digital Millennium Copyright Act¹⁸ ("DMCA") becomes more important. The DMCA implements the World Intellectual Property Copyright Treaty and Performances and Phonograms Treaty ("WIPO treaties") and explicitly provides limitations on liability for copyright infringement to internet service providers ("ISPs"). An increasing number of franchisors provide their franchisees and others with various internet enabled means of communication, which could permit the franchisors to come within the definition of an ISP. Accordingly, franchisors which provide such resources may be able to assert that the protections afforded by the DMCA to a traditional ISP are available to franchisors as well. The WIPO treaties require ratifying countries to update their laws against piracy of copyrighted materials in accordance with the treaties. Each country also must extend its laws "to the electronic commerce marketplace epitomized by the Internet".

The DMCA defines an ISP as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material as sent or received". Section 512(a), as amended by the DMCA, states that an ISP is not liable for copyright infringement "by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the...(ISP), or by reason of the intermediate and transient storage of that material" in performing this service. This limitation is conditioned on: (1) the transmission being at the request of a person or entity other than the ISP; (2) selection of the material transmitted by a person or entity other than the ISP; (3) selection of the recipient of the material transmitted by a person or entity other than the ISP; (4) the ISP not maintaining a copy accessible to anyone other than the requesting party; (5) the ISP not maintaining a copy longer than is reasonably required for the transmitting, routing, or provision of connections; and (6) the ISP transmitting material without modification. In addition, to be protected by the limitations on liability provided in the DMCA the ISP must have designated an agent to receive notifications of claimed infringement.

Section 512(a) insulates ISPs from claims of contributory copyright infringement resulting from aiding users in accessing material on the Web. Section 512(b) limits ISPs' liability regarding system caching, which involves storing a copy of material in the system as a result of a request. Specifically, Section 512(b)(1) provides that an ISP is not liable "for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service

¹⁷ e-Bay's current User Agreement states that the site "contains robot exclusion headers and you agree that you will not use any robot, spider, other automatic device, or manual process to monitor or copy our web pages or the content contained herein without our prior expressed written permission". <http://pages.ebay.com/help/community/pmg-user.html> (visited April 2, 2001).

¹⁸ Pub. L. No. 105-304, 112 Stat. 2860 (1998).

provider". This language protects ISPs from claims of direct infringement for storing copies, or equivalent reproductions, of the work on the ISP systems at a user's request. This protection is conditioned on: (1) the material having been made available on the Web by someone other than the ISP; (2) the material being transmitted at the direction of someone other than the ISP; and (3) the storage occurring as part of an automatic process for the purpose of making it available to the users. Furthermore, the ISP must not modify the material, must comply with any requirements imposed by the person making the material available on the Web, must ensure that any access requirements, such as passwords for users, are met, and must disable access expeditiously if notified that the material was made available without authorization of the copyright holder.

In addition to the DMCA, one of the remaining sections of the Communications Decency Act (section 230) provides possible protections for franchisor ISPs. Specifically, the act states that "no provider of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". In addition, "no provider or user of an interactive computer service shall be held liable on account of (a) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected, or (b) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described... [in the preceding sentence]". In posting to a web site materials furnished by third parties, and in providing Internet, Extranet or similar services to franchisees, franchisors should consider how best to avail themselves of these statutory protections.

V. Online privacy

A. Background

Online privacy issues have become critical in recent years, as studies and surveys illustrate the anxiety and concern of internet users and other members of the public over these issues and the impact that such concern can and does have in the success of any e-commerce strategy.

A recent joint survey by Ipsos-Reid and Columbus Group of Internet users in Canada¹⁹ showed that, contrary to popular belief, the vast majority of internet users (82%) have shared personally identifiable information online. Of particular interest to businesses was the finding that there were two definite reasons why Internet users were more likely to submit personal information at one site rather than another: one major factor that made internet users more comfortable in providing personal information was the company's reputation (74%), and the other was the stated privacy policy on such web site which explained the company's intended use of the submitted information.

This survey also disclosed that a privacy policy constitutes the leading opportunity for businesses to build trust with users who have never felt comfortable disclosing personal information online. Fifty-seven per cent of such internet users stated that a solid online

¹⁹ Released on March 1, 2001, found at <http://www.columbusgroup.com>.

privacy policy would most likely make them reconsider sharing personal information, while 53 per cent stated that the company's reputation would also influence their decision. Interestingly enough, even with the Canadian government's recent adoption of privacy legislation, only 36 per cent of these users claimed that increased government regulation would make them more comfortable.

Perhaps more importantly, the survey found that 18 per cent of internet users who have shared personal information claim to have experienced a breach of their online privacy. Presumably, the actual percentage of breaches is higher, the cited number only reflecting the breaches of which the users were aware.

Legislators in many countries have not remained indifferent to these concerns and findings. Most countries have begun legislating or regulating the collection, use and disclosure of personally identifiable information, namely any information which allows an individual (*i.e.* not a corporation or other legal entity) to be identified (*e.g.*, name, address, telephone number, e-mail address and any other information relating to an identified or identifiable individual).

This portion of this paper will provide a brief overview of the legislative framework relating to online privacy in the U.S., the European Union and Canada, particularly from the perspective of U.S. franchisors who carry on business, or intend to carry on business, in any country of the European Union and Canada.

1. Which Law Applies?

One of the most significant hurdles to widespread acceptance of online privacy initiatives for the worldwide communication medium of the Internet is the sometimes significantly different privacy rules contained in legislation from country (or group of countries, such as the E.U.) to country, and within such country or groups of countries. Will compliance with these different standards require the establishment of parallel systems within an organization ?

In fact, even a determination of which country's privacy laws actually apply to a given set of circumstances will often be difficult to pin down with any degree of certainty. Which will be the determining factor: is it the physical location of the corporate branch where decisions are made, the physical location of the computer server which handles or stores the information, the location of the individuals whose personal information is at issue, the location from which the web site containing such information is accessible, or some other factor ? The response in one country will often conflict with the response in another country, which could lead one to conclude that compliance with several countries' privacy legislation is required in order to avoid potential liability.

