Domain Names: Has Trade Mark Law Strayed From Its Path?

HASAN A. DEVECI

Abstract

Trademarks and domain names are infringed by an unauthorised ‘use in the course of trade.’ Trademark infringement predates the Internet, of course, but by eroding the geographic boundaries that traditionally allowed multiple users to apply the same or similar mark in different countries or in relation to different products, the Internet has aggravated the illegitimate use of trademarks. Part I of this article will outline the nature and justify the protection of intellectual property but argue that unlike passing off registered trademark law has strayed from its path. Part II will examine judicial attitudes towards trademarks and domain names and contend that emphasis on the reputation of the trademark rather than reputation in the product underlines current problems. Part III will review the nature of domain name disputes, comment on dispute resolution policies and suggest indexed linking or classified registration of domain names as one possible solution.

1 Introduction

1.1 Why monopolise intellectual property rights?^2

Regulating the creation, use and exploitation of intellectual property encourages investment.

Art. 2, para. viii, of World Intellectual Property Organisation (WIPO) Convention (1967) defines 'intellectual property' as 'rights relating to literary, artistic and scientific works . . . inventions . . . trade marks, service marks, and commercial names and designations.' Accordingly, 'commercial names and designations' such as domain names and trademarks are intellectual property. But because the word 'property' is synonymous with 'ownership' three issues become relevant: first, distinction between the product and the rights vested therein. Second, should property rights themselves be protected? And, if so, third, what should be the scope of protection granted to trademarks and/or domain names?

First, property and rights analogy: Let's, for instance, take a song printed on a CD. The inventor of the CD retains the patent rights in the disk while the purchaser acquires a personal property in the disk. Similarly, the author may retain the copyright in the lyrics while the record company, the producer and others may own the trademark, production rights etc under which the record is sold. Second, general and intellectual property: 'Intellectual Property Rights (IPRs)' gained acceptance late in the eighteenth century but the debate, driven by the 'exclusive right' of the owner to 'use and exploit' such property, about the status and legitimacy of intellectual property continues unabated. As names in the English language, 'Harrods' and 'Harry Potter' are in the public domain and could be used time and again by anyone as a person's name but as a trademark or a domain name these names can only be used by one person or body, the trademark owner.3 Can such monopoly denying others the use of what would otherwise be in the public domain be justified? Commentators have argued that as with physical labour the financial rewards expected to flow from mental or creative effort are an incentive and that removing the reward stifles the incentives and hence creativity. Supporters also brace a stronger, moral, argument in that third parties should not reap where they have not sown and that the public should be protected from false claims.4

---

^2 Following the industrial revolution reference was made to industrial property that conjured up a picture of patents and trademarks as distinct from intellectual property. The historical attribution of industrial and intellectual is relevant only to explain the development, nature and scope of protection of the collection of disparate intellectual property rights.


^4 In Perry v Truefit [1842] 6 Beav 96 Lord Mangdale MR explained the rationale for trademarks. He said: 'A man is not to sell his own goods under the pretence that they are the goods of another man; he can not be permitted to practice such a deception, nor to use the means which contribute to that end.'
Opponents admit that, for instance, Microsoft would not have invested millions of dollars in developing Windows as an operating system had it not aspired to dominate World markets but suggest that inner drive and ideology are equally strong motives. They point to creators like Van Gogh who did not sell a single painting in his lifetime and draw attention to Linux, the freely available operating system competing with Microsoft’s Windows. Third, there are clearly arguments on both camps but the fact remains that economic growth and prosperity depend on balancing conflicting interests, hence, for our purposes, the scope and protection of trademarks and domain names. Eliminating ‘free riders’ desirous of exploiting an established trademark may well protect both the investment and the consumer but registered trademarks protect a ‘class’ of products to which the mark may yet have to be applied and registrants of domain names covet global exclusivity. Has trademark law overreached its raison d’être? The argument is deferred to the next and concluding sections, when the interaction between trademarks and domain names would have been explored.

1.2 What are trademarks and domain names?

A trademark is a badge of origin, a domain name is an electronic address. For years, even before the industrial revolution, traders used marks to indicate ownership and, later, as a mark of origin distinguishing the goods of one trader from those of another. So successful was the practice that guilds were formed whose members used the mark to confer quality, value and authenticity. As the mark acquired distinctiveness and reputation in relation to specific goods or services, hence the trademark, it became part of the trader’s good will. If and where an identical or similar mark was applied to identical or similar products the common law action of passing off based on the tort of deceit was initiated to prevent confusion in the minds of the purchasing public and thus protect the trader’s good will. Nineteenth and twentieth century legislation emulated the blue print for passing off. Whilst rights are immediate upon registration; protection is still product and country specific, and essentially, rests on the idea of avoiding confusion.

A domain name is a user-friendly text representation of computer readable binary numbers; it identifies the electronic address of an e-merchant much the same as a postal address or a telephone number on the global network. Although trademarks are commonly used as domain names on the face of it trademarks and domain names are functionally different, a trademark informs us as to who produced the goods or supplied the services whilst a domain name tells us where to find the product in

---

5 Though often confused with the electronic address, in fact, the domain name is only part of the Universal Resource Locator (URL). For example, in the e-mail: ‘deveci@sbu.ac.uk’ and the URL: ‘http://www.sbu.ac.uk/deveci/’ only ‘sbu.ac.uk’ is the domain name.
question. Moreover, ‘confusion in the minds of the public’ forms the basis of an action for passing off and trademark infringement. But, commentators have argued that confusion in domain names is unlikely because if the domain name is known the user will not be typing in and hence call up the wrong name. Reliance on the search engine demonstrates that the trademark come domain name is not as well known in the relevant market place; the fact that a big brand name is recognised from its advertisements is not necessarily an indication that the brand is associated with specific goods.\(^6\) In practice, users seek out data rather than specific names; search engines compile a list of relevant websites, which are then downloaded by the user for further examination.\(^7\) By implication trademark law should not extend to the governance of domain names. Nevertheless, it may be argued that advertising and or familiarity elevated domain names initially designed to find the goods or services into visible messages of quality distinguishing one e-merchant from another in the way that trademarks distinguish the products of one merchant from those of another.\(^8\) It is equally arguable that domain names qualify as trademarks within the meaning of the Trade Marks Act 1994. S.1 of the Act defines a trademark as ‘any sign ... capable of distinguishing’ the goods or services of one undertaking from those of other undertakings. In *Philips Electronics v Remington*\(^9\) Jacobs J defined a sign as ‘anything which can convey information’. The New Shorter English Dictionary defines a ‘sign’ as ‘a mark, symbol or device used to represent something or distinguish the object on which it is put.’ Surely, a domain name is a ‘sign’ that conveys information but is it ‘capable of distinguishing’? By its very nature a domain name is unique used to distinguish one website from another and as such it is an unregistered trademark deserving the protection of trademark laws.

1.3 *How different are passing off and registered marks?*

*Passing off protects acquired reputation, registered marks are immediate and futuristic*

When trademarks were eventually registered, in the nineteenth century, the registered holder was granted exclusive rights to use the mark but only in the country and in relation to a specific class of goods or services for which the mark was registered. But that is where the similarity with passing off ends. Like the protection of copyright and patents passing off follows a period of gestation and its scope is clearly delimited. Copyright protects

---

\(^6\) See *Radio Taxicabs*, MBNA American Bank that referred to ‘sophisticated Internet users’ and Avery Dennison Corp v Sumpton 51 U.S.P.Q.2d 1801.

