Franchising and the Internet

Robin Bynoe
Lee Plave

1 OVERVIEW

It is a truism that business worldwide has been transformed by the Internet, particularly over the last ten years. Franchising too has been affected by the Internet. See chapter 9 for some examples of precisely how.

This chapter will address, in a small way, some of the issues pertaining to how franchisors and franchisees used the internet. No one chapter could capture all such issues; indeed, neither could a single volume or a series of volumes. However, we will attempt to illuminate some of the most common and important issues facing franchise systems.

Introduction

Internationalism is inherent in the nature of the Internet – whether in advertising, e-commerce sites, or otherwise – because the medium is borderless. Consumers can contact any website, conduct business, anywhere in the world. The only limitations are those that are practical (*e.g.*, it is difficult to render many services in a remote transaction) and those introduced by law (*e.g.*, those that limit the sale of certain products, impose taxes, or otherwise make a transaction more difficult). Laws that impact e-commerce may also include the law of a jurisdiction that forbids a particular contact or particular trade, or it may be the legal terms that the proprietor of the website imposes in its terms and conditions. These laws frame the context in which businesses operate, online as well as in the "real world," and have a significant impact on businesses, whether or not they consider themselves to be engaging in online commerce.

For example, while some businesses may consider themselves to be heavily reliant on the internet for direct e-commerce, such as the sale of goods or services (consider the online reservation systems used by many companies in the hospitality and travel business), others may focus less on the internet but nonetheless rely upon the medium in different ways (for example, websites that drive traffic to conventional bricks-and-mortar locations, or that help consumers find store locations).

Different Legal Approaches to the Internet

In some instances, the law of the internet (such as it may be) reflects conceptual differences among different societies, especially on matters pertaining to what is described as "free speech," which can sometimes clash with deeply-felt beliefs as to the concepts of privacy and defamation.[1] A recent article published in The New York Times contrasted Google's regulatory challenges in China and the EU thusly: "Google has a problem in China. But it may have bigger headaches in Europe. On issues as varied as privacy, copyright protection and the dominance of Google's Internet search engine, the company is clashing with

[1] See, e.g., Adam Liptak, *When American and European Ideas of Privacy Collide*, The New York Times, p. WK1 (Feb. 28, 2010).

lawmakers, regulators and consumer advocates. And the fights are escalating across Western Europe."[2]

The clash between freedom of the "press" on the one hand and privacy on the other is further highlighted by the February 2010 decision of an Italian court convicting three Google executives of violating the privacy rights of an Italian boy who was depicted in a video that third parties uploaded to You Tube (which Google later purchased) before it was removed, two months later.[3] Because the internet is a global medium, website consent ostensibly meant to be read in one country can easily be seen and downloaded in another, and in many countries, a defamation case may be heard against the author.[4] In commercial terms, that highlights the need for careful planning as to the content and direction of a website.

Franchising Best Practices.

The usual structure for franchising is that the franchisor splits its market geographically among different franchisees, developers, and master franchisees. A master franchisee typically will also sub-divide its territory among different sub-franchisees. To a degree, these territorial divisions run counter to the unbounded nature of the Internet. For example, if a customer can place an order with any provider of the franchised system's goods or services, no matter where in the world, how might that impact affect the territory granted by a franchisor to a particular franchisee?

This consideration is more critical in relation to some franchised goods or services (for example remote sales requiring delivery by post or courier) than others (such as fast-food restaurants or the provision of local services). Nonetheless, due consideration must be given to the creation of one or more websites for the brand.

Consider as well that the hallmark of franchising has been, and continues to be, uniformity. The franchisor's mark must stand for a particular level of quality in terms of service, products, and the overall customer experience. Franchisors and franchisees strive to deliver on the promise of the mark and accomplish the same goal – providing each customer the best experience – in the "real world" consistent with the uniform standard that the franchisor has set for the franchise system. The internet presents challenges to accomplishing the same goal online.

---

2 Eric Pfanner, *In Europe, Challenges for Google*, The New York Times, p. B1 (Feb. 2, 2010).

3 Nick Pasa, *Google Italy ruling threat to internet freedom*, The Daily Telegraph (posted Feb. 24, 2010) (available at http://www.telegraph.co.uk/technology/google/7308384/Google-Italy-ruling-threat-to-internet-freedom.html).

4 Compare Dow Jones & Company v Gutnick, (2002) 210 CLR 575 (High Court of Australia determined that content downloaded in Australia gave rise to defamation claim there in case involving an article published in The Wall Street Journal) with ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707 (4th Cir. 2002), cert. denied, 2003 U.S. LEXIS 596 (U.S. Jan. 13, 2003). In ALS Scan, the Court of Appeals noted that "a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts. Under this standard, a person who simply places information on the Internet does not subject himself to jurisdiction in each State into which the electronic signal is transmitted and received. Such passive Internet activity does not generally include directing electronic activity into the State with the manifested intent of engaging business or other interactions in the State thus creating in a person within the State a potential cause of action cognizable in courts located in the State." 293 F.3d at 714. The ALS Scan decision adapted the logic of the leading doctrine, the so-called Zippo continuum, which has been applied to many cases determining whether personal jurisdiction exists in cases involving, principally, internet contacts. Zippo Mfg. Co. v. Zippo DOT Com, 952 F. Supp. 1119 (W.D. Pa. 1997).

Generally speaking, the best practice for franchisors is to have a single unified website for the brand to serve each different "market." (For this purpose, a "market" can be seen differently by different people, but for many businesses, each country comprises a separate market due to legal differences, language and cultural considerations, and other practical issues, as explained below.) This approach, gives each franchisee in the territory a webpage within the franchisor's website, so that there is information about that franchisee and its offerings subsumed within the franchisor's main site. One of the authors of this article previously coined this to be the "Full-Monty" approach.

One of the considerations that a franchisor must face is whether to permit its franchisees to use the web independent of the franchisor. In general, doing so invariably leads to inconsistency, in terms of the content, look and feel, and legal approach taken to the presentation of information to consumers. This, of course, runs precisely opposite to the goal of uniformity that franchisors and franchisees alike seek to accomplish to develop and enhance (as well as reap the benefit of) a strong common brand. Here, the "Full Monty" approach gives each franchisee a chance to be seen online, yet it does not dilute the systemwide uniformity that is essential to most franchise networks, as illustrated below.

In strategic terms, the following four models for operating websites illustrate how most franchise networks approach franchisees' use of the Internet:

I. *"Wild Wild Web"* - The franchisor allows its franchisees to establish their own websites and domain names, essentially placing no restrictions on the franchisees' use of the Internet.

II. *"The Luddite Option"* - The franchisor prohibits its franchisees from using the Internet or websites in any manner relating to the franchised business or the franchisor's trademarks.

III. *"Same Old Same Old"* - The franchisor treats franchisee use of the Internet and websites as advertising, thus allowing franchisees to use the web and create websites, provided that the sites and materials are submitted to the franchisor for review in the same way as with submission of traditional advertising, such as proposed newspaper advertisements.

IV. *"The Full Monty"* - The franchisor establishes one network-wide website for each market, and provides all of its franchisees with a webpage on that website.