Franchisors should be concerned with privacy legislation as, in principle, all personal information is subject to such legislation, from the obvious, such as personal information concerning to its customers, to the less obvious, such as personal information relating to its employees or its franchisees or their employees, or even a franchisee's client lists remitted to a franchisor at the expiration or termination of the franchise relationship. A thorough review of information collection practices should be undertaken by each franchisor to determine where it faces the greatest exposure to claims for infringement of privacy, and an examination of information required to be provided through international franchise agreements, either on a recurring basis or on a one-time basis (such as termination or expiration of the term), is an essential component of a comprehensive review.

2. How is Data Collected?

Before commencing our review of the legislative framework regarding online privacy and security, it would be useful to review the manner in which personal information is usually collected online. In fact, the method of collection will, in many countries, impact upon the extent of the collector's obligations to inform the individual or obtain consent from the individual in connection with said collection of information.

The most transparent manner in which to collect personal information is to ask the individual to provide information directly. For example, a customer's address, credit card data, age or preferences may be provided directly by the customer on a web site.

A less transparent method of collecting personal information is through the use of "cookies", which are small computer files stored on the customer's personal computer when browsing the web site. These cookies usually store and use information about a customer (e.g. user names, recent internet searches, passwords, etc.) to customize what is seen by such customer when he returns to the web site. While most internet browser software allows for a systematic or selective refusal to accept cookies, many internet users are unaware of the existence or use of cookies or their ability to configure their browser software so as to refuse the placing of cookies on their personal computer. Interestingly enough, a recent decision in the U.S.²⁰ dismissed a class action suit against DoubleClick, Inc., an internet advertising agency, stating that the placing of cookies of a computer user's hard drive is not an invasion of privacy. Its reasoning was based on the fact that a visit to a web site constitutes communication between the web site and the computer user visiting the web site, and that DoubleClick, Inc. gained legitimate access to the communication when it obtained the authorization of the web site operator, as one of the participants to the communication, to place cookies on the computer user's hard drive.²¹

Perhaps the least transparent manner in which personal information is collected is what has become known as "click-stream data", which internet users carry with them and leave traces of on web sites they visit. As internet users browse a web site, the web site operator may collect information as to the user's IP address, the name of their Internet Service Provider, the type of computer and internet browser used by the internet user and how long they have stayed on the web site in which pages have been visited.

Of course, as technology develops there is an ever-increasing number of less transparent methods by which information can be collected, including e-mail wiretapping and "Web bugs" (tiny hidden images that can embed in Web pages to track users as they surf the Web and read e-mail) which can be used to develop detailed profiles of individual users.

As we will later see, in certain countries which have adopted privacy legislation, the obligations of an organization which collects personal information online will generally increase (from an obligation to inform to an obligation to obtain an implied or express consent) as the transparency of the means of collection of information decreases.

²⁰ *In re DoubleClick Inc. Privacy Litigation*, 2001 WL 303744 (S.D.N.Y., March 28, 2001).

²¹ For a somewhat different treatment of the same issues, see *In re Intuit Privacy Litigation*, 2001 WL 370081 (C.D. Cal. April 10, 2001).

B. U.S. Legislative Framework

The current legislation in the U.S. with respect to online privacy is a patchwork of industry-specific regulation,²² rules protecting certain classes of individuals, and enforcement of published private policies by the Federal Trade Commission (the "FTC") and by state authorities under "mini-FTC" state laws.

In order to better understand where privacy legislation is headed in the U.S., it would be useful to highlight the nature of the current political discussions in the U.S. concerning online privacy. Typically, consumer advocate groups will take the position that the potential for misuse of personal information has become so great that the Government has a duty to intervene to protect its citizens against any unauthorized collection, use or disclosure of such information. Opponents generally point out that that abuses having historically been relatively minor, consisting generally of unwanted e-mail marketing or transfer to third parties for business solicitation purposes²³, and argue that proper business use of personal information relating to consumers' profiles will result in less spam marketing as each business targets its advertising. Opponents also point out that current consumer practices off-line are often more susceptible of abuse (credit card number disclosure by phone, giving a credit card to a waiter, etc.) than online practices.

After much prodding by consumer and privacy advocates, and general resistance by business groups, the conventional wisdom in Washington, D.C. less than a year ago had Congress enacting internet privacy legislation in 2001. Congress seemed to be eager to respond to the general online privacy concerns of American internet users, while being mindful of businesses' desire to use the information for cross marketing and other promotional purposes subject to certain safeguards.

The prospect of inactivity by Congress concerning online privacy leading to various state initiatives on this front also served to focus the minds of business groups. Better to have federal legislation which pre-empts state laws, they reasoned, than having to comply with multiple state initiatives. Some members of Congress were even speculating publicly that the question was not whether, but when, new privacy legislation would be introduced in 2001, and that the debate would center on whether web sites will be required to let users "opt-in" to make personal information available or whether web sites will be allowed to access personal information by default unless users indicate they wish to "opt-out".²⁴

However, recent months have seen a turning of the tide. A lobbying battle began in March 2001, with industry-funded studies showing that proposed restrictions on how companies collect and use personal information would trigger higher prices for internet shoppers and further brake a slowing economy in the U.S. A report on catalogue apparel retailers estimated that companies would need to boost their total mailings to achieve the same number of responses if they were barred from using their consumer information

²² For example, the Gramm-Leach-Bliley Financial Services Modernization Act of 1999, which entered into effect July 1, 2001, the Electronic Communications Privacy Act, and most recently, the Bankruptcy Reform Act of 2001 (s.420).