\(^7\) Jacob J in *Avnet* [1998] FSR 16 at 18 noted that search engines look for words and not for words in relation to goods or services so that a searcher looking for a word in a context may well find the word in a wholly different context.

\(^8\) The domain name ‘ebay’ with 55m registered users is as well known as Rolls Royce operating in the physical world.

creativity and patents protect an invention, and so passing off protects the acquired reputation; the result of prolonged human efforts. A copyright holder is protected against substantive copying of the text but has no monopoly over the plot and a patent grants an inventor exclusive rights over the invention but others may gain rights over different uses for that very invention. Even with passing off the exclusive rights of the trademark owner are evolutionary and product specific. Yet, unlike copyright and patents, and even passing off, registered trademarks are designed to protect not past achievements but future expectations. The registrant gains immediate exclusive rights upon registration and in relation to the class of goods or services for which the mark is ‘intended’ to be applied.10
The worry is advertising, promoting the mark itself rather than the product to which it is to be attached. Trademarks, reinforced by advertising, may generate the flow of information to the consumer and set a benchmark for satisfactory quality. But, registration without reputation comes loaded with problems: first, advertising often transforms the trademark from a mark of origin to a ‘salient salesman’ promoting ‘the’ desired product or image. It is not unusual for people who have never worn ‘Levis’ trousers to recognise the advert and even sing the tune. Consumers are likely to buy Canon scanners not because they formed an informed opinion but because they know of Canon’s reputation in cameras, without necessarily using one. Second, over advertising could mislead the consumer into thinking that the goods or services of the trademark owner are of better quality than they actually are. Third, registration of a mark without reputation in a product denies others the use of an identical or similar mark and consequently excludes others from the competitive market space for those products.11
Fourth and worst, in the case of domain names, the subject of this article, the registrant covets and expects ‘exclusivity’ unrestricted by product classification or geographic boundaries. The risk is that the greater the reputation of the trader the wider will be the protection of the mark thus displacing the very raison d’être for trademarks.

2 Trademark and domain name disputes

2.1 Passing off: Does it protect reputation of the mark or in the product?

Not reputation of the mark but the reputation represented by the mark in the product. The action for passing off has so often adapted to commercial changes that formulating a precise and accurate statement in a short form is intensely

---

10 An applicant must declare a bona fide intention to use the mark and a registered trademark may subsequently be challenged for ‘non-use’ but, unlike passing off where protection is aligned with reputation, evidence of established reputation is not a pre-requirement of S.32(3), TMA 1994.

11 See the ECJ’s liberal interpretation in Canon and Jacob J’s concern in British Sugar.
difficult.\textsuperscript{12} Nevertheless, in \textit{Reckitt \& Coleman Products v Borden Inc.}\textsuperscript{13} Lord Oliver reduced the elements to the trinity of \textit{confusion} leading to \textit{deception}, and \textit{damage}; but, note that the requirements are interrelated and may impact on one another.

Reputation, represented by the mark, is ‘the attractive force that brings in custom . . . it has the power of attraction sufficient to bring customers home to the source from which it emanates.’\textsuperscript{14} Injunction is granted against ‘a person, competing in trade, who seeks to attach to his product a name or description with which it has no natural association so as to make use of the reputation and good will which has been gained by a product genuinely indicated by the name.’\textsuperscript{15} Thus, protection is not of the mark \textit{per se} but that which is represented by the mark; representation as to the ‘source’ of the product ‘genuinely indicated’ by the trademark. It follows that the name or description, representing the mark, must be sufficiently distinctive so as to have a causative impact on customer behaviour.\textsuperscript{16} For instance, if I stop to eat at a motorway complex do I stop because it is conveniently placed on the motorway or because the restaurant has a reputation –am I conveniently at or have I purposefully travelled to the restaurant in question? Only the latter could be attributed to reputation. Manifestation of the mark may be by some word, sign or badge or even a name or a descriptive term so long as the trademark is distinctive of the claimant and is perceived as a trademark by relevant consumers. In \textit{Parker Knoll v Knoll International} the English furniture makers acquired their name and mark from a kind of spring invented in the 1930, by Wilhelm Knoll of Stuttgart. A nephew of Knoll who set up Knoll International in the US wished to enter the UK market. The House of Lords restrained the US-based business from using the name ‘Knoll’ holding that Parker Knoll had acquired a \textit{secondary meaning} in the UK. In contrast, in \textit{Efax.com Inc v Mark Oglesby}\textsuperscript{17} an American Company using ‘efax.com’ as their domain name with allegedly 5000 customers in the UK was refused an injunction against ‘efax.co.uk’. Parker J observed that ‘efax’ was essentially descriptive and an example of generic \textit{e-language} terminology that crept into common use. He held that confusion, if any, caused by the similarity of names resulted from the

\begin{footnotesize}
\begin{enumerate}
\item Evren Warnink \textit{BV v Townend} [1979] AC 731, at 742. Lord Diplock laid down five essential ‘characteristics’ for a successful action in passing off. At 755–6, Lord Fraser, enumerated five different characteristics, hence, presenting two different sets of requirements for the same cause of action.  
\item IRC v Muller \& Co’s Margarine [1901] AC 217, p.224.  
\item The representation may be manifested by some word, sign or badge, or even a name so long as the name will have acquired a \textit{secondary meaning} as in \textit{Parker Knoll v Knoll International} [1962] RPC 265 or Evren Warnink \textit{v Townend \& Sons} [1979] AC 731.  
\item Masons Computer Law Reports [August 2000].
\end{enumerate}
\end{footnotesize}
Misrepresentation is the intentional or innocent ‘misappropriation’ by the defendant of the claimant’s reputation in a way that is likely to cause confusion in the minds of the purchasing public. Confusion is used not in the sense of not knowing whose products the public is buying but in the sense that the misrepresentation by the defendant causes (deceives) the public into thinking that the goods or services of the defendant are in fact those of or associated with the claimant. In *Reckitt & Colman v Borden*, Reckitt & Colman had for many years sold lemon juice in plastic containers resembling natural lemons in colour and shape. Borden started selling lemon juice in similar containers but, in order to distinguish their product and avoid confusion, Border attached a suitably distinctive label to their container. Injunction was granted against Borden from marketing their product in any container so nearly resembling the JIFF lemon shaped container. As Lord Oliver explained ‘... where the article sold is conjoined with an object ... of a shape or configuration which has become specifically identified with a particular manufacturer, the latter may be entitled to protection against the deceptive use in conjunction with similar articles of [sic] objects fashioned in the same or a closely similar shape. ... The deception alleged lies not in the sale of plastic lemons ... but in the sale of lemon juice ... in containers so fashioned to suggest that the juice ... emanates from the source with which the containers of those particular configurations have become associated in the public mind.’ An interesting example of applying familiar principles of passing off to the world of e-commerce arose in *Radio Taxicabs v Owner Drivers Radio Taxi Services* where the claimants operated a website at ‘www.radiotaxis.co.uk’. The defendants who were in a similar business published their services from their website at ‘www.radiotaxis.com’. In proceedings for passing off the court refused an injunction against the defendants concluding that reputation and distinctiveness in the name Radio Taxis within the taxi trade was itself not sufficient, the same had to be shown in relation to the general public.