Options I and II are unattractive models for franchisors and franchisees alike. Unrestricted use of the Internet will almost certainly lead to inconsistency in the "look and feel" of the websites, thus damaging the public's perception of the network's uniformity. Also of primary concern are the risks of legal attacks on the franchisor's trademarks for failure to exercise control over the trademarks, claims of franchisee encroachment, and network-wide unrest. At the opposite extreme, a blanket prohibition on franchisees' use of the Internet may be unrealistic.

Option III initially appears to be a workable model, especially from an initial cost perspective, because each participant bears its own costs. On further analysis, however, this model reflects many flaws, some of which have significant implications, such as difficulty in maintaining uniformity and in effectively updating the various websites and coordinating domain names, and the potential for display of inappropriate materials. Moreover, leaving franchisees to develop their own websites independently increases the likelihood that the franchisee will, inadvertently or otherwise, fail to comply with the various legal requirements that are inherent in such a venture.

While Option IV (The Full Monty) may be initially more expensive, the costs are usually marginal and protect against the risks associated with the other models, and affords the franchisor – and the entire franchise network – greater ability to respond quickly to changes in the markets. As to cost issues, the overall expenditures required for Option IV may not be very high when compared to the collective (and arguably wasted) expenditures of the franchisees as each "reinvents the wheel" when developing individual websites. Additionally, depending on the terms of the relevant franchise agreements, the network-wide advertising fund may be able to cover some or all of the website development costs.

Conclusion: Option IV – the Full Monty Approach – is the preferable model in most franchise systems, particularly when implemented as part of an overall technology strategy.

Various tactical considerations can be accomplished with a single website for the brand in each market (as contrasted with a website operated by different stakeholders, such as different franchisees in each market). Among these are:

- First, franchisors developing an Internet presence for their franchise network should strive to create and maintain a uniform "look and feel" for all websites associated with the network. Inconsistencies in the "look and feel" of a network's websites may damage the public's general perception of the network's uniformity, which is a hallmark of any franchise network. From a legal perspective, lack of uniformity may dilute the franchisor's trademarks, or lead to claims that content on non-franchisor controlled websites violate another party's intellectual property rights.

- Second, franchise networks will benefit from using a model that allows for easy updating of the information circulated to the public via the Internet (such as seasonal promotions, product changes or franchisee information).

- Third, it is important that the franchisor have a coordinated approach to the registration and maintenance of domain names; this strategy protects the entire network against both the stockpiling of valuable domain names by a rogue party and legal attacks upon the franchisor's trademarks by unlicensed users.

- Fourth, coordination of Business-to-Customer ("B2C") e-commerce, both with respect to the offering of products and services and the fulfilment of customer orders, will likely be essential to the success of any e-commerce program and the long-term health of the franchise network in general. Failure to fulfil orders properly and promptly is one of the leading reasons that some e-commerce businesses have failed. In addition, such failures may prompt FTC charges that the franchisor violated the FTC's Mail Order Rule, 16 C.F.R. Part 435.

- Fifth, franchise companies should structure the websites and webpages so that potential customers will obtain readily useable search results when searching the Internet for their franchise network or outlets. Franchisors should remember that while the Internet offers rapid access to a wealth of information, their mere presence on the Internet will not prove worthwhile unless their websites can be easily found.

- Sixth, franchisors and franchisees alike should focus on delivering to the customer the best possible online presence that is consistent with the goal of presenting the best possible in-store (or in-person) experience and/or products. This goal is difficult to achieve unless the franchise company implements comprehensive web policies.

In each instance, notwithstanding that there may be a franchisee, master franchisee, or developer for the brand in a particular country, the franchisor is still the party that should

have ultimate control over the brand site in that market. Appropriate provisions should be inserted into the relevant agreements to vest these controls with the franchisor. At the very least, these provisions should address matters such as selection and registration of domain names, a policy regarding use of the web by the master franchisee and its subfranchisees, a social media/networking policy, an e-commerce policy, web development issues (e.g., what party owns the copyrights in the website content), and other technology issues. Even where there is a different website for each market, the websites can be coordinated by the franchisor and have a consistent look and feel from one market to the next.[5]

***What is a Market*?**

As for how to define each "market," it seems that there are some obvious reasons why different countries require a different website. For example, there are different languages, consumer preferences, cultural issues (e.g., photos of customers that include men and women together may not be as favourably received in some countries as in others, and stylish photos of customers in one country may be seen as out of touch in other parts of the world), and, finally, legal requirements. Even where a common language is employed, a single site using the same language (e.g., English) may not be appropriate for customers in Australia, Canada, England, Ireland, and the U.S. – given different tastes, customer expectations, currency for payment, and the like.

Domain name considerations also apply. Consumers in local markets may prefer to visit websites with country-code TLDs (ccTLDs) – such as *.ca* for Canada, *.uk* for the United Kingdom, *.jp* for Japan, *.au* for Australia – which are available through the registrars for each ccTLD. A study released in 2001 by the Canadian Internet Registration Authority (CIRA) found that over 70% of Canadians would prefer to shop online at a website that uses the *.ca* ccTLD, which indicates that the merchant is Canadian, rather than the generic *.com* gTLD.[6]

Jurisdiction issues also militate in favor of separate websites for each country. A website designed for use by customers in just one country may use pull-down boxes with address choices and currency options that make it clear the site is intended for use in just one country. That, among other factors, may make it less likely that the operator of the site will be deemed to nonetheless be doing business elsewhere, which could lead to being haled into court in another country because the site was seen there and interacted with by consumers in that country. For example, a Japanese-language website meant to serve customers in one country (e.g., Japan) may be of interest to customers in another country (e.g., Brazilians of Japanese descent, where there is a large Japanese community) who speak the same language.[7] Appropriate terms of use can help to limit exposure to claims

---

[5] An outstanding example can be found in the different websites maintained by Marriott International, Inc. for consumers who live in different countries. A visit to Marriott.com (US), Marriott.ca (Canada), Marriott.fr (France), Marriott.com.cn (China), Marriott.jp (Japan), and Marriott.com.au (Australia) will reveal a common approach to virtually all elements of the website, yet compliance with local requirements pertaining to consumers in different countries – because the websites offer roughly the same service (rooms at hotel properties located worldwide). In contrast, the websites maintained for the "McDonald's" franchise system in different markets are substantially different – precisely because the offering – a product served locally – differs from country to country.

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

[7] While not all countries subscribe to the reasoning in the ALS Scan and Zippo cases, described supra, the logic of those decisions makes a degree of sense and may be persuasive in other settings. For example, the US Court of Appeals declined to exercise jurisdiction in a case where a website originating from Spain did not appear to have been designed or intended to reach customers in New Jersey, and the court noted that the websites were entirely in Spanish, the prices for its merchandise were in Pesetas or Euros, the merchandise could only be shipped to addresses within Spain, and U.S. addresses were not accommodated. Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d at 454. A different outcome based on consistent reasoning was reached in Euromarket Designs, Inc. v. Crate & Barrel Limited, 96 F. Supp. 2d 284 (N.D. Ill. 2000) (and as otherwise discussed in the text with

made by remote viewers of the site, and also make clear that the franchisee (not the franchisor) is the party providing the goods or service to the customer (where that is the case).