²³ See, e.g., Joint Survey, *supra* note 118, in which a recent survey found that, of Internet users who claimed that their privacy was violated online, 86% stated they were subscribed to unwanted e-mail marketing and 43% stated that their data was transferred to a third party.

²⁴ Last year, Senators McCain, Abraham and Spencer co-sponsored a bill requiring web sites to ask users if they consent to have personal information collected from them (*i.e.* an "opt-in" choice). While the bill was not adopted into law, it may be resurrected this year as a "middle of the road" approach, which may garner the support of business groups, perhaps with an "opt-out" choice.

databases to tailor their marketing initiatives to the most promising consumers. This study, by the Privacy Leadership Initiative²⁵ and the Direct Marketing Association²⁶, estimated that companies would have to raise prices by \$1 billion if they could not use consumer information for marketing purposes. Another study, funded by over 90 banks and financial services firms, estimated that privacy proposals would cost those 90 institutions \$17 billion per year in additional expenses, with customers having to absorb a \$1 billion "information tax"; the study cited mortgage discounts to customers who have their mortgage and current accounts with the same bank, as an example of a benefit that could disappear. The studies also said that tougher privacy laws may increase the risk of fraud and restrict available consumer credit, for example by barring an internet retailer from verifying address information with a credit company.

In addition, an industry coalition including IBM, Ford and Procter & Gamble has announced it is planning a \$30 million national advertising campaign for the fall of 2001 aimed at easing privacy concerns of consumers. The Online Privacy Alliance²⁶, another industry coalition of large corporations such as Time Warner and Verizon, is lobbying legislators to give them more time to regulate themselves.

Finally, claims that adopting legislation to regulate online privacy would unfairly single out e-commerce as compared to traditional sales have also contributed to a growing sense of Congressional grid lock on this issue. In the current climate, there remains considerable uncertainty as to whether comprehensive privacy legislation will in fact be passed in 2001, but continuing public pressure may force some lawmakers to forge ahead in the near future.

In this context, following is a brief review of the existing legislative framework in the U.S. While it is beyond the scope of this paper to review industry-specific legislation, we will nevertheless briefly examine privacy legislation for the protection of children and bankruptcy reform legislation recently passed, with a view to highlighting the different approaches which may be adopted. Finally, we will conclude with an examination of the FTC's role in ensuring compliance by businesses with their own privacy policies and self-regulatory initiatives concerning privacy.

1. Children's Online Privacy Protection Act of 1998

The federal Children's Online Privacy Protection Act of 1998 and the corresponding rules thereunder issued by the FTC ("COPPA"), which became effective on April 21, 2000, protect individually identifiable information collected from children under age 13, any other information that permits the identification or contacting of a child, as well as certain other information collected through cookies or otherwise (including hobbies and other interests).

Anyone who operates (i) a commercial web site or online service directed at children under 13 that collects individually identifiable information from children or (ii) a general audience web site but with knowledge that it collects personal information from children, must comply with COPPA.

²⁵ The Privacy Leadership Initiative is a partnership of CEOs from major corporations, such as IBM, Ford Motor Company, AT&T, Dell, Compaq, Intel, Procter & Gamble and DoubleClick, and various business associations.

²⁶ <http://www.the-dma.org>.

²⁷ <http://www.privacyalliance.org>.

Compliance with COPPA requires, *inter alia*, the placing of a prominent online notice of the type of information that is collected, the manner of use and disclosure of such information, and an undertaking by the operator not to require any child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation.

Compliance with COPPA also requires that the operator must make reasonable efforts (taking into consideration available technology), before personal information is collected from a child, to ensure that notice is given to the child's parents, containing the same information included in the online notice, and to obtain verifiable parental consent for the collection, use and disclosure of the personal information. Parents must be informed that they can review their child's information, ask to have it deleted and may refuse to allow any further collection or use of the child's information.

Currently, the FTC uses a *sliding scale* approach to parental consent in which the required method of consent will vary based on how the operator uses the child's personal information. In other words, if the operator uses the information solely for internal purposes, a less rigorous method of consent is required. If the operator discloses the information to others or makes it publicly available (e.g., through a chat room or message board), a more reliable method of consent is required, such as a fax or signed letter from the parent, taking calls from a toll-free number, accepting and verifying a credit card, etc. If a parent revokes their consent, the operator may terminate the child's right to use the service provided, but only if the relevant information is necessary for the child's continued participation, for example, a message or chat board. The FTC's sliding scale approach will sunset in April 2002, subject to a review planned for October 2001.

However, COPPA regulations include several exceptions that allow operators to collect a child's e-mail address without getting the parent's consent in advance. These exceptions cover many popular online activities for kids, including contests, online newsletters, homework help and electronic postcards. COPPA also provides a "safe harbor" for web sites that comply with various self-regulatory guidelines that are industry-sponsored and FTC-approved.

However, in an interesting turn of events, the United States Court of Appeals for the Third Circuit last year upheld the decision of a district court in the case of *American Civil Liberties Union v. Reno*,²⁸ held that COPPA's reliance on community standards to identify material that is harmful to minors "must lead inexorably to a holding of a likelihood of unconstitutionality of the entire COPPA statute". John Ashcroft, the current Attorney General of the United States, has applied for and obtained leave to appeal to the United States Supreme Court.²⁹

2. Bankruptcy Reform Act

An example of the piece-meal approach to privacy issues is found in the recent federal bill titled "S. 420 Bankruptcy Reform Act of 2001" (the "BR Proposal"), which was approved by the U.S. Senate with an amendment that will in many cases bar companies in bankruptcy proceedings from selling lists of customers' personal data to other companies if the bankrupt company had promised not to share that data in the first place.

²⁸ The decision of the United States Court of Appeals for the Third Circuit is reported at 217 F.3d 162, and the district court decision is reported at 31 F. Supp. 2d 473.

²⁹ *Ashcroft v. American Civil Liberties Union*, U.S. No. 00-1293, certiorari granted May 21, 2001.