---

18 In *Procter & Gamble Co v Office for Harmonisation in the Internal Market* (C383/99 P) [2002] Ch 82 (ECJ) the ECJ ruled that though descriptive of a function ‘Baby-Dry’ is registerable as a trademark for nappies providing the proposed mark is distinctive and is likely to be perceived as a trademark by relevant consumers.

19 The risk with highly distinctive marks is that the mark may evolve into a ‘generic’ term and that the public may begin to use it to describe the kind of articles to which it has been applied. For instance, though the word ‘Hoover’ is the trade name for certain vacuum cleaners and other electronic products in the public mind it has come to describe any form of vacuum cleaner. See the ‘Corona’ cigars dispute in *Havana Cigar v Oddenino* [1924] 1 Ch.179.

20 [1990] 1 All E.R 873.

2.2 Registered trademarks: How relevant are confusion and/or reputation?

Confusion is a requirement but is being challenged by reputation.

In view of the fact that the relative grounds for refusal (opposition) in S.5 and the grounds of infringement in S.10 correspond with and incorporate the respective articles of the EC’s Approximation of Trade Marks Laws Directive 1989, it may be helpful to list and summarise the respective provisions.22

<table>
<thead>
<tr>
<th>Opposition TMA–TM Dir.</th>
<th>Infringement TMA–TM Dir.</th>
<th>Scope and requirements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.5 Art.4 (1)</td>
<td>S.10 Art.5 (1)</td>
<td>refusal—infringment if used in course of business identical mark . . . identical product</td>
</tr>
<tr>
<td>(2)(a) (1)(b)</td>
<td>(2)(1) (1)(b)</td>
<td>identical mark . . . similar product similar mark . . . identical/similar product</td>
</tr>
<tr>
<td>(3) (1)(b)</td>
<td>(3) (1)(b)</td>
<td>earlier mark has reputation in the UK sign takes unfair advantage . . . detrimental to . . . mark</td>
</tr>
</tbody>
</table>

It follows that a trademark is infringed if an offending sign is used 'in the course of trade' in one of three ways. First, an identical sign is used in relation to identical products. Second, an identical sign is used in relation to similar products; or a similar sign is used in relation to identical or similar products and there is the likelihood of confusion in the minds of the public. Third, an identical or similar sign is used in relation to products that are not similar and the use of the sign takes advantage of or is detrimental to the distinctive character or the repute of the trademark. In effect, the third kind of infringement combines two facets: ‘unfair advantage’ reminiscent of passing off and ‘detrimental effect’ mirroring the American concept of dilution. The pertinent questions are:– was there ‘use in the course of trade’, were the marks or products identical or similar, and was there ‘likelihood of confusion’?

Was there ‘use in the UK, and was the ‘use’ ‘in the course of trade’?

Since trademark law is territorial, the use must be in the ‘UK’ and ‘in the course of trade.’ Though a jurisdictional issue, use in the UK is particularly relevant to the Internet and is likely to arise where the trader is outside the

---

22 Whether in opposition or infringement proceedings it is important to remember that whilst a liberal interpretation of the statute will afford greater protection for the earlier trademark it will equally diminish the opportunity for others to enter the market with identical or similar trademarks.
UK but the web pages are accessible in the UK. In 1–800 Flowers Inc v Phonenames Limited\(^{22}\) Phonenames were a UK company marketing the alpha-numeric phone concept where the telephone number on the pad corresponded to the letters spelling a particular trade; for instance, ‘356–9377’ read FLOWERS and ‘758–6237’ spelled PLUMBER and so on. 1–800Flowers Inc, a US corporation offering international floral services accessed through a freephone and a website, applied to register ‘800-FLOWERS’ in the UK. Phonenames objected to the registration. Jacob J rejected the application to register. On the issue of access Jacob J said: ‘the mere fact that websites can be accessed anywhere in the world does not mean, for trade mark purposes, that the law should regard them as being used anywhere in the UK.’ Similarly, in Euromarket Designs Incorporated v Peters & Anor\(^{24}\) the American owners of the UK trademark for ‘Crate & Barrel’ failed to convince Jacob J that a furniture shop by the same name who run a web page incorporating the domain name ‘crateandbarrel-ie.com’ accessible in the UK infringed their UK trademark. Jacob J’s view that mere access does not of itself amount to ‘use in the UK’ was confirmed by the Court of Appeal in 1–800 Flowers Inc. Parker LJ said: ‘the very idea of ‘use’ within a criteria area would seem to require some active step in that area on the part of the user that goes beyond providing facilities that enable others to bring the mark into the area.’ The ‘active step’ suggested by the court must invite an association between the sign and the product in question; the mark or sign must be used so as to indicate a source of origin of the goods or services. In Trebor v Football Association\(^{25}\) the defendants were manufacturers of sweets whose sweets packets included cards depicting famous footballers. Where the card was of an England player the photograph also carried the England team logo with the three lions, which was the registered trademark of the Football Association. In an action for infringement Rattee J held that the manufacturer did not ‘affix the sign’ to the cards within the meaning of S.10(4). He observed that the logo appeared on the card ‘only because it is worn by the player whose photograph appears on the card as part of that player’s England team football strip, to show that the player himself is an England player.’ More recently, Arsenal Football Club v Matthew Reed\(^{27}\) raised a question thought to have been swept away in British Sugar; namely, must the trademark be use in a ‘trademark sense?’ Here, Reed sold football souvenirs and memorabilia at stalls situated outside the club’s stadium. Arsenal claimed that the unauthorised selling of items carrying words and signs associated with Arsenal infringed the club’s trademark. As with Laddie J, the ECJ

---

\(^{22}\) [2000] ETMR 369.
\(^{24}\) [2001] FSR 288.
\(^{25}\) [1997] FSR 211.
\(^{26}\) Ibid. at 216.
\(^{27}\) [2002] EWHC 2695 (Ch).
confirmed that the essential function of a trademark is to guarantee to consumers the real ‘origin’ of goods or services by enabling them to distinguish the claimant’s goods from those of other suppliers but reached a different conclusion.28 According to the ECJ words and signs imprinted on the items sold suggested an association between the defendant’s goods and the club and the fact that the public perceived the sign as a badge of support for or loyalty to the club is immaterial. In contrast, Laddie J dismissed Arsenal’s claims on two grounds. First, Reed had put up notices informing the public that the items were not official products; hence, there was no confusion and no passing off. Second, the public’s perception of the sign as a badge of support for or loyalty to the club meant that the trademark did not function as an indication of ‘origin’ and as such was not being used as a trademark.29

Are the marks and or products identical or similar –S.10(1–3)?
A trademark may be infringed, inter alia, where the infringing sign is identical with the trademark and is used in relation to goods or services, which are identical or similar. Where the mark is merely similar, as in S.10(2)(b), there is also the requirement of confusion. The confusing ‘confusion’ debate in S.10(2) (b) is of two kinds: first, how is ‘the likelihood of confusion’ interpreted? That is, does the similarity of goods necessarily lead to confusion, or should the similarity of goods and the likelihood of confusion be proved as separate requirements? Second, and equally confusing, is the relationship between confusion and association; does confusion include association or is association an alternative introducing a new and wider form of infringement? In comparing the sign and the prior trademark the courts of the UK, the US and the ECJ seem have adopted a common theme; confusion: do the marks appear to be the same, do they sound or look alike and does it cause confusion?