Franchise Territorial Issues in the Age of the Internet

Franchisors and franchisees are generally free to contract on issues pertaining to technology in the United States. Agreements should expressly contemplate and permit e-business, and it is even more important to carefully consider (and, where appropriate, avoid) exclusive arrangements that could preclude e-business and other developments. This is particularly so in the case of franchise agreements, given the length of time that franchise agreements last, as these arrangements commonly have terms that run from 20-40 years. Agreements of that length mean that the parties must implement a relationship and structure that will last long after the bounds of any realistic understanding as to what technology will be applied and how the "internet" will function in the short- and longer-term future (consider how archaic 10- and 15-year old technology seems at any given point in time).

Granting territorial "exclusivity" without accounting for the possibility of e-business may be particularly short-sighted in long-term franchise transactions. Among other things, territorial restrictions may be difficult to enforce. For example, if a distributor is authorized to sell the products in a specified territory and that distributor establishes an e-commerce website in the territory that is also accessible to customers outside the territory (which of course is inevitable), potential problems exist without regard to whether the territory is an "exclusive" or "non-exclusive" territory.[8]

By now, most franchise companies have already discovered the value of the Internet as an effective tool for promoting their systems, communicating efficiently with their franchisees and suppliers, and in some instances, capitalizing on the opportunities presented by "e-commerce" - the selling of goods and services on the Internet. Other franchisors, however, remain in position to only evaluate their options. The emergence of social media and social networking sites as substantial commercial online venues has considerably changed the dynamic and added urgency to the need for a proper structure as to the franchise relationship – including agreement terms – relating to the internet and technology matters.

General Notes

As chapter [ ] suggests, of course, many of the advantages brought by the Internet in franchising concern the relationship between the franchisor and the franchisee more than the relationship of either with the customer. For example, the franchise agreement may provide for an intranet operated by the franchisor through which all reporting can be done by the franchisee and which incorporates what used to be the paper-based operations manual, with the intranet being updated instead of loose-leaf pages being replaced. These

---

respect to the parallel UK case, Euromarket Designs Incorporated v. Peters & Anr, [2000] EWCH Ch 179)). In the U.S. case, the defendant's website originally allowed U.S. customers to enter their address. After initiation of the lawsuit, the website bore the statement "Goods Sold Only in the Republic of Ireland" on its opening page and expressed prices in Irish pounds. However, users of defendant's website could still ship and bill orders to U.S. addresses. The federal court noted that the billing address information fields on defendant's website were clearly organized for U.S. formatted addresses.

[8] See, e.g., Travel Impressions, Ltd. v. Kaufman, 1997 U.S. Dist. LEXIS 23217 (E.D.N.Y. 1997) (reprinted at Bus. Franchise Guide (CCH) ¶¶ 11,470 and 11,471) (court denied injunction against franchisee's use of the internet as medium for marketing to customers within a portion of Manhattan; unclear whether that use of the franchisor's marks was prohibited or permitted under the franchise agreement).

techniques do not affect the relationship between franchisor or franchisee and the customer and do not require further consideration in this chapter.

We will deal with a number of such areas commenting on them from the perspective both of Europe and the United States. Entire books have been written about many of these topics and we shall take it as our task to draw attention to them rather than give a definitive account of them.

2 THE WEBSITE AND THE BRAND

When content is placed onto a website, it almost always can be seen throughout the world. Even in places where internet access is discouraged or even blocked, in many instances there are ways for people to see a particular site. The purpose of a site relating to a franchise system is to promote the brand that the franchisor owns, that the franchisor licenses to the franchisees, and that both the franchisor and its franchisees hope will be exploited for their common benefit. Therefore, brand strategy and trademark protection are even more important for franchise systems in the internet era.

Brands have two aspects. One is how they work legally, and that essentially brings trade mark law into play. The other aspect is that the brand name stands for the products and services that the franchisor and franchisee offer to their customers. In respect of both, the internet complicates matters. Where a website features a trademark, that mark will be viewable in multiple jurisdictions, and although the mark will be single and unchanging, the legal implications flowing from its use will be diverse.

Franchisors, like all trademark owners, face special challenges as well in terms of timing. Trademark registration applications may take several years to be processed by the applicable government agencies. Moreover, there are many countries with “first-to-file” registration regimes. Consequently, trademark owners are well-advised to develop a strategy for filing trademark registration applications sufficiently in advance of their franchise expansion plans to take these factors into account.

Here, as well, the internet has an impact. A trademark used in one country is often exposed early via the internet, and often before the trademark owner has any designs on expanding into other countries. The internet effect puts an even higher premium on strategizing about when to file trademark registration applications. Many a company has found that its entry into an international market is blocked, or at least complicated, because an “enterprising” local party has seen and applied to register the company’s trademark sooner than the company was able to do so.

The first-to-file regime that applies in some countries in the context of trademark registrations generally applies throughout the world in connection with domain name registrations. Because of the obvious and central role that domain name registrations play to brand usage on the internet, franchisors are well-advised to develop and implement a strategy of early and vigorous domain name registration and enforcement throughout the world.

The Essence of Brands and Trade Marks

Trade marks are essentially national. Trademarks and service marks are typically registered on a country-by-country basis. Just a few examples of government agencies responsible for trademark registration include Australia’s IP Office (a division within the Department of Innovation, Industry, Science and Research), the Canadian Intellectual Property Office (where Canadians register “trade-marks”), the Chinese Trademark Office, the Japanese Patent Office, the U.K. Patent Office (which operates under the moniker “Intellectual

Property Office"), and the U.S. Patent and Trademark Office (part of the Department of Commerce).[9]

There are several multi-national regimes, however, for trademark registrations. These include two in Europe. One of the European regimes is the Community Trade Mark (CTM), which is available in addition to national marks. A so-called CTM registration can be obtained by filing with OHIM – the Office for Harmonization in the Internal Market (the EU's trademark agency), and it applies in all 27 countries within the EU. However, even where a CTM registration is obtained, it will generally be enforced in national courts, and the approaches of national courts to the same Euro-legislation is often startlingly divergent. The second European multi-national system involves a so-called "Benelux" registration, which covers Belgium, the Netherlands, and Luxembourg through a joint registration system covering their three nations, which is administered by the Benelux Office for Intellectual Property.

A third, and most important regime, is a global registration system administered through the World Intellectual Property Organization (WIPO), known colloquially as the Madrid System, or the Madrid Treaty and Protocol.[10] The Madrid System offers a streamlined route to multiple registrations by extending a trademark owner's home-country registration to other countries by means of an expedient and efficient series of national registrations.

Examples of Issues

Let us assume that a mark is a word. That mark may be registered in some jurisdictions and not others. It may infringe in some jurisdictions, because someone else has rights in respect of the mark, and not others. It may infringe in some jurisdictions and not others in relation to particular categories of goods or services, because the scope of the relevant registrations varies.