This amendment results from the well-publicized case involving Toysmart.com. When Toysmart.com went out of business, its majority shareholder (Walt Disney Co.) planned to sell the customer database to a third party seemingly in violation of Toysmart.com's privacy policies. Following intervention by the FTC, Walt Disney Co. itself purchased and subsequently destroyed the database under a bankruptcy court's order.

In a nutshell, the BR Proposal states that if the "debtor has disclosed a policy to an individual prohibiting the transfer of personally identifiable information about that individual to unaffiliated third parties, and the policy remains in effect at the time of the bankruptcy filing, the trustee may not sell or lease" that personal data. However, there is an important exception, somewhat vaguely worded, which would allow such transfer if the bankruptcy court, after notice and hearing and due consideration of the facts, circumstances and conditions of the sale or lease, approves the sale or lease as not being inconsistent with the bankrupt company's prohibition on personal data transfers.

While the BR Proposal must, at the time of writing of this paper, still be examined by a House-Senate conference committee session to produce a unified bill which will again be voted upon before becoming legislation, it provides an accurate glimpse of the type of piecemeal privacy legislation that has the best opportunity of being adopted in the short term.

3. Federal Trade Commission Act

The Federal Trade Commission Act ("FTC Act") has been used on several occasions by the federal government to ensure that companies comply with their own published privacy policies or statements and do not mislead the public with respect to personal information collected by such companies. This has been achieved by using section 5(a) of the FTC Act, which makes it unlawful for a person to engage in any "unfair or deceptive acts or practices in or affecting commerce". In addition, the FTC Act has also been used against individuals that sent unsolicited commercial e-mail with false reply addresses. However, the FTC Act does not create any private right of action.

A few words are in order with respect to a practice which has been developing in recent years, namely online "profiling" (*i.e.* linking personally identifiable information with internet users' clickstream data or other recorded online behaviour for the purpose of producing targeted advertising) and which seems to have struck a nerve with several public interest groups and the FTC.

The concerns arise from the fact that many banner ads displayed on Web pages are not selected and delivered by the web site visited by a consumer, but by network advertising companies that manage and provide advertising for numerous unrelated web sites and which do not merely supply banner ads, but also gather data through online profiling which is invisible to Web surfers. While often anonymous, in some cases the profiles derived by network advertisers from tracking consumers' activities on the Web may be (and sometimes are) linked or merged with personally identifiable information and with data on the consumers' offline purchases, or information collected directly from consumers through surveys and registration forms.

Last year, for example, several public interest groups requested the FTC to enjoin DoubleClick Inc., which had acquired Abacus Direct Corporation (a company that does research on catalogue buying with over 88 million 5-year buying profiles that contain such personal information as name, addresses and family makeup) from tying personally identifiable information to information collected through DoubleClick's "cookies" and to prohibit web sites from registering their subscribers or visitors in the Abacus database without the websurfers' affirmative consent.

In response to the public's privacy concerns regarding online profiling, the Network Advertising Initiative (NAI), an organization regrouping all of the leading internet network advertisers, was formed in November 1999 and developed a self-regulatory proposal addressing such concerns. Subsequently, the FTC issued a report on online profiling, in two parts in June and July 2000³⁰, which endorse the NAI self-regulatory proposal and calls for Congress to enact legislation to provide privacy protection for consumers with regard to such online profiling practices which would complement the NAI self-regulatory structure by guaranteeing compliance by the 10 per cent of the network advertising industry which are not members of NAI. Meanwhile, NAI members have agreed to put their self-regulatory principles into effect immediately while Congress considers the Commission's recommendations concerning online profiling. Briefly, the NAI self-regulatory proposal address the four information practice principles articulated by the FTC (notice, choice, access, and security) in its reports.

- *Notice*: NAI members must contractually require (and make reasonable efforts to enforce) host web sites to give notice to consumers of profiling activities on such web sites and allow the consumer to opt out of such profiling activities. A "robust" notice, appearing at the time and place of information collection, is required if personally identifiable information is collected; for other information, a clear and conspicuous notice in the host web site's privacy policy is sufficient.
- *Choice*: Consumers will be allowed to decide whether to participate in profiling activities once the required notice has been given. The method in which choice is exercised depends on various factors. For example, opt-out choice is required for prospective uses of personally identifiable information, but opt-in choice is required if previously collected non-personally identifiable data will be linked to personally identifiable information.
- *Access*: Consumers will have reasonable access to personally identifiable information and other information that is associated with personally identifiable information retained by a network advertiser for profiling.
- *Security*: Network advertisers will make reasonable efforts to protect the data they collect for profiling purposes from loss, misuse, alteration, destruction, or improper access.

However, the debate regarding online profiling seems to be far from over. While the FTC has endorsed the NAI principles discussed above concerning online profiling, many consumer advocates feel that these principles do not adequately protect consumer privacy, largely due to (i) the invisibility of online profiling, (ii) the fact that profiles are often associated with personally identifiable information and (iii) the perceived reluctance of previously established self-regulatory bodies to pursue privacy violations committed by companies. Many consumer advocates are of the view that the principles of the 1980 Fair Information Practices of the Organization for Economic Cooperation and Development (OECD)³¹ be adopted into federal legislation in the U.S. As discussed later, many countries (including Canada and the European Union) have adopted legislation which reflect these Fair Information Principles with some adjustments.

³⁰ The two parts of this report may be found online at <http://www.ftc.gov/opa/2000/07/onlineprofiling.htm> and <http://www.ftc.gov/opa/2000/06/profiling>.

³¹ <http://www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm>.

4. State Law

While it is beyond the scope of this paper to review the numerous privacy-related bills pending at the state level dealing with privacy issues, it should be noted that many states have enacted mini-FTC Acts that provide individuals with a private right of action which is absent from the federal FTC Act.