In The Coca-Cola Co. of Canada v Pepsi-Cola Co. of Canada30 the claimants contended that the use of ‘Pepsi-Cola’ by the defendant infringed their registered trademark for ‘Coca-Cola’. Similarity between the marks was determined by reference to public perceptions; was it likely that the consumer would confuse ‘Coca-Cola’ with ‘Pepsi-Cola’? Lord Russell expressed the view that in its hyphenated form the first word ‘Coca’ rather

---

28 Ibid. para.5. The ECJ concluded that where a third party uses in the course of trade a sign which is identical to a validly registered trade mark on goods which are identical to those for which it is registered, the trade mark proprietor of the mark is entitled, in circumstances such as those of the present case (self-emphasis), to ... prevent that use. It is immaterial that, in the context of that use, the sign is perceived as a badge of support for or loyalty or affiliation to the trade mark proprietor. 'Laddie J disregarded the ECJ’s finding because upon a reference by the national courts the ECJ has no jurisdiction to conclude on matters of fact, and even less so to reach a different finding.

29 See also Primark Stores Ltd v Lollypop Clothing Ltd [2001] FSR 637, below.

than the second word ‘Cola’ would remain in the average memory. If so, by
the same reasoning, the distinctive and memorable word in ‘Pepsi-Cola’,
would be the first word ‘Pepsi’ and not ‘Cola’. Hence, no infringement. In
Schieffelin & Co v The Jack Co of Boca Inc31 the claimant owned the trademarks
in ‘Dom Perignon’ and the shield design label appearing on its champagne
bottles. The defendant used ‘Dom Popingnon’ and a similar shield in
relation to popcorn, also sold in champagne bottles. The court comment-
ed that ‘the test for determining similarity was whether the respective
marks convey the ‘same general overall impression’ to the purchasing
public when viewed separately. Ultimately, the crucial question is whether
the similarity is likely to cause confusion’.32 Though the champagne and
popcorns were not similar, the court observed that the two marks and
shields were strikingly similar on both auditory and visual levels and,
therefore, granted injunctive relief. In Sabel BV v Pauma AG33 the ECJ held
that: ‘the global appreciation of the visual, aural or conceptual similarity of
the marks in question, must be based on the overall impression given by the
marks, bearing in mind, in particular, their distinctive and dominant
components, in the perception of the average consumer.’ Avnet Inc v Isoact
Limited (Avnet)34 involves the use of an identical mark but in relation to
different products. Avnet Inc, a business that carried advertisements for
different manufacturers in the US, also owned the trademark ‘Avnet’ in the
UK for advertising services. Isoact Ltd, is an Internet Service Provider (ISP)
with particular interest in aviation that used the words Aviation Network
and Avnet in its business. Isoact registered ‘avnet.co.uk’ as a domain name and
allowed others to place advertisements on its site. Avnet Inc alleged
that the domain name registered by Isoact was identical to their
trademark used in connection with identical services, within the meaning
of S.10(1). Jacob J refused Avnet Inc’s application for summary judgement
on the grounds that there was no confusion; the parties were engaged in
different businesses, Avnet Inc. in the business of advertising (class 35) and
Isoact in business as Internet Service Providers (if registered, probably class
42). Reed Executives PLC v Reed Business Information Ltd35 concerns the use of
different domain names but confusion was held to arise from the use of
megatags. The claimants founded in 1960 run employment agencies
through a network of high street branches. They are registered holders of
the trademark ‘Reed’ in respect of ‘Employment Agency Services included
in Class 35’ and operate the ‘reed.co.uk’ website. The defendants used the
word ‘Reed’ in relation to their publishing business since 1983 and

31 850 F Supp 232 [SDNY 1994].
32 At p.244, and at p.245 the court observed that champagne and popcorn were different products;
though the goods were ‘related in use’ they did not ‘serve the purposes, fall within the same class, or used
together.’
operated the ‘totaljobs.com’ website where the defendants posted vacancies advertised in their publications. The word ‘Reed’ incorporated in the defendant’s logos was prominently displayed on their website and was also used as one of a list of metatags, which, although not visible to the eye, was readable by search engines responding to key word or phrases typed in by the user.\(^{36}\) The court had to determine whether the claimant’s registered trademark is sufficiently wide to cover the defendant’s provision of services through the medium of totaljobs.com. That is, are the services and the mark identical or similar and if similar is there confusion? Justice Pumfrey found that the activities of the claimant and the defendant were similar because, as with the claimants, ‘totaljobs.com acts as a go-between clients and candidates.’ That is not all, Justice Pumfrey had no doubt that the use of the word ‘Reed’ in relation to the visible logos and copyright notice as well as the invisible metatag is capable of causing confusion. He said: ‘the concept of use is wide enough to cover invisible use in metatags which is visible in the search result. . . .the short test, which must be applied with caution, is whether the sign tells the truth about the site.’\(^{37}\)

Is association tautology for confusion?

Where the competing marks are only similar S.10(2) (b) requires that there must also be a ‘likelihood of confusion . . . which includes the likelihood of association’. What is not clear is (a) whether similarity of products by itself constitute confusion, (b) whether association is an alternative for confusion and (c) whether association is restricted to classical association as to origin or extends to mere association implying simply the existence of organisational or economic links.

The relationship between similarity and confusion was raised \textit{British Sugar v James Robertson}\(^{38}\) where both parties included the word ‘Treat’ in their trademark. British Sugar, producers of a range of sugar related products, registered the trademark ‘Silver Spoon Treat’ used as syrup topping for ice creams and other desserts. James Robertson, manufacturers of a range of jams, produced a toffee-flavoured spread, which they sold alongside Robertson’s other range of jams, as ‘Robertson’s Toffee Treat’. British Sugar contended that the similarity of the products was sufficient to constitute confusion within the meaning of S.10(2) (b). Rejecting the argument Jacob J said: ‘The sub-section does not merely ask ‘will there be confusion?’: it asks ‘is there similarity of goods?’’, if so, ‘is there

---

\(^{36}\) Search engines are a website, which will on request ‘crawl’ the Internet and return list of other sites containing a particular word or phrase typed into the search window by the user. In order to respond quickly, search engines maintain vast indexes of words and pages (not merely sites) which contain the words. Website owners wishing to rank high on the list returned seek to have specific words included in search engine directories, which they then incorporate into metatags—the invisible component of the website.


\(^{38}\) [1996] RPC 281.
likelihood of confusion?’ The point is important. For if one elides the two questions then a ‘strong’ mark would get better protection for a greater range of goods than a ‘weak’ mark. For instance, ‘Kodak’ for socks or bicycles might well cause confusion, yet these goods are plainly dissimilar from films or cameras.’