Just because the word is registered as a trade mark by a franchisor in one or more jurisdictions, and the same word is registered by someone else in other jurisdictions, and the classes of goods or services involved are similar, it does not necessarily follow that the accessibility of the franchisor's website in those other jurisdictions will infringe the rights of those with registrations in those other jurisdictions. The Crate & Barrel case (Euromarket Designs Incorporated v. Peters & Anr, [2000] EWCH Ch 179) is instructive. It concerned Euromarket, part of the American group that owned the well-known chain of shops trading as "Crate & Barrel". Euromarket had registered CRATE & BARREL as a trade mark in the United Kingdom. The defendants ran a small shop in Ireland, also called "Crate & Barrel", and they had a website. The website was in the nature of things accessible in Britain, as well as everywhere in the world, and Euromarket claimed that it infringed Euromarket's rights under its British trade mark registration. The court found otherwise. It concluded that the defendants' purpose in setting up their website was not to drum up trade in Britain or anywhere else outside Ireland, but to promote their Irish shop and to persuade people physically to go to their shop and buy things. So although trade mark use of the CRATE & BARREL mark in Britain would have infringed Euromoney's trade mark rights, this was not deemed to be an offending use - as the use was not aimed at Britain. (Notably, however,

[9] A helpful directory can be found on the WIPO website, at http://www.wipo.int/directory/en/urls.jsp.

[10] The Madrid Agreement Concerning the International Registration of Marks of April 14, 1891 (as revised at Brussels on December 14, 1900, at Washington on June 2, 1911, at The Hague on November 6, 1925, at London on June 2, 1934, at Nice on June 15, 1957, and at Stockholm on July 14, 1967, and as amended on September 28, 1979).

this in an English case, and the approach may vary jurisdiction by jurisdiction. Moreover, it is in the nature of franchises to be international and in the nature of a franchisor's website to assert a world-wide brand. One lesson to be drawn from this case is the importance of securing at the outset a mark that is robust internationally. Another lesson is that franchisors should beware of offering warranties as to the enforceability of their trademarks world-wide, and franchisees should beware of accepting whatever they are offered in that department without independent enquiry.)

Do Brands Always Work Internationally?

We are all familiar with the experience of encountering in some remote territory a brand with which we are thoroughly familiar at home, and finding it different. (One example is the "Church's Chicken" franchise system, which, in some international settings, uses the mark "Texas Chicken".) In some countries with different languages and alphabets, a different mark in the local language is needed (in China and elsewhere in Asia, the Middle East, Greece, and Russian-speaking countries, a phonetic transliteration of the name, a name that conveys the concept of the company's offerings, or a combination phonetic-conceptual name may be needed).

The difference may be subtle, designed to accommodate local prejudices or styles, or it may be blatant, as where the name with which we are familiar means something obscene or hilarious in the local language, and has to be changed, but with the inoffensive substitute still dressed up with the corporate colours and other trappings of the original. Of course the changes, subtle or blatant, will rarely be accidental. The fine tuning will often be the result of many hours of the time of advertising consultants.

With a unified global website, however, no such fine tuning is possible. Not only does the brand have to work universally, but the product as described has to be universally acceptable. No part of the offering may offend any religious or other group, unless they were never likely to want it in the first place. Nothing must look ridiculous or tacky.

Inoffensiveness, combined with a certain obviousness, will therefore be at a premium.

Domain Names

There are various kinds of domain names: (1) generic top-level domains (gTLDs);[11] (2) country-code top-level domains (ccTLDs);[12] (3) internationalized domain name (IDN) ccTLDs (e.g., in a non-Latin alphabet set, such as Arabic, Greek, Mandarin, or Russian);[13] and (4) regional top-level domains (rTLDs).[14] ICANN is also considering allowing private parties to apply for other top level domains under the "new gTLD" program, which would allow for a domain name such as *dot-InternationalBarAssociation* or, for that matter, a

[11] Originally, there were just seven gTLDs: .com, .edu, .gov, .int, .mil, .net, and .org. As of March 2010, there are 21 gTLDs: .aero, .arpa., .asia, .biz, .cat, .com, .coop, .edu, .gov, .info, .int, .jobs, .mil, .mobi, .museum, .name, .net, .org, .pro, .tel, .travel.

[12] ccTLDs are two-letter names, such as .ca (Canada),.de (Germany), .uk (United Kingdom), and .us (United States) and correspond to a particular country. As of March 2010, there were approximately 250 ccTLDs, some of which operate on their own and others of which have derivative extensions, such as .com.au, widely used by Australian businesses.

[13] ICANN is according IDN ccTLDs "fast-track" treatment (ICANN is the Internet Corporation for Assigned Numbers and Names). As of January 2010, applications for four IDN ccTLDs were in process from registries in Egypt, Russia, Saudi Arabia, and the UAE.

[14] These include .eu and .asia.

commercial name such as *dot-CocaCola*. ICANN contemplates that the filing fee for such a domain name registration will be US$185,000.[15]

Franchise companies need to contemplate various factors in deciding how to handle domain names. Among these are: (1) which domain names to register; (2) in which gTLDs, and (3) in which ccTLDs. Complications arise for franchisors because many trade names incorporate characters such as apostrophes that cannot be reproduced in domain names, and some trademarks consist of two or more words – so for example, the name "Acme Coffee" might be registered in the dot-com gTLD without spaces (AcmeCoffee.com) as well as with a hyphen separating the two words (Acme-Coffee.com).

Franchisors, like other trademark owners, may register domain names for "offensive" reasons as well as for "defensive" reasons. Variations on names – e.g., to include obvious and common typographical errors – might be ones that a franchisor ought to register so that it can avoid the prospect of cybersquatters doing so on their own.

One strategy is to consider "cluster registrations." By registering the domain name in all of the most likely-used gTLDs and ccTLDs relevant to the trademark owner's business operations, the company may avoid some confusion and dilution, and may preclude other parties from registering and "squatting upon" important domain names. It may also be prudent to register local misspellings of the company name, the company name and trade name in any of the 76 different non-Latin character sets in which registrations are available,[16] hyphenated versions of two-word marks, foreign language translations, as well as common "nicknames" by which the company is known in the industry (*e.g.*, FedEx, Mickey D).

Companies should also consider whether to acquire widely-used pejorative extensions of their house marks, especially in the marquee gTLDs (such as .com), examples of which would include "Acmesucks.com," "Acmefraud.com," and "Acmebeware.com."

Cybersquatting. In the U.S., domain names can also be protected in the U.S. under the 1999 Anticybersquatting Consumer Protection Act (the "ACPA"). Internationally, domain names can be protected under ICANN's Uniform Dispute Resolution Procedures (the "UDRP"), which apply to virtually all gTLDs and, with some variation, to almost all ccTLDs as well.

In roughly 75-80% of cases brought under the ICANN UDRP process, trademark owners have succeeded in recovering domain names from parties who own infringing domain name registrations.[17] In some cases, these decisions not only cover commercial use, but also "commentary" usage, such as domain names containing a party's trademarks with the suffix "sucks." In a decision handed down in May 2005, a WIPO panel ordered the domain name airfrancesucks.com to be transferred to Air France, concluding that the pejorative connotation of the term "sucks" may be unfamiliar to non-English speakers, and therefore, "a

---

[15] The details can be found at http://www.icann.org/en/topics/new-gtlds/draft-rfp-clean-04oct09-en.pdf.

[16] A domain name registration can be obtained in a TLD using any of 76 different character sets, applying the IDN Language Registry Tables. These range from Greek to Hebrew, Arabic to Kanji (Japanese), and Cyrillic to Chinese, and Swedish to Korean. A complete list can be found at *http://www.iana.org/domains/idn-tables*.