5. Industry Self-Regulation

In addition to specific efforts such as the NAI initiative concerning online profiling practices discussed above, there exist several self-regulatory bodies. Some offer "seal" programs, the most prominent of which are as follows:

- Both TRUSTe³² and BBB Online³³ provide an online "seal of approval" for web sites that meet certain criteria and disclose, *inter alia*, the type of information that is gathered by the web site, how the information will be used and who will receive personal information. Both TRUSTe and BBB Online have dispute resolution procedures, use security measures, provide periodic monitoring and have children's compliance programs.

Other bodies do not offer seal programs, but seek to give consumers sufficient assurances regarding the treatment of their personal information. For example:

- The Online Privacy Alliance³⁴ regroups various companies with significant activities on the Internet. Each member must comply with general privacy guidelines, which require an online operator to: (i) adopt and implement a privacy policy stating what information is collected and how it is used; (ii) give customers the choice to consent to the use of their information when the use is not related to the purpose of its collection; (iii) keep the information secure; and (iv) take steps to ensure that the information is accurate, complete and timely.
- The Direct Marketing Association³⁵ requires that its members adhere to a certain set of guidelines which became effective July 1, 1999 and require, *inter alia*, online notice to customers stating what information is being collected and how the information is being used and give customers the choice to "opt-out" of having their personal information used by third parties.
- The Global Business Dialogue on Electronic Commerce (GBDe)³⁶, which regroups large organizations in the U.S. and throughout the world, has developed Personal Data Protection Guidelines which are represented to be minimum standards for the protection of consumer privacy that can be applied globally.

C. Fair Information Practices of the OECD

Long before internet use became ubiquitous, the OECD³⁷ Council adopted, on September 23, 1980, the Guidelines governing the Protection of Privacy and Transborder

³² <http://www.truste.org>.

³³ <http://www.bbbonline.org>.

³⁴ Online Privacy Alliance, *supra* note 126.

³⁵ Direct Marketing Association, *supra* note 125.

³⁶ <http://www.gbd.org>.

³⁷ Current OECD members include: United Kingdom, Germany, Netherlands, United States, Canada, France,

Flows of Personal Data,³⁸ which have become known as the Fair Information Practices. While these guidelines constitute nothing more than a recommendation, they are of interest because many of the OECD countries have acted on them and adopted legislation which reflect, in material respects, the principles contained in the Fair Information Practices.

The Fair Information Practices comprise eight principles that establish consumer control over the collection and use of personal information. The eight principles may be very briefly summarized as follows:

- *Collection Limitation*: Data collection occurs by lawful and fair means, with the knowledge and consent of the individual to whom it pertains;
- *Data Quality*: Data collected must be relevant and accurate;
- *Purpose Specification*: The purposes for which the information is collected must be specified at time of collection;
- *Use Limitation*: Data must not be used or disclosed for purposes other than those specified at the time of collection;
- *Security Safeguards*: Reasonable measures must be taken to protect data from unauthorized access, use or disclosure;
- *Openness*: Individuals should be readily able to avail themselves of data collection practices and be able to contact the entity collecting the data;
- *Individual Participation*: Ability of the individual to know if information concerning him has been collected, access the information and cause it to be corrected if inaccurate; and
- *Accountability*: The data collector should be held accountable for failing to comply with any of the above principles.

D. European Union Legislative Framework—a U.S. Perspective

In 1995, the European Union (“E.U.”) adopted its Data Protection Directive (95/46/EC)³⁹ (the “Directive”) requiring its Member Countries to bring national laws into conformity by late October 1998. Under the Directive, the Member Countries are required to enact laws to protect personal information and restrict the flow of such data to non-Member Countries whose laws do not adequately satisfy the Directive’s standards. This particular requirement was of immediate concern to the E.U.’s trading partners, including the United States and Canada, who faced the potential disruption of commercial relationships if the protection they afford to personal information are not considered “adequate” by E.U. standards.

Following the Directive’s adoption, the United States and the E.U. began discussions regarding whether the United States’ laws provide adequate protection for personal data

Mexico, Italy, Japan, Sweden, New Zealand, Australia, Hungary, Norway, Austria, Spain, Czech Republic, Iceland, Poland, Belgium, Ireland, Portugal, Denmark, Korea, Switzerland, Finland, Luxembourg, Turkey and Greece.

³⁸ They may be found online at <http://europa.eu.int/comm/internal-market/en/media/dataprot/inter/priv.htm>.

³⁹ It may be found online at http://www.privacy.org/pi/intl_orgs/ec/final_E.U._Data_Protection.html.

gathered from E.U. citizens. These discussions between the E.U. and the U.S. Department of Commerce led to an agreement relating to the protection of E.U. information conveyed to United States companies, which was formally approved on July 27, 2000 by the European Commission as creating a "safe harbor" to the Directive for U.S. companies.⁴⁰ The safe harbor allows U.S. companies to collect personal information about European citizens while complying with strict E.U. privacy guidelines. As at the effective date of July 1, 2001, any transfer of personal information about European citizens to U.S. companies from any countries in the European Union could be stopped unless U.S. companies comply with safe harbor principles.

U.S. reaction to the safe harbor had initially been lukewarm. However, as at the time of writing of this paper, nearly 90 U.S. companies have taken advantage of the safe harbor provisions, including some large multinationals such as Intel, MicroSoft, Hewlett-Packard and Procter & Gamble. The principal reason for continuing concern over the safe harbor seems to be an understandable reluctance to building and maintaining two separate data-collection systems for the U.S. and for Europe. The potentially high costs of maintaining separate systems are obviously an important factor, but the public relations pressure that could flow from U.S. companies complying with stricter standards for E.U. citizens than American citizens may pose a more fundamental barrier.