Cases that followed British Sugar further defined, and restricted, the meaning of confusion; confusion, they held, must exist in the relevant market place. In the context of the Internet in 1–800 Flowers Jacob J suggested that a fishmonger in Bootle using the web as a shop window does not want to sell fish to the entire world. Similarly anyone who accesses a web page but does not live in Bootle or does not want to buy fish will realise that they are not the target audience and move on.39 Though there may be no confusion as to the ownership of the page itself confusion may still arise if the contents suggest a relationship where none exist. In Musical Fidelity Limited v David Vickers40 the claimant, M, was a manufacturer and supplier of hi-fi equipment, and registered holder of domain names incorporating variations of the words ‘musical fidelity’. The defendant, V, who had at one time been an authorised distributor for M’s products, set up a web site at ‘www.musicalfidelity.co.uk’. V’s homepage was distinctly headed as ‘Vickers Hi-Fi’ but was followed by the words ‘Welcome to the website of one of Musical Fidelity’s oldest retailers’ (self-emphasis) and promoted itself as ‘The North of England Hi-Fi Specialists’. M alleged that V’s use of the domain name amounted to a passing off and also infringed M’s trademark. M argued the words ‘oldest retailer’ falsely suggested that V ‘was and is’ one of M’s authorised distributors when he is not. Rimer J held that V had no defence to an action for passing off and, contrary to S.10(1), that V used in the course of trade a domain name identical with M’s registered trademark in relation to identical goods.

The issue of similarity of products and confusion as separate questions seem well settled; one must ask whether the products are similar and, if so, then ask whether the similarity is so close as to cause confusion. Even so, there remains the relationship between confusion and association; is association infringement in its own right or is it inclusive in the element of confusion? S.10(2)(b) is based on Article 4(1)(b) of the EC Trade Mark Harmonisation Directive 1988 which is itself founded on Benelux law and a decision of the Benelux court in Claeryn/Klerin.41 The products in this case were gin and detergent. The claimant had demonstrated that though a customer was unlikely to confuse the origin of the two products on seeing the defendant’s mark the same customer would ‘call to mind’ the registered mark of the claimant; ‘association’ but not ‘confusion’. The

Benelux approach endorses the commercial realism that a trademark is more than a badge of origin and is capable of creating goodwill of its own, independent of the source of the product. Do and indeed should the English courts, and for that matter the ECJ, recognise the enhanced concept of the trademark, or does it cling on to the traditional idea of the trademark as a badge of origin? In Wagamama Ltd v City Restaurants Plc, Laddie J found ‘little justification for any such extension’. The defendants applied to register the name ‘Rajamama’ in relation to an Indian-themed restaurant. The claimant who owned the trademark for ‘Wagamama’, a Japanese word used in relation to a Japanese-style noodle bar in London, objected to the application. Laddie J concluded that ‘the likelihood of association’ was indeed a tautology and did not add anything to the ‘likelihood of confusion’. Laddie J referred to Deutsche Renault AG v Audi AG where the ECJ spoke of a ‘direct risk of confusion’ in the classical sense of association as to origin and the ‘risk of confusion in the broader sense’. Laddie J rejected the latter because if the broader scope were to be adopted ‘our Act would be creating a new type of monopoly not related to the proprietor’s trade but in the trade mark itself.’ Since the decision in Wagamama the ECJ has concluded on Sabel BV v Puma and, in the context of S.10(3) the English courts have ruled on Baywatch, One in a Million and Oasis Stores. In Sabel BV v Puma AG both marks depicted a leaping puma and both were registered in respect of leather goods and items of clothing. Relying on Article 4(1)(b), which is almost identical to S.10(2)(b), Puma opposed Sabel’s application. A dictum in the judgement remarked that the mark could be infringed even though there was no likelihood of confusion. However, despite the dictum, the primary finding was that in the absence of confusion, mere association between the two marks is not infringement. The court observed that the words ‘which include’ between the words ‘confusion’ and ‘association’ could be construed only in one way; the likelihood of association is not an alternative to but served only to clarify the meaning of confusion.

2.3 Quandary in the courts: Has trademark law strayed from its path?
Reputation overreached confusion and mere ‘calling to mind’ deemed association!

---

[82] [1995] FSR 715.
[83] Deutsche Renault AG v Audi AG [1995] I CMLR 461 at 483, 484 acknowledging protection from association as to origin the court said: ‘… there is a risk of confusion between two trademarks not only when the trade concerned might mistakenly assume that the goods concerned come from one and the same undertaking (direct risk of confusion) but also when the mistaken assumption relates to the existence of an organisational or economic link between the undertakings concerned, such as a licensing agreement under which one undertaking is authorised to manufacture a product with the same properties as the product of the other (risk of confusion in the broader sense).’
[84] Note similar concerns expressed by Jacob J in British Sugar.
[85] [1998] RPC 199.
And, finally, reputation in S.10(3): does the mark have reputation in the UK that is due to its distinctiveness and is ‘confusion’ a factor? S.10(3) pivots on use that ‘takes unfair advantage of’ or ‘is detrimental to’ the reputation of the trademark, hence, the twofold protection is of the trademark itself. This, unfortunately, at least in principle, spells the beginning of the end and ushers the protection of the trademark per se rather than the trademark as a badge of origin.

But, first, what degree of reputation is required, and, in the context of the Internet, can access in the UK generate reputation? The Athlete’s Foot Marketing Association v Cobra Sports\(^46\) and Sheraton Corporation v Sheraton Motels\(^47\) cases concerned the presence of ‘good will’ in an action for passing off. In Athlete’s Foot the American business had a reputation in the UK but had no customers and therefore could not prevent the UK retailer from selling shoes under the same name. Walton J ruled that the complainant need not actually carry on business in the UK ‘provided they have customers here’. In Sheraton, the claimants run a chain of high-class hotels in the US, but at the time had no hotels in the UK. The court granted an interim injunction preventing the defendants from using the name ‘Sheraton Motels’ because the claimants had established sufficient ‘good will’ through hotel bookings frequently made by agents in London. In ascertaining whether the mark has reputation in the UK, guidance may be sought from General Motors Corporation v Yplon.\(^48\) This was a reference from the Belgium courts to ascertain whether General Motors owning the sign Chevy for motor vehicles could restrain Yplon from using an identical sign for detergents.

The ECJ stated that ‘a mark would have a reputation where it was known by a significant part of the public concerned by the products or services covered by the trade mark.’\(^49\) The Court also suggested a number of different criteria including ‘the market share held by the mark.’\(^50\) As with good will in an action for passing off, reputation in the context of registered trademarks is not assessed merely by general public knowledge of the mark but rather reputation of the mark in relation to the specific products or services covered by the mark.