[17] See ICANN statistics, at *http://www.icann.org/en/udrp/proceedings-stat.htm*.

large proportion of internet users therefore are likely to be confused by '-sucks' domain names." [18]

Monitoring domain name use and handling disputes over domain names have proven to be a major issue for most companies. In the U.S., actions can be brought under the ACPA, which took effect November 29, 1999.[19] Under this standard, among other things, the trademark owner must prove that the domain name was registered or used in "bad faith." The statute provides nine examples of the factors that courts may consider in assessing whether or not bad faith is present; these factors are not exclusive and courts may consider other factors as well.[20] The ACPA applies to foreign trademarks used in U.S. commerce[21] as well as U.S. trademarks, both registered[22] and unregistered.[23]

In a successful ACPA action for a domain name that was registered, used, or trafficked in after the Act took effect, the plaintiff can be awarded a transfer of the domain name, statutory damages ranging from $1,000 to $100,000 per domain name infringed, and legal fees.[24] For example, in Electronics Boutique Holdings Corp. v. Zuccarini,[25] the court

---

[18] Societé Air France v. Virtual Dates, Inc., Case No. D2005-0168 (WIPO, May 24, 2005). But see Asda Group Limited v. Kilgour, Case No. D2002-0857 (WIPO, Nov. 11, 2002), a case involving an English-language website concerning a British party, in which the panel determined that language confusion was unlikely: "[B]y now the number of Internet users who do not appreciate the significance of the '-sucks' suffix must be so small as to be de minimis and not worthy of consideration. The Panel notes that the Complainant puts forward no evidence to substantiate that contention. The Panel believes that Internet users will be well aware that a domain name with a '-sucks' suffix does not have the approval of the relevant trade mark owner." See generally NAF Panels Diverge on Proprietary of 'Sucks' Domains in Cases Involving Identical Parties, 10 Electronic Commerce & L. Rep. (BNA) 38, at 963-94 (Oct. 5, 2005).

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

[20] 15 U.S.C. § 1125(d)(1)(B)(i).

[21] See International Bancorp, LLC v. Societe Des Bains De Mer et Du Cercle des Etrangers a Monaco, 329 F.3d 359 (2003); cert. denied, 157 L. Ed.2d 891 (2004) (upholding claim against European casino that advertised in U.S.); Federation Internationale de Football Assoc. v. Cyclelogic Inc., 2004 U.S. Dist. LEXIS 19245 (S.D. Fla. May 13, 2004) (copamundial.com and copadomundo.com).

[22] See, e.g., Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona, 2003 U.S. App. LEXIS 10840 (4th Cir. June 2, 2003) (ACPA and U.S. trademark law apply to dispute involving a claim by the Barcelona city council against two residents of Spain who formed a Delaware corporation (Barcelona.com, Inc.), reversing lower court and UDRP panel); March Madness Ath. Assoc. LLC v. Netfire, Inc., 2005 U.S. App. LEXIS 1475 (5th Cir. Jan. 24, 2005) (upholding transfer of *marchmadness.com*); Nike, Inc. v. Circle Group Internet, Inc., 318 F. Supp.2d 688 (N.D. Ill. 2004) (*justdoit.net*).

[23] See Wal-Mart Stores, Inc. v. Samara Bros., 529 U.S. 205 (2000); DaimlerChrysler v. The Net, Inc., 388 F.3d 201 (6th Cir. 2004).

[24] In Ernest and Julio Gallo Winery v. Spider Webs Ltd., 129 F. Supp.2d 1033, 1047-48 (S.D. Tex. 2001), aff'd, 286 F.3d 270 (5th Cir. 2002), the court awarded statutory damages of $25,000 for violations of the ACPA and the Texas Anti-Dilution Statute. The court noted that even though the domain name had been registered before the ACPA took effect, the defendants (who warehoused nearly 2000 domain names) used and trafficked in the domain name after the ACPA's November 29, 1999 effective date. Id. On appeal, the U.S. Court of Appeals for the Fifth Circuit affirmed, and in doing so rejected the defendants' argument that it was not acting in bad faith because it was holding the domain name to sell it only if the ACPA was declared unconstitutional. Ernest and Julio Gallo Winery v. Spider Webs Ltd., 286 F.3d 270 (5th Cir. 2002); see also Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 265, 268 (4th Cir. 2001) (same). But if the domain name was registered before the ACPA took effect, legal fees may not be awarded under the ACPA. See March Madness Athletic Assoc. LLC v. Netfire Inc., 2005 U.S. App. LEXIS 1475 (5th Cir. Jan. 24, 2005).

[25] 56 U.S.P.Q.2d (BNA) 1705 (E.D. Pa. 2000), motion to set aside denied, 2001 U.S. Dist. LEXIS 765 (E.D. Pa. 2001). See also Victoria's Cyber Secret v. V Secret Catalogue, Inc., 161 F. Supp.2d 1339 (S.D. Fla. 2001) ($120,000 plus legal fees and transfer of four domain names).

assessed the full range of penalties with respect to a repeat cybersquatter, including $500,000 in statutory damages and over $30,000 in legal fees.

The ACPA also provides for the possibility of *in rem* jurisdiction, where the plaintiff cannot locate the domain name registrant (*e.g.*, where the registrant gave incorrect contact information to the registrar or did not update the contact information on file), or where the registrant can be located but is not subject to the *in personam* (personal) jurisdiction of U.S. courts.[26] Under the *in rem* clause, the lawsuit is to be filed against the domain name itself. Jurisdiction is typically in the district where the registrar or registry is located.[27] *In rem* jurisdiction continues to exist once it is determined to be present.[28] The ACPA's *in rem* clause has withstood constitutional challenge.[29]

The decision of whether to challenge a cybersquatter by bringing suit under the ACPA or initiating arbitration under the UDRP typically should be made on a case-by-case basis, taking into account many factors. For a trademark owner to prevail,[30] the trademark owner must establish three elements that: (1) the contested domain name is identical or confusingly similar to a trademark or service mark to which they have rights;[31] (2) the current holder has no rights or legitimate interests in the domain name; and (3) the domain name was registered, and is being used in bad faith.[32] Proceedings under the UDRP are quick and awards are limited to orders that the domain name in question be transferred. While these proceedings are in the nature of arbitration, the terms of the UDRP itself state that a decision rendered under those procedures is subject to judicial review,[33] a conclusion that has been confirmed by U.S. courts.[34] As such, the ACPA may be used to overturn an UDRP decision

---

[26] 15 U.S.C. § 1125(d)(2). See, e.g., Alitalia-Linee Aree Italiane, S.p.A v. Casinolitalia.com, 128 F. Supp.2d 340 (E.D. Va. 2001) (*in rem* case can only be brought if *in personam* jurisdiction cannot be obtained in U.S.).

[27] See, e.g., Mattell, Inc. v. Barbie-Club.com, 2002 U.S. App. LEXIS 23149 (2d Cir. 2002).

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

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

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

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

[32] In a case involving non-use, and mere registration of a domain name, an ICANN panel deemed the registration tantamount to bad faith under the UDRP where the registered name was widely know (here, the name Mario Lemieux, a NHL Hall of Fame player), there was no showing that the registrant made a good faith use of the name, nor did the registrant make any demonstrable legitimate use of the name. Lemieux v. Creato, eResolution No. AF-0791 (May 24, 2001). A different perspective on whether bad faith can be shown can be found in a 2006 case, in which the complaining party owned a federal trademark registration, but was unable to prove bad faith where the registrant established that its use of the domain name and corresponding mark started before the complaining party began to use the similar name. Entre-Manure LLC v. Integriserv, NAF Case No. FA0606000741534 (Aug. 16, 2006).