The costs of, and inherent difficulties in, maintaining separate systems for multinational companies remains the central difficulty posed by international privacy initiatives. Even within the E.U., compliance with the safe harbor principles does not ensure compliance with the national legislation of E.U. Member States in which they are carrying on business. To cite just one example, the privacy legislation in some Member States exempts corporate data from the privacy guidelines, while other national legislation does not. This creates a maze of rules and regulations which makes strict compliance difficult to achieve. As a result of this apparent confusion, the E.U. has funded a data standards group⁴¹ to examine the need for and best approach to achieve standardization between Member Countries of the E.U. on personal data protection issues, in order to ensure that different practices in data protection do not create barriers to efficient trade. This group has produced a draft report on the Initiative for Privacy Standardization in Europe⁴², making concrete proposals to make compliance easier to achieve throughout the E.U., and has scheduled an open meeting early in the fall of 2001 for discussion of the draft report which should be finalized shortly thereafter.

Other uncertainties may also be prompting U.S. companies to adopt a "wait and see" approach; for example, does the Directive even apply to U.S. companies whose web sites are accessed by European citizens and thereby collect personal information in circumstances where such web sites do not use any "equipment" in the Member States to do so? There is disagreement in the E.U. on this issue as a result of a provision of the Directive stating that it will apply to anyone "making use of equipment" within the E.U. for transmitting personal information. Some Member States, such as Britain, tend to view the Directive restrictively, and would likely be of the view that the Directive should not apply in such cases. Others, such as France and Austria, have a more expansive interpretation of the Directive, claiming in effect that anyone who collects personal data from the E.U. has to abide by the Directive, regardless of whether they have a physical

⁴⁰ It may be found online at <http://www.export.gov/safeharbor/> or <http://www.ita.doc.gov/td/ecom/menu.html>.

⁴¹ The European Committee for Standardization/Information Society Standardization System (CEN/ISSS).

⁴² It may be found online in pdf format at <http://www.cenorm.be/iss/iss/projects/dataprotection/ipse/cover.htm>.

office in the E.U. Once again, an E.U. advisory committee of data protection commissioners has been studying this issue and is trying to define what is meant by use of the term “equipment” in the Directive, including whether the placing of an electronic “cookie” on an E.U. consumer’s computer would qualify as “equipment”. In the absence of any concerted position across the E.U., this issue may well be resolved in a different manner before the local courts of various Member States.

Meanwhile, back in the U.S., members of Congress have begun expressing serious concerns about what is perceived to be the “extra-territorial” enforcement of E.U. principles on American companies and about the impact of the Directive on commerce and trade. Their concerns are fueled by the fact that several Member States⁴³ still have not implemented the Directive in their national laws. Further doubts were raised by a report⁴⁴ by Consumers International, a UK-based group of 263 consumer organization in more than 100 countries, which found that many E.U. web sites do not comply with the Directive and that most popular U.S. web sites were more likely than E.U. sites to give users choices about joining company mailing lists or having information passed on to third parties.

As a final comment before looking at the safe harbor principles in greater detail, it should be noted that there are other means available to U.S. companies for the purpose of complying with the Directive. U.S. companies who operate in only one Member State may choose to negotiate an agreement with that State’s data protection commissioner to ensure appropriate data protection. European companies transmitting personal information to the U.S. may also include privacy safeguards in their contracts with the U.S. companies receiving the information.

In this regard, the European Commission has developed “standard clauses”⁴⁵ which would be contractually imposed on U.S. companies to ensure that European companies could continue to transmit personal data to U.S. companies which have not adhered to the safe harbor principles. But even this initiative has created further controversy: earlier this year, the U.S. Commerce and Treasury Departments wrote to a top European Commission official to complain that the proposed clauses would impose unduly burdensome requirements which are incompatible with real-world operations and that uncertainty about the use of contracts would result from their application. It was also reported that the U.S. has requested that implementation of the rules be delayed in respect of financial institutions in order for further discussions to occur. The initial reaction of a spokesman for the European Commission was that the U.S. letter appeared to be based on a total, complete and utter absence of understanding of the fact that the Commission is aiming to make it easier for companies transferring data from the E.U. to countries outside the E.U. by clarifying the provisions in contracts which would best ensure adequate protection of personal data.

Regardless of the current policy disagreements, the safe harbor principles remain in place and must be understood by anyone who wishes to obtain personal information relating to European citizens.

⁴³ At the time of writing of this paper, France, Germany, Ireland and Luxembourg still have not complied, although each of their Parliaments is considering draft legislation.

⁴⁴ The press release of Consumers International, and accompanying links to the report, may be found online at <http://www.consumersinternational.org/news/pressreleases/privacy250101.html>.

⁴⁵ The standard clauses proposed by the European Commission may be found online in pdf format at http://europa.eu.int/comm/internal_market/en/media/dataprot/news/.

A few general remarks are in order before reviewing the safe harbor principles:

1. Safe Harbor: General Overview

The safe harbor principles are comprised of certain principles, which we will examine briefly, and a Frequently-Asked-Questions on self-certification (collectively, the "Safe Harbor Principles").

The Safe Harbor Principles are intended solely for use by U.S. organizations receiving personal information from the European Union for the purpose of qualifying for the safe harbor from the Directive and the presumption of "adequacy" it creates. Most Member States have adopted privacy legislation which must be complied with if a U.S. organization does more than simply receive personal information from the European Union including, without limitation, collecting, using or disclosing personal information while carrying on business in such Member State.

Other key issues to retain are that decisions by U.S. organizations to qualify for the safe harbor are entirely voluntary, and an organization's failure to self-certify in accordance with the Safe Harbor Principles does not mean it does not provide effective protection for personal information or that it does not qualify for the benefits of the safe harbor; in fact, organizations may qualify for the safe harbor in different ways, as will be seen later. Organizations that decide to adhere to the Safe Harbor Principles must comply with them in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so.