Taking ‘unfair advantage’ is a remnant of passing off, recalling the concept of a ‘free rider’ in circumstances where ‘the plaintiffs have done nothing to deserve this detriment, nor the defendants this benefit.’\(^51\) Use that is ‘detrimental to’ the repute of the mark occurs where the ‘value added by the mark was, or was likely to be, reduced.’ In effect, S.10(3)
emulates the American notion of dilution defined as ‘the blurring of a mark’s product identification or the tarnishment of the affirmative association a mark has come to represent.’ In Madgecourt Ltd’s Trade Mark Application\textsuperscript{52} Madgecourt applied to register the words ‘MCL PARFUMS DE PARIS’ for goods including soaps, toiletries, perfumes, suntanning preparations and dentifrices to be manufactured in the UK. Federation Des Industries La Parfumerie (FIP), an association of French perfumeries, contended that unless the goods were actually manufactured in Paris or by a Parisian company the offending mark would suggest a false indication as to origin and thereby cause confusion in the minds of the public. The applicant’s declared intention to obtain perfume oils from France did not impress the Trade Mark Registry. The registry took judicial notice of the international reputation for perfume enjoyed by France, and Paris in particular, and decided that the words ‘Parfums de Paris’ created an expectation, which was not true. Nevertheless, the registry allowed the registration in respect of dentifrices to proceed thus displaying both a willingness to take judicial notice of reputation but also a determination to curb the scope of trademark and contain the mark’s protection to the product for which it holds an established reputation. Strange as it may be, the likelihood of confusion’ is required in S.10(2)(b) where the product could be identical or similar but not expressly required in S.10(3) where the sign is used with products that are not even similar. In cases, represented by Baywatch Productions Co.Inc v Home Video Channel\textsuperscript{53} and BASF Plc v CEB (UK) Plc the English courts removed the inconsistency by extending the requirement of ‘confusion’ to S.10(3). But, the picture is far from clear. In opposition proceedings in Oasis Stores Ltd v Ever ready Plc James J ruled that it was possible for the damage referred to in S.5(3) to occur without the likelihood of confusion. And, in Canon Kabushiki Kaisha v Metro-Goldwyn Meyer\textsuperscript{54} the ECJ slighted the issue of confusion. It held that the ‘registration of a trademark may have to be refused, despite the lesser degree of similarity between the goods or services covered, where the marks were very similar and the earlier mark, in particular, its reputation is highly distinctive.’\textsuperscript{55}

Market strategists justify the different approaches in British Sugar and Canon by what they classify as ‘complimentary products’ where one can not function without the other. In Canon a video film has no function without a video recorder but in British Sugar whereas toppings are a condiment for desserts a spread is served as a breakfast component. Nevertheless, one has

\textsuperscript{52} [2000] ETMR 825.  
\textsuperscript{53} [1997] FSR 22.  
\textsuperscript{54} [1999] ETMR 1.  
\textsuperscript{55} [1999] ETMR 1 at para.19. In Canon Metro-Goldwyn Meyer had applied to register the mark ‘Cannon’, with a double ‘n’, for video film cassettes in Germany despite Canon’s established reputation for video recorders.
to ask whether the courts adhere to the notion of ‘confusion’ as the basis for trademark protection or yield to commercial pressure and display a willingness to shift the emphasis from reputation in the product to reputation of the trader; from confusion in the minds of the public to the reputation of the mark itself.

3 The Uniform Dispute Resolution Policy and reform

3.1 What is new in domain name disputes?

Browsers and erosion of geographic boundaries intensified scramble for notable names.

If domain names are functionally different and the use of search engines make it less likely for the user to be confused in the trademark sense why are there domain name disputes? There are three underlying reasons; first, legislation enacted for the terrestrial world in yesteryear is not necessarily applicable to the cyber world. Second, it is arguable that domain names are used as and are, at least unregistered, trademarks. Third, and most significant, is that domain names are global and unique.

A domain name is truncated into the self-selected Second Level Domain (SLD) and the pre-determined generic Top Level Domain (gTLD) the latter being country coded or universal. ‘efax.com’ and ‘efax.co.uk’ being two commercial examples. In this instance, ‘efax’ representing the SLD goes to the root of the problem: first, ‘efax.com’ is more memorable than ‘efax.co.uk’ hence the gold rush for the universal ‘dot.com’. Whether the ‘dot.com’ or the ‘dot.co.uk’ ‘efax’ is spelt the same and sounds the same. Whilst the computer can distinguish between the two variant in the mind of the user both appear to be the same, hence, the likelihood of confusion. Whereas trademarks are country and product specific domain names are global and generic; trademarks that were logically separated into country and product trademarks incorporated into domain names converged into globally unique namespaces. Accepting that business is all about creating an image, the scramble for and willingness to litigate over ‘unique namespaces’ is not surprising. Broadly, three types of disputes have crowded the courts; legitimate claim or good faith, free speech or fair use and cyber squatting or cyber typo.

Legitimate use is represented by cases like Pitman and Prince. Pitman Training Ltd v Nominet UK56 concerned the name ‘Pitman’ in which Pitman Training and Pitman Publishing, a subsidiary of Pearson plc, were until 1985

---

part of the same business. ‘Pitman.co.uk’ was initially allocated to Pitman Publishing but, in error, was later allocated to Pitman Training. In accordance with Nominet policy giving priority to the first registrant the court restored the name to Pitman Publishing. In Prince plc v Prince Sportswear Inc\textsuperscript{57} the UK IT and the US sportswear businesses were the registered trademark owners of ‘Prince’ in their respective products and countries. Prince Inc alleged that ‘prince.com’ was allocated to Prince plc by InterNic, US, diluted Prince Inc’s Federal trademark. In proceedings commenced by Prince plc, the UK court upheld Prince plc’s challenged and InterNic kept ‘prince.com’ for Prince plc.

Bad faith/abusive registration or cybersquatting occurs where the name was registered, acquired or used in a manner which took unfair advantage of or was unfairly detrimental to the complainant’s rights.\textsuperscript{58} Squatting is not new; Harrods Ltd v UK Network Services Ltd\textsuperscript{59} is a cyber version of Harrods Ltd v Harrod Ltd.\textsuperscript{60} Perhaps the best known, and more relevant, UK case is British Telecommunications Plc v One In A Million Ltd and Others.\textsuperscript{61} The defendant had registered a number of well-known names as domain names, and admitted their intention to sell the same to the highest bidder. But they contended (a) that people with names like ‘Sainsbury’ and ‘Ladbroke’ could have a legitimate interest in the domain name and, if so, registration by itself could not be deceptive; and (b) that registration by itself did not denote ‘origin’ and therefore there was no ‘use’ in a trademark sense. The High Court ruled that (a) declared intention to sell constituted ‘use in the course of trade’ and (b) the mere existence of a domain name similar to a well-known name raised the risk of deception. In agreement, the Court of Appeal concluded that placing of a household name such as ‘marksandspencer’ on the Internet suggests an association with the name and its good will, sufficient to justify injunctive relief.

The practical consequences of the decision are hardly questionable and, indeed, are welcome. Nevertheless, the emphasis on the reputation of the trader rather than the reputation of the trader in the product sets a dangerous precedent. First, ‘intention to sell’ was held to constitute ‘use in the course of trade’. But, though a non-exhaustive list the guidance offered by S.10(4) directs that the trademark must be used in relation to a product whether affixed to a product or in the course of advertising. Second, the decision that the mere existence of a domain name similar to a well-known trademark raises the risk of deception goes far beyond any decision to date.