[33] UDRP, ¶ 4(k).

[34] See, e.g., Dluhos v. Strasberg, 321 F.3d 365 (3d Cir. 2003); Parisi v. Netlearning, Inc., 139 F. Supp.2d 745, 751-52 (E.D. Va. 2001). Cf. Storey v. Cello Holdings LLC, 182 F. Supp. 2d 355 (S.D.N.Y. 2002) (the final

on a disputed domain name and obtain the return of a wrongfully transferred domain name. In 2004, Nike, Inc. brought an ACPA action to recover a domain name (www.justdoit.net) that Nike alleged had infringed on its "Just Do It" mark, after a WIPO panel had earlier refused to transfer the domain name because it found a lack of the "bad faith" needed to rule on *Nike's* behalf.[35]

3 E-COMMERCE

European law has much to say on the formation of agreements for the sale of goods and services over the Internet and for their enforceability. It also regulates the use of the Internet to promote commercial opportunities, which at one end of the spectrum constitutes spam. European law uses the concept of the "consumer" who has special privileges under the law.

The Construction of an E-commerce Contract

The European Union has legislated about what constitutes a valid contract in e-commerce. It had some difficulty doing this because the rules for the construction of a valid contract are different in common law from civil law jurisdictions. The European rules are contained in the E-commerce Directive (Directive 2000/31/EC), in which English law is combined with civil law concepts. The rule is to be found in Article 11 and requires a three-stage process: a making available by the e-trader; a communication by the customer; and an effective (actually received) confirmation by the e-trader. If everything is drafted properly that fits neatly with the common law sequence of invitation to treat, offer and acceptance. The terminology actually used on many websites is confused, with what a well-advised e-trader would want to call an invitation to treat worded as an offer, and so on. Where goods or services are made available from a website using American, and therefore common-law, terms and conditions, it is important to establish that the process of purchase laid out in the terms and conditions works in Europe. It is perfectly possible to do this, but it has to be done.

In the U.S., federal law makes clear that electronic signatures on agreements are acceptable. The Millennium Digital Commerce Act, known as E-SIGN ("E-SIGN"), has pre-empted almost all contrary federal and state laws placing conditions on the use of electronic signatures, agreements or records.[36] The law established a nationwide rule that electronic signatures, contracts, and records are to be treated the same, in general, as paper-and-ink signatures, contracts and records. It contains provisions that insure legal validity of electronic signatures and contracts, permits the electronic delivery of legally-required notices and disclosures, and allows for the satisfaction of record retention requirements through electronic means. At the same time, E-SIGN contains consumer protection measures requiring consumer notice and consent before electronic records can be binding. By granting nationwide legal recognition to electronic signatures and records in the United States notwithstanding laws that require "written" documents, E-SIGN made online transactions and online notices to consumers significantly easier.

Distance Selling

---

disposition of a trademark infringement case – here, dismissal with prejudice – serves as a decision on the merits in favor of the defendant, and precludes the later filing of an arbitration proceeding under the UDRP).

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

[36] P.L. 106-229. Most of the provisions of E-SIGN took effect on October 1, 2000.

All goods sold over the Internet (together with goods sold by telephone or otherwise remotely) fall within the ambit of the Distance Selling Directive[37]. The rules can be summed-up as follows:

- The rules are for the benefit of customers and not for business purchasers;
- The consumer is entitled to clear information, including details of the goods or services offered, delivery arrangements and payment, details of the supplier and a summary of the consumer's cancellation right before the contract of purchase is concluded;
- This information must be provided in writing;
- The consumer has a cooling-off period of seven working days within which he or she may cancel the purchase. There are exceptions (for example in relation to perishable goods) and in certain cases the cooling off period is longer.

Applicable Law

There is an immensely complicated body of law designed to ascertain the governing law and the appropriate forum for the resolution of disputes under contracts where the contracting parties are in different jurisdictions. In practice, this arises in circumstances where contracts are not formally documented. It is extremely rare for sales to be made through a website without terms and conditions and it is rare for the terms and conditions not to provide for governing law and forum. Within Europe, such a choice is likely to be conclusive, except where one of the parties is a consumer.

Whatever the terms and conditions say as to governing law (for contractual obligations Rome I Regulation (Reg. (EC) No. 593/2008) and for non-contractual obligations Rome II Regulation (Reg. (EC) No. 864/2007) and forum, the consumer is entitled to nominate his or her own governing law and forum (Brussels I Regulation (Reg. (EC) No. 44/2001) as appropriate for any dispute. Consumer law has not been harmonised within Europe and the rules in Germany, for example, are quite different from those in Britain. In practice this makes little difference, particularly when taken together with the cancellation rights under the Distance Selling Directive. If a consumer is dissatisfied with something bought through e-commerce the seller will never in practice argue the point.

Spam

European law attempts to deal with spam through data protection law, while in the US, the applicable legal regime attacks spam directly. In both cases, there appears to have been limited effect upon the mounting volume of spam.

Spam is in the eye of the beholder, but is often considered a bulk e-mail message advertising goods or services that is sent to a recipient without his or her prior consent (and without an underlying business relationship from which consent to exchange such communication can be implied).[38] In 2009, a McAfee study suggested that spam costs

[37] Directive 97/7/EC.

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

businesses $182.50 per employee per year.[39] But in 2005, a University of Maryland report concluded that the economic impact of deleting spam was $21.6 billion a year.[40]

The large volume of spam on the internet is a function of the relative lack of security of the e-mail protocol, SMPT, and of the economics of spam: unlike commercial mail that is sent through conventional postal services, sending a massive volume of e-mail costs a spammer little more than sending the same message to the small group of people most likely to be interested in receiving the message. Over time, spam countermeasures may curb the volume of e-mail that reaches the inboxes of consumers, but even that cheery assessment may be overstated, given the vulnerability of computers, the sophistication of hackers, and the fact that one country's laws may slow, but not stop, spammers outside that country (let alone those who transmit spam from within the same country).

There are different types and degrees of spam. At the sordid end of the market there is mainly pornographic material. Much of this involves massive quantities of e-mails sent to addresses that might or might not exist, in the hope of striking lucky. To send an 'unsubscribe' response to such a message is to confirm your existence and to invite even greater quantities. At the other end of the spectrum there is e-mail marketing undertaken in good faith to people at addresses that exist, who might well be known to the sender and are believed to be potentially interested in the offers being made.

In a report to the U.S. Congress, the Federal Trade Commission commented on the proposal to create a "Do Not Email" registry, akin to the widely-used and popular national "Do Not Call" registry. The FTC reported that:

> *The Commission does not believe that a National Do Not Email Registry would result in any appreciable reduction in the amount of spam. In fact, it could actually increase the volume of spam. This perverse result is likely because illegal marketers who send spam would use a National Do Not Email Registry as a directory of valid email addresses.* [41]

The law varies radically between the US, on the one hand, and Europe on the other.