For example, if an organization joins a self-regulatory privacy program that adheres to the Safe Harbor Principles, it qualifies for the safe harbor from the Directive. Organizations may also qualify by developing their own self-regulatory privacy policies provided that they conform with the Safe Harbor Principles. However, where in complying with the Safe Harbor Principles an organization relies in whole or in part on self-regulation, its failure to comply with such self-regulation must also be actionable under section 5 of the FTC Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts. In addition, organizations that are subject to a statutory, regulatory, administrative or other body of law (or of rules) which effectively protects personal privacy may also qualify for the safe harbor from the Directive.

In all cases, E.U. safe harbor benefits are assured from the date on which each organization wishing to qualify for the safe harbor from the Directive self-certifies to the U.S. Department of Commerce (or its designee) its adherence to the Safe Harbor Principles in accordance with the guidance set forth in the Frequently Asked Question on Self-Certification. This self-certification must be reaffirmed annually.

An organization that wishes to extend safe harbor benefits to human resources personal information transferred from the E.U. for use in the context of an employment relationship must indicate this when it self-certifies to the U.S. Department of Commerce (or its designee) and conform to the requirements set forth in the Frequently Asked Question on Self-Certification. As mentioned earlier in this paper, organizations will also be able to provide the safeguards necessary under the Directive if they include the Safe Harbor Principles in written agreements with parties transferring data from the E.U. for the substantive privacy provisions.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities.

2. Safe Harbor Principles

The Safe Harbor Principles define “personal data” and “personal information” as data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the E.U., and recorded in any form.

The Safe Harbor Principles can be broken down into seven distinct principles, as follows:

- *Notice*: When individuals are first asked to provide personal information to an organization, the organization must inform such individuals, in clear and conspicuous language, about: (i) the *purposes* for which it collects and uses information about them, (ii) *how to contact* the organization with any inquiries or complaints, (iii) the *types of third parties* to which it discloses the information, and (iv) the *choices and means the organization offers individuals for limiting* its use and disclosure. If this cannot be done at the time of collection of the information, disclosure must be made as soon as practicable thereafter, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.¹⁴⁵
- *Choice*: Generally, an organization must offer individuals conspicuous, readily available, and affordable mechanisms to choose (opt out) whether their personal information is to be: (a) disclosed to a third party or (b) used for a purpose that is incompatible with the purpose for which it was originally collected or subsequently authorized by the individual.

However, for sensitive information (*i.e.* personal information specifying racial or ethnic origin, medical or health conditions, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), individuals must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of the opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

- *Onward Transfer*: In order to disclose information to a third party, organizations must apply the Notice and Choice Principles. However, where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it first either: (i) ascertains that the third party subscribes to the Safe Harbor Principles or is subject to the Directive or another adequacy finding or (ii) enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Safe Harbor Principles. If the organization complies with these requirements, it will not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

⁴⁶ It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform tasks on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

- *Security:* Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.
- *Data Integrity:* Consistent with the Safe Harbor Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
- *Access:* Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
- *Enforcement:* Organizations must include mechanisms for ensuring compliance with the Safe Harbor Principles, recourse for any individual to whom the data relates that is affected by non-compliance with the Safe Harbor Principles, and consequences for the organization when the Safe Harbor Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Safe Harbor Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Safe Harbor Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

E. Canadian Legislative Framework

On January 1, 2001, the Personal Information Protection and Electronic Documents Act (the "Canadian Personal Information Act") came into effect in Canada, being the culmination of several years' worth of efforts by the Canadian government, academics, consumer advocate groups and business groups to develop privacy legislation acceptable to those involved in the process. The Canadian Personal Information Act incorporates, as one of its schedules, the Canadian Standards Association's Model Code for the Protection of Personal Information, which was developed by business groups in their own consultative process, and is largely based on the 1980 Fair Information Practices of the OECD reviewed earlier in this paper.

In order to grasp the extent and scope of the Canadian Personal Information Act, the following terms must be explained:

"personal information" includes any factual or subjective information, recorded or not, about an identifiable individual—for example (i) the name, age, ID numbers, income, ethnic origin, or blood type of an individual, (ii) the opinions, evaluations, comments or

social status of an individual, or (iii) disciplinary actions, employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs). However, personal information does *not* include the name, title, business address or telephone number of an employee of an organization.

“commercial activity” means any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund-raising lists.

“consent” is a voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

“use” refers to the treatment and handling of personal information within an organization, while “disclosure” means making personal information available to others outside the organization.

1. Gradual Implementation

The Canadian Personal Information Act is being implemented over the course of three years as follows:

January 1, 2001: In its first stage, the Act applies to personal information (except personal health information) that is collected, used or disclosed in the course of commercial activities by federal works, undertakings and businesses, including personal data about their employees. This includes, but is not limited to, federally-regulated organizations such as banks, telecommunications and transportation companies.

In addition, at this stage the Act applies to disclosures of personal information *for consideration* across provincial or national borders, by organizations such as credit reporting agencies or any organization that leases, sells or exchanges mailing lists or other personal information. The information itself must be the subject of the transaction and the consideration must be exchanged for the information.

January 1, 2002: At this stage, the Canadian Personal Information Act will extend to personal health information for the organizations and activities covered in the first stage. Personal health information is defined as information about an individual's mental or physical health, including information concerning health services provided and information about tests and examinations.

January 1, 2004: Finally, the Canadian Personal Information Act will extend to the collection, use or disclosure of personal information in the course of any commercial activity *within* any province. However, the federal government may exempt organizations and/or activities in provinces that have adopted substantially similar privacy legislation. The Act will also apply to all personal information in all interprovincial and international transactions by all organizations subject to the Act in the course of their commercial activities.

Quebec is the only province that currently has legislation dealing with personal information in the privacy sector. The federal government of Canada has stated that this legislation meets the test of substantial similarity and that organizations and activities subject to the Quebec legislation will be exempted from the application of the Canadian

Personal Information Act for intraprovincial matters within the Province of Quebec. These matters would otherwise have been subject to the Canadian Personal Information Act on January 1, 2004. Other provinces and territories are currently considering privacy legislation governing the private sector.