\textsuperscript{57} [1998] FSR 21.
\textsuperscript{58} Nominet’s Dispute Resolution Policy Paragraph 1. Reverse domain name hijacking is where the claimant attempts to have transferred to itself a domain name legitimately registered by another. See, for instance, Société Des Produits Nestlé SA v Pro Fiducia Threuhand AG (Case No. D2001–0916) [2002] ETMR 32 –determined by WIPO Arbitration and Mediation Center.
\textsuperscript{59} [1996] RPC 697.
\textsuperscript{60} [1924] 41 RPC 74.
\textsuperscript{61} [1999] RPC 1.
The fact remains that if such a domain name were accessed by users, search engines make the risk of confusion highly unlikely and even if a search engine were not used the web page would surely be blank and so a user could not be deceived. Third, by the same token confusion by 'association' too is unlikely. This is because even if users were led to believe that the domain name was registered by the true holder of the trademark association is not merely the ‘calling to mind’ but must relate to association as to origin, classical association. 62 Desirable though the decision in One in a Million may have been practical decisions do not necessarily make good laws. In Madgecourt the Trademark Registry took notice of the international reputation enjoyed by France but only in so far as the industry had an established reputation; namely, only in relation to perfumes. Yet, in Canon the ECJ has elevated the significance attached to ‘reputation’, in Claeryn/Klerin 63 the Belgian courts extended association to association by way of ‘calling to mind’ and in Panavision v Toeppen 64 the American courts declared that registration with intention to sell amounted to commercial ‘use’. Are the UK courts in danger of following suit; interpreting the Trademarks Act in the spirit of the US’s Federal Dilution Act 1995 and the Anti-cybersquatting Consumer Protection Act 2000, 65 is ‘reputation’ surpassing ‘confusion’ as a criterion for trademark protection?

3.2 Has the Uniform Domain-Name Dispute-Resolution Policy failed? 66

The UDRP designed to cope with cybersquatting is not the panacea for all disputes. The UDRP is adopted by most registries and is written into the Registration Agreement between the Registration Authority and the domain name holder. Proceedings before accredited dispute-resolution panels under the UDRP may cover registered as well as unregistered marks and names protected by common law action for passing off. 67 Paragraph 4 sets out the circumstances obliging the parties to submit to administrative proceedings

---

62 Note rejection of association by ‘calling to mind’ in Wagamama, Deutsche Renault AG, and the ultimate decision in Sabel v Puma.
64 954 F Supp. 1296, 2 ECLR 789 (DC Calif.1996).
65 FDA 1995 protects against dilution of the mark per se and the ACPA 2000 requires bad faith but if the registration is by a ‘professional dealer’ there need not be commercial ‘use’.
66 When registration of gTLDs passed from Network Solution Inc. to ICANN to be shared by the regional registries the dispute resolution policy met a similar faith. ICANN established the Uniform Domain-Name Dispute Resolution Policy often referred to as UDRP which came to be adopted by most regional registries. See ‘http://www.icann.org/udrp/udrp.htm’ for WIPO sponsored panels, ‘http://www.internic.net/’ for NIS and ‘http://www.nominet.org.uk’ for Nominet policies.
67 ICAN sponsored arbitration panels are WIPO based in Geneva, Switzerland, National Arbitration Form (NAF) in Minneapolis, Minnesota, eResolution in Quebec, Canada and CRP Institute for Dispute Resolution in NewYork, USA. Nominet, the UK’s registration authority, has adopted the UDRP but offers its own Dispute Resolution Service (DRS).
and includes a non-exhaustive list of ‘bad faith registrations, but access to
the courts before, during or after the proceedings are not excluded.68

The advantage of the UDRP is that whereas foreign decisions are subject
to multilateral treaties as well as public policy, as an arbitration tribunal,
decisions of the UDRP sponsored panels are enforced as decisions of the
country in which enforcement is sought.69 The weakness is that there is no
 provision for mediation or appeal, and it is also said that administrative
tribunals tend to favour challengers already holding a trademark. Nomi-
net, the UK’s registration authority, devised its own Dispute Resolution
Policy. On the whole, Nominet replicates the UDRP but differs from it in
 three respects: Nominet is itself involved in the proceedings, it provides for
a system of appeal and incorporates a system of mediation. The greatest
criticism against both systems, however, is that they are designed to deal
with cybersquatting; for instance, both could resolve One in a Million but
not Prince plc.

3.3 Has trademark law served its purpose?
Declare ‘confusion’ as a dominant factor and index link or country code domain
names.

In essence, this article traced the evolution of trademarks from a mark
denoting ownership to a source of origin and then re-aligning itself as a
mark conveying quality, value and authenticity. The precise scope of
trademarks remains unresolved. The decisions of the ECJ and of Laddie J
in Arsenal FC stand at opposite ends as do the decisions in Arsenal FC and
Primark Stores Ltd v Lollypop Clothing Ltd.70 In Arsenal FC the ECJ opined that
the notice informing buyers that the memorabilia is not official and that
the public perceived the memorabilia as a badge of loyalty is immaterial.
The court explained that persons coming across the goods later would be
mislead because they would not be aware of their source. Hence, the ECJ
confirmed the mark as an indication of origin but concluded that the use of
the mark infringed because the goods or services bearing the mark have
been manufactured or supplied under the control of a single undertaking
which is responsible for their quality and authenticity. Emphasis on control
of a single undertaking is reflected in Primark where Lollypop sold jeans
manufactured to Primark’s specifications, supplied by Primark’s author-
ised manufacturer but without having first passed Primark’s quality
control. Echoing the ECJ’s decision in Arsenal Pumfrey J ruled that
although the defendant’s jeans were not counterfeit jeans, because the
claimant had no opportunity of verifying their quality the jeans did not

68 Individuals with famous names can turn WIPO and access the UDRP as did the actress Julia Roberts or
69 In Telnikoff v Matuszewich [1991] 1 All ER 817 the claimant succeeded in an action for defamation in the
UK but for policy reasons could not enforce the judgement in the USA.
70 [2001] FSR 637.
originates from the claimant either, thus infringed the trademark of the owner.

Disputes are not new to the Internet but the Internet propelled the e-merchant onto the global arena and thus intensified the battle for zealously guarded trademarks, now registered as domain names. The last 150 have demonstrated that even identical trademarks could co-exist in different countries or in relation to different products. Recently, similar outcomes have been recorded in relation to domain names; ‘efax.com’ failed to prevent ‘efax.co.uk’ from using an identical name for electronic fax services and ‘mbna.com’ was registered to a Mr. Freeman, not the bank. Yet, in the last 10 years the courts have been inundated with domain name disputes commenced by claimants coveting global monopoly unrestricted by product classification.

The basis of passing off, followed through into the Trademarks Acts, remains the claimant’s reputation represented by the mark, and misrepresentation by the defendant causing confusion in the minds of the purchasing public. Though some decisions were cloudier than others were, on the whole, good will/reputation meant not mere knowledge of the mark but of a representation by the mark, measured by the market share held in the UK.\(^{71}\) Moreover, though the word does not appear in S.10(3) the *Baywatch* line of cases introduced confusion as a requirement. So far the courts have insisted on reputation represented by the mark and unauthorised use likely to cause confusion in the minds of the public. Passing off and trademark law has served us well because hitherto reputation has been subservient to and did not override confusion. But, in the challenge between co-existence and global monopoly, symbolising consumer versus trader interest, how are the courts to meet the dilemma created by commercial realities and cybersquatting?

A global directory of domain names and a search facility through a common interface had been suggested but that would only prevent the registration of names that were identical or similar to names already on the register. It would not work against pre-emptive registration. The alternative was the increase in the gTLDs. Whilst the increase of gTLDs from 6 to 12 doubled the space for identical or similar SLDs registrants had simply taken the opportunity to register the SLDs in different variations of the gTLDs and consequently multiplied domain name disputes.\(^{72}\) Defensive registration was designed to counteract attempts by cybersquatters to register the desired SLD in a variant of the gTLD. Admittedly, the basket of

---

\(^{71}\) Sheraton Corporation v Sheraton Motels, Athlete’s Foot Marketing Association Inc v Cobra Sports and General Motors Corporation v Yplon.