In the US, a federal law took effect on January 1, 2004, called the "CAN-SPAM Act of 2003." [42] The CAN-SPAM Act established a national standard for regulating non-deceptive commercial electronic mail and also provides criminal penalties for falsification techniques used by professional "spammers." The CAN-SPAM Act requires that all commercial e-mail messages include an opt-out, a physical address, and an indication that the e-mail is a solicitation. The law leaves it up to the sender of the e-mail to determine how to indicate that the message is a solicitation. There are no specific labelling requirements (although the FTC is authorized to consider adding such requirements in the future). The federal law pre-empts many state-level labelling requirements. The opt-out, address and solicitation indication requirements imposed on commercial e-mail do not apply to "transactional or

---

[39] McAfee Research Report, "March 2009 Spam Report" (March 2009) (available at http://newsroom.mcafee.com/images/10039/mar_spam_report.pdf).

[40] Ian Martinez, "Spam Remains Costly, Americans Remain Unwilling to Accept New Technology," Wash. Internet Daily, Feb. 4, 2005, at 3.

[41] Federal Trade Commission, "National Do Not Email Registry: A Report to Congress," at 32 (June 2004) (footnotes omitted) (copy available at *http://www.ftc.gov/reports/dneregistry/report.pdf)*.

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

relationship" e-mail messages, such as ongoing commercial relationships that are not primarily solicitations. However, these requirements do apply to all other commercial electronic mail, which is defined as any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.

Unlike the United States, Europe benefits from having a consistent body of data protection law, and it is mainly this that the European Commission has used to attempt to deal with spam. The European Union adopted its Directive on Privacy and Electronic Communication in 2002. Member States are required to bring it into effect in national law by 31st October 2003. The United Kingdom has published draft regulations to that end, the Privacy and Electronic Communications (EC Directive) Regulations 2003: "the Regulations" and "the Directive", for our purposes, respectively.

The intention of the Directive (Directive 2002/58) is clear. Article 13(1) states:

> *"The use of … electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who* ***have given*** *[*our emphasis*] their prior consent."*

"Electronic mail" under Article 13(1) is defined widely and includes SMS messages.[43]

Previously it was sufficient that subscribers were given the opportunity to opt out of – withdraw their consent to - receiving direct-marketing e-mails. Individuals retain the right under data-protection legislation to require at any time that they no longer receive e-mails from a particular marketer. Now, under the Directive, you can market to them only if they opt in – give an informed consent in advance. In an opt-out the customer will receive further communications unless he or she ticks a box declining them; in an opt-in there will be no further communications unless the customer ticks the box agreeing to receive them.

The Directive goes on to discuss what, in addition to an unambiguous tick in the box, "consent" means. Article 13(2) states:

> *"…where a natural or legal person obtains from its customers their electronic contact details for electronic mail* ***in the context of a sale of the product or a service*** *[our emphasis] …the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that the customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use."*

This definition of consent is very restrictive. The e-mail address has to have been obtained in the context of an actual or negotiated sale by the proposed sender, the contact details being obtained in accordance with the provisions of the Data Protection Directive. The customer must therefore have been given the opportunity to opt out of its contact details being used for direct marketing purposes. If the e-mail address has been taken from a business card or a registration form on a website, or through an advertising promotion, that does not count, unless the provision of the address amounted to actual consent. Under this wording one is not permitted even to e-mail a person to ask if they would like to receive promotional e-mails.

---

[43] In contrast, the U.S. CAN-SPAM Act does not yet apply to text messages. A proposal pending in the U.S. Senate would amend that Act to cover text messages as well as conventional e-mail messages. S. 788 111th Cong. (2009) (the "m-SPAM Act of 2009"), is pending in the Committee on Commerce, Science, and Transportation.

What it amounts to is that sending a business message to someone who is not expecting it is unlawful.

Strangely there is no comparable restriction in relation to the sending of physical junk mail. However, the cost associated with printing and mailing junk mail through the postal service is one factor that tends to make it less of a pervasive problem. Indeed, among the proposals occasionally raised with an eye toward reducing e-mail spam is the notion of charging a per-e-mail fee to the sender.

In Britain, however, the position is less restrictive. The equivalent provision to Article 13(2) of the Directive, Regulation 21(3)(a), says that a sender is allowed to send a marketing e-mail where it has

> *"obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient."*

Indeed, the UK Department for Business, Innovation and Skills (BIS) has said that so long as the e-mail address was obtained "legitimately", it will be satisfied:

> *"Our view is that the most important safeguards here are that contact details are fairly collected and subscribers are clearly informed of, and given a chance to object to, use of their data for direct marketing by that same business."*

What "legitimately" and "fairly" means is anyone's guess, but it would appear to render acceptable the use of e-mail addresses taken from website enquiries, the willing proffering of business cards and so on. Indeed it sounds very like the old opt-out position: the subscriber is given a chance to object to receiving e-mails, as was the position before. Of course, in the last resort it is not what the BIS thinks, but the Information Commissioner, who administers the data protection regime in the UK, and ultimately the courts, that matters.

The position in relation to deemed consent therefore is a mess. So, however, is the position in relation to actual consent. What every e-mail marketer wants to know is whether a pre-ticked opt-in, that can be unticked, counts as a consent. Neither the Directive nor the Regulations tell us. The Information Commissioner's guidance states that clear knowledge on the part of the subscriber is the overriding consideration.

There is then a large and surprising loophole. The beneficiaries of the Regulations are "individual subscribers". These are defined as individuals who contract with service providers for the delivery of e-mail services. Employees with e-mail accounts at work do not contract with service providers; their employers do. Schoolchildren with e-mail accounts at school do not contract with service providers; their schools do. In other words, when you are at home, the law will protect you from the anguish of receiving an unexpected communication, but if the spammers want to stuff your inbox at work or at school with come-ons by nymphets with webcams and by legal conference organisers, that's fine.

To make things even more confusing, the wording may mean that where the employer is an individual or a group of individuals, employees are protected, but not where the employer happens to be a company.

There is another European initiative that restricts spam. The Electronic Commerce (EC Directive) Regulations 2002 provides that a commercial e-mail must:

(a) be clearly identified as such;

(b) clearly identify the sender; and

(c) clearly identify any associated offers and promotions.

Furthermore, an unsolicited commercial e-mail must be clearly and unambiguously identified as such as soon as it is received. This is intended to combat the evil of the spam message that pretends in its subject line to be a personal message, so that you don't immediately bin the message.

Of course, the great majority of spam, and much of the particularly objectionable spam, comes from the Far East. Those spammers care very little what EU Directives say, and even less how they are massaged by the UK Government. Those spammers will continue unaffected whatever restrictions are imposed by law.

Viral Marketing

As regards viral marketing, we are again principally concerned with the Privacy & Electronic Communications Directive. The Privacy & Electronic Communications (EC Directive) Regulations 2003, bringing it into effect in the UK, provide that:

> *"A person shall neither transmit nor instigate the transmission of unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by or at the instigation of the sender."*

The point is that a simple recommendation by a 'user' to a 'friend' is not caught by the Regulations, but where the website encourages the user to recommend the website to a friend and makes it easy for the user to do so, that may amount to *instigation* and may therefore cross the line into illegality.