2. Privacy Guidelines

As a starting point, it is important to note that under the Canadian Personal Information Act, collection, use and disclosure of personal information must be limited to purposes that a *reasonable person* would consider appropriate in the circumstances. While somewhat vague, this principle imposes an absolute limit against indiscriminate collection of personal information which may be irrelevant to the transaction at hand.

As mentioned earlier, the Canadian Personal Information Act adopts the Canadian Standards Association's Model Code for the Protection of Personal Information as Schedule 1 to the Act. The model code lists the following 10 principles of fair information practices, which form the ground rules for the collection, use and disclosure of personal information in Canada:

a. Accountability: Organizations are required to be accountable for their information practices. In particular, organizations must: (i) comply with all 10 principles contained in Schedule 1 of the Act, (ii) appoint an individual (or individuals) to be responsible for the organization's compliance, (iii) protect all personal information held by it or transferred to a third party for processing (e.g. by imposing contractual obligations to provide a comparable level of protection) and (iv) develop and implement personal information policies and practices.

b. Identify, Document and Disclose Purposes: Organizations must identify the reasons for collecting personal information no later than at the time of collection. In particular, organizations must: (i) identify and document in its files the purpose for which such information is needed and the manner in which such information will be used, (ii) inform the individual from whom the information is collected the purpose for which such information is needed, and (iii) identify any new purpose for the information and obtain the individual's consent before using it. These obligations generally correspond to the Notice requirements under the 1980 Fair Information Practices of the OECD.

c. Inform and Obtain Consent: Organizations must inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data and obtain the individual's consent no later than at the time of collection, as well as when a new use for such information is identified. The form of consent should take into consideration the reasonable expectations of the individual, the circumstances surrounding the collection and the sensitivity of the information collected.

An important rule of thumb is to obtain express consent (similar to the "opt-in" choice in the U.S.) whenever personal information may be considered sensitive. Otherwise, implied consent (similar to the "opt-out" choice in the U.S.) would likely be sufficient.

d. Limit Collection: Organizations must neither collect personal information indiscriminately nor deceive or mislead individuals about the reasons for their collection of personal information. In particular, organizations must limit the amount and type of the information gathered to what is necessary for the identified purposes, and identify in their information-handling policies and practices the type of personal information such organization collects.

e. Limit Use, Disclosure and Retention: Organizations must use or disclose personal information only for the purpose for which it was collected, unless the individual consents or unless the use or disclosure is otherwise authorized by the Canadian Personal Information Act. Personal information must be kept by organizations only as long as necessary to satisfy the identified purposes and, if used to make a decision about an individual, for a reasonable time period to allow the individual to obtain the information after the decision and pursue redress. Consequently, organizations must destroy, erase or render anonymous personal information that is no longer required for an identified purpose or a legal requirement.

f. Accuracy: Organizations must keep personal information as accurate, complete and up to date as is necessary for the purposes for which it is used, taking into account its use and the interests of the individual, and so as to minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

g. Safeguards: Organizations must protect personal information, regardless of the format in which it is held, by security safeguards appropriate to the sensitivity of the personal information it keeps. In particular, organizations must protect the information against loss or theft and from unauthorized access, disclosure, copying, use or modification.

h. Openness: Organizations must make available to individuals, without unreasonable effort on their part, generally understandable information about its policies and practices for the management of personal information, and make these policies and practices generally understandable. In particular, the following information must be made available: (i) the name or title and address of the person in the organization who is accountable for its privacy policies and practices, and to whom requests for access to personal information should be sent, (ii) the means by which an individual can gain access to his or her personal information, (iii) brochures or other information that explain the organization's policies, standards or codes and (iv) a description of the type of personal information made available to related organizations (such as subsidiaries).

i. Individual Access: When requested, organizations must inform individuals of the existence, use or disclosure of any personal information about them and, subject to certain limited exceptions, give such individuals access to their information. Organizations must also correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient, and provide a copy of the information requested, or reasons for not providing access, and advise third parties where appropriate.

In particular, organizations must respond to access requests as quickly as possible and no later than 30 days after receipt of each request, subject to certain exceptions.

j. Challenging Compliance: Organizations must develop simple and easily accessible complaint procedures and inform complainants of avenues of recourse, including their own complaint procedures, those of industry associations, regulatory bodies and the Privacy Commissioner of Canada. Organizations must investigate all complaints received, correct any inaccurate personal information and take appropriate measures to correct information handling practices and policies.

3. Provincial Privacy Legislation

Once again, it is important to note that each province may adopt its own privacy legislation; in fact, the three-year hiatus before the application of the Canadian Personal Information Act to the collection, use or disclosure of personal information within a

province is meant to encourage the provincial adoption of privacy legislation. While the Province of Quebec is currently the only one which has done so to date, the Province of Ontario is evaluating draft legislation in this respect and a number of other provinces are currently studying the possibility of doing so. In particular, there are serious reservations about the constitutionality of the Canadian Personal Information Act with respect to personal information which is collected, used or disclosed solely within the boundaries of one province.

Of course, provincial legislation will add one more layer of obligations for organizations collecting personal information in Canada, but most provinces are considering legislation which would substantially conform to the Canadian Personal Information Act or the 1980 Fair Information Practices of the OECD.

VI. Conclusion

The world is becoming ever smaller through use of the Internet. As this occurs, tensions inevitably develop, in the relationship between online and offline businesses, properties and cultures, and in the clash of disparate laws and sensibilities. Franchisors pursuing an e-strategy for their businesses must be aware of these tensions, how they can impact their businesses and how they can best be addressed to avoid adverse results. While this paper has surveyed some of the most significant internet issues affecting franchising, franchisors should remain alert to developments and be sensitive to the myriad other issues shaping the ongoing evolution of the law and business practices affecting e-commerce.