There are two ways in which this might normally be done. The first is to provide a means, such as a standard form of e-mail, so that the user can send an e-mail recommending a website or a franchisor's service or goods to a friend, on the basis that the website will acquire the e-mail address of the friend only when the friend responds. We will call that "Method A". The other method ("Method B") is where the user provides the website with the details of the friend at the outset and the website sends the e-mail to the friend, either referring to the user or not referring to the user or as if in the name of the user.

In either case, one often finds incentives offered by the website to the user if the friend responds (or even, in the case of Method B, anyway).

The legal position is uncertain. All that we have to go on are the Regulations and the code of conduct recommended by the UK Information Commissioner, and his equivalent in other European countries. We can however draw the following conclusions:

1) Method A is much safer than Method B.

2) In communicating with the friend, it is important not to impersonate the user. If the website is sending the e-mail to the friend, either it should be in the user's own words or it should make it clear that the website is communicating with the friend having got the friend's details from the user. This concern does not arise with Method A.

The UK Information Commission says that it is 'safer' not to give visitors any incentive. To do so suggests that the website is the "instigator" of the message since the user would not communicate with the friend unless he has some incentive to do so. To say that it is "safer"

not to give an incentive is not however the strongest language one can imagine, and we know that incentives are routinely given. It may be safe to assume that the less like cash the incentive is the better, so that to go into a prize draw, or to get points that might be redeemed at some point in the future would be better than cash, since it would look less than a straight incentive and more like a loyalty programme. However, we have no authority for that.

- The website should get the user to confirm that the friend had confirmed to the user that the friend consents to receiving the communication. This would be as part of the click-through process before the "send" button is clicked.

- The website should check that the friend has not already requested that he should not be contacted by you. This does not arise under Method A.

- The website should inform each user that it will tell the friend that it got the friend's details through the uses. This does not arise under Method A.

- If the websites obtain the e-mail address of the friend using Method B you should not use that address for any other purpose until the friend responds. Again, this does not arise under Method A.

The Information Commissioner points out a risk that a competitor might impersonate a user in order to get the website to send out multiple unwanted e-mails so as to create bad feeling amongst prospective customers. There are two possible ways of dealing with this. One is to limit the number of friends that a user can recommend. The second is not to allow users to fill out the form without volunteering their names and addresses (although of course there is nothing to stop them using false names and addresses).

The authorities that administer data protection law elsewhere in Europe, particularly in Spain, take a rather less accommodating view of the law, and in Spain, fines are a distinct possibility, even for a first offence.

European Competition Law.

EU competition law also affects the way franchise agreements should deal with internet usage by franchisees and distributors. The Vertical Restraints Block Exemption,[44] interpreting Article 81(1) of the Treaty of Rome, prohibits any agreement or concerted practice which has the object or effect of "preventing, restricting, or distorting" competition. Breach of Article 81(1) may put a franchisor at risk of fines or of having non-compliant franchise agreements deemed unenforceable. In relevant portion, the Vertical Restraints Block Exemption addresses internet sales in an indirect manner. Article 4(c) of the Exemption bars limits on passive sales methods. Passive sales are those in which the seller responds to the buyer's request, and where the seller did not solicit the requests. Article 4(c) of the Exemption notes that in order to qualify for the exemption, a vertical agreement may not include:

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

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

To provide guidance as to this standard, the Commission issued Guidelines on Vertical Restraints on November 13, 2000.[45] In relevant part, the Guidelines addressed internet sales as follows:

> Every distributor must be free to use the internet to advertise or to sell products. A restriction on the use of the internet by distributors could only be compatible with the Block Exemption Regulation to the extent that promotion on the internet or sales over the internet would lead to active selling into other distributors' exclusive territories or customer groups. In general, the use of the internet is not considered a form of active sales into such territories or customer groups, since it is a reasonable way to reach every customer. The fact that it may have effects outside one's own territory or customer group results from the technology, i.e. the easy access from everywhere. If a customer visits the web site of a distributor and contacts the distributor and if such contact leads to a sale, including delivery, then that is considered passive selling. The language used on the website or in the communication plays normally no role in that respect. Insofar as a web site is not specifically targeted at customers primarily inside the territory or customer group exclusively allocated to another distributor, for instance with the use of banners or links in pages of providers specifically available to these exclusively allocated customers, the website is not considered a form of active selling. However, unsolicited e-mails sent to individual customers or specific customer groups are considered active selling. The same considerations apply to selling by catalogue. Notwithstanding what has been said before, the supplier may require quality standards for the use of the internet site to resell his goods, just as the supplier may require quality standards for a shop or for advertising and promotion in general. The latter may be relevant in particular for selective distribution. An outright ban on internet or catalogue selling is only possible if there is an objective justification. In any case, the supplier cannot reserve to itself sales and/or advertising over the internet.[46]

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

4 ELECTRONIC DISCLOSURE FOR FRANCHISORS

Regulations pertaining to the offer and sale of franchises, which are well-known in the U.S., exist across the globe in varying form, and in varying degree, in 22 other countries. While initially, U.S. authorities reluctantly accepted the idea of electronic disclosure, they have (in part spurred on – if not required – by the federal E-SIGN Act, discussed above) now fully embraced the concept of e-disclosure. As part of its 2007 amendments to the Franchise Regulation Rule, 16 C.F.R. Part 436, the Commission wrote "[the Rule] permits franchisors to furnish disclosures electronically through a variety of media, including CD-ROM, Internet

---

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

[46] Id. at ¶ 51.

website, and email." [47] Moreover, the FTC made it very clear that it was willing to consider, broadly, many methods of providing disclosure as well as many methods of obtaining a "signature" to a disclosure receipt – again, taking its cue from the E-SIGN Act – but wisely not limiting franchisors to the technology known in 2007 when the amended Rule is likely to be in place for quite some time to come.[48]

*****

Franchisors and franchisees are, by their nature, innovative. Hence, whether they are individually willing to try and adopt new technologies, their nature as businesspersons suggests that they will gravitate toward methods and procedures to make more efficient and better able to market and deliver goods and services to their customers. In this regards, franchise companies have embraced technology and the internet. New technologies and internet applications – such as social media (worthy of its own chapter and more) – are constantly developing, evolving, morphing, and emerging as the business community and consumers find new ways to reach one another.

However, as we attempt to illuminate some of the most common and important issues facing franchise systems, we are humbled by the recognition that what we write relates to the world as we know it – and that we know that world will change. The principle that "nothing endures but change" dates back to the Greek philosopher Diogenes Laertius, but it was expressed more recently by the 20th Century author Isaac Asimov. Asimov wrote that "[t]he only constant is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be." [49] Diogenes and Asimov drew conclusions that fittingly summarize the state of things today as relates to franchising and the internet.

[47] 72 Fed. Reg. 15444, 15452 (2007).

[48] While the FTC Rule requires franchisors to keep a "signed receipt" for at least three years from each completed transaction, 16 C.F.R. § 436.6(i), the term signature is meant to be broad interpreted, and includes "a person's affirmative step to authenticate his or her identity. It includes a person's handwritten signature, as well as a person's use of security codes, passwords, electronic signatures, and similar devices to authenticate his or her identity." 16 C.F.R. § 436.1(u).

[49] Isaac Asimov, Asimov on Science Fiction (1983).