\(^{72}\) A press release on 26th February 2002 confirmed that the creation of new gTLDs had increased complaints to WIPO by 100% in the last quarter of 2001 adding that new gTLDs and the opportunity to register domain names in non-ASCHII characters such as Chinese have ‘created new opportunities for cybersquatters.’
registered domain names widen the scope of protection for the registered holder but it also leads to the scarcity of name spaces making cybersquatting even more attractive. Instead, the technology that spearheaded globalisation could also provide the solutions.

The third option, advocated here, is that without necessarily changing the law the courts and business business could facilitate co-existence on a global scale whilst at the same time obviating ‘the likelihood of confusion.’ The courts could discourage litigation by restricting the meaning of ‘association’ and ‘reputation’, and insisting that ‘confusion’ forms the hub of any successful claim. Earlier registration could still be a criteria in determining priority but the courts could take greater account of the actual reputation and the likelihood of confusion because of the reputation that the mark of either party has in relation to the specific product in question. Some businesses already engage in voluntary cross-linking arrangements whereby holders of similar domain names share a website or intermediary homepage and redirect visitors to the other’s sites as appropriate. For instance, Playtex Apparel Inc and Playtex Products Inc share the intermediary homepage ‘www.playtex.com’ and license the use of their respective trademarks on the shared website. The practice could be extended if encouraged by the judiciary. Although reversed on appeal, in ‘zumpolle.nl’ the District Court of The Hague set aside the first-come-first-serve rule for domain name registrations, even though there was no infringement of intellectual property rights. The dispute involved two shops called ‘Zumpolle’ selling leather goods, originally owned by the same person and established at about the same, one in The Hague and one in Amsterdam. Zumpolle Amsterdam commenced proceedings to obtain the domain name ‘zumpolle’ already registered by Zumpolle at The Hague. The District Court ruled that the best interest of the companies and of the public would be served if the current holder placed a notice informing visitors to the site that another independent Zumpolle store operated in Amsterdam and provided a link to Zumpole Amsterdam’s (future) website. Regrettably, the Court of Appeal of The Hague disagreed and granted exclusive use of the domain name to the first registrant.

Domain name registrars too can play their role. Accepting the premise in Avnet that reaching a wrong web site does not confuse a surfer, domain name registrars could minimise the risk of confusion either by adopting

---

73 A narrow interpretation by the courts would, for instance, make it possible for ‘avnet.com’ to continue selling goods by catalogue and ‘avnet.co.uk’ to be registered as an Internet Service Provider because the parties trade in different product. Similarly, in Canon Metro-Goldwyn Meyer would be able to register ‘cannon’ as a trademark both because of the difference in the products and because Cannon has no reputation in video film cassettes.

74 Jacob J observed that a user who used a search engine is not likely to be mislead by arriving at a wrong site because as soon as he discovers that he reached a wrong site he will click on the back icon and move on. Indeed, the user who relies on a list generated by a search engine is unlikely to visit each URL on the list. Instead, the user will be guided by the abstract appearing below each URL than the URL itself.
the practice used in registering trademarks – adopt country code and product classification, imposing a cross-linking provision in their contract with applicants, or index-linking identical or similar domain names. Using Avnet as an example the alternatives may be explained as follows. First, indexed linking; ‘avnet.com’ is registered simply as ‘avnet’ without the ‘dot.com’ and is then transformed into a common homepage comprising of links to all ‘avnet.dot’ registrants. Registrants listed on the homepage are then required to use a limited number of words to describe their site for the benefit the user, in the same way that search engines produce a list and an abstract below each URL. Second, classified registration. In this instance registration of a domain name would be country coded and classified according to the goods or services offered. For instance, Avnet advertising would be registered as ‘avnet(35).co.uk’ and Avnet the Internet service provider would be registered as ‘avnet(42).co.uk’. Global registration could be facilitated through WIPO as if it were a country-coded trademark. Indeed, at regional level, trademark registrations could be deemed as domain name registration and vis-a- versa. Cross-linking would alley fears of confusion of parties having legitimate interest in the name and index-linking would effectively rule out the threat posed by cyber squatters.
Consumer Privacy, On-Line Business and the Internet: Looking for Privacy in all the Wrong Places

Lilian Edwards

Abstract:

Consumer choice and power is enhanced by the Internet but simultaneously consumer privacy is threatened. Privacy can be protected or ‘regulated’ online, as Lessig theorises, by the market, norms, law or ‘code’. This article argues that although none of the first three modes of protection are satisfactory, this does not mean ‘code’ solutions such as P3P should be embraced uncritically. The true answer may be that consumers are simply prepared to sacrifice privacy on-line to embrace the correlative advantages but this choice is uninformed and does not prevent fears about privacy impacting on consumer confidence in e-commerce. A new effort must be made not to abandon law as unenforceable in dealing with problems such as spam and privacy, but to explore how it can be amended and globally harmonised to provide sanction and backing to self regulatory and technical solutions.

1 Co-Director of the A4RB Centre for Intellectual Property Law and Technology. Senior Lecturer, University of Edinburgh.
1 Introduction: the opportunity and the problem

‘You do a survey and consumers say they are very concerned about their privacy. Then you offer them a discount on a book and they’ll tell you everything.’

Esther Dyson, *Wired*, April 9 2002

The Internet is widely regarded as a positive force for the empowerment of consumers. Goods can be bought from a far wider section of vendors, both local and foreign, than was ever previously possible for an individual consumer; this has helped to break down artificially high domestic prices and spur on competition. Price and quality comparison are enhanced by technologies such as 3D modelling and services such as price comparison search engines. Less abled and empowered consumers such as the old, sick, rural dwellers, and children, will find access to goods vastly improved by the web. The one-to-one nature of the Internet combined with other new technologies such as the .mp3 music file compression format and digital archiving allows access to bespoke goods and services, such as personalised CDs, newspapers, clothes, etc which would previously have been the reserve of the rich (if available at all). Information about almost all topics can be sourced for free at the click of a mouse, hugely enhancing consumer know-how and shopping savvy.

But what the Internet gives with one hand it often takes away with the other. Although the Internet has empowered consumers, it also poses a serious threat – perhaps the most serious current threat – to their privacy. On line businesses, and Internet service or access providers (hereafter, ‘ISPs’) providing goods, services and information on-line typically collect, process and store vast amounts of personal information about consumers, often without their knowledge or consent. Often the real reason services are provided – apparently – for free is just so as to collect such data. Personal data – such as consumers’ names, ‘real world’ addresses, ages, family, marital, employment and income status, shopping habits, web-surfing habits, nationality etc – is of enormous commercial value, particularly when used to create both identifying and anonymised profile detail about typical consumers. Indeed such data be one of the biggest (or sole) assets of ‘dot.com’ companies, which often have little in the way of fixed assets or capital. Customer databases have already figured as a

---

2 Parts of this article appeared in an earlier form in Edwards L. and Howells G. ‘Anonymity, Consumers and the Internet: Where Everyone Knows You’re a Dog’ in Nicoll C., J.E.J. Prins and van Dellen M.J.M. eds *Digital Anonymity and the Law* (T.M.C. Asser Press, 2003). My thanks to Prof. Geraint Howells for his contribution to this research.

3 *Infra*, n.69.
controversial asset in the many dot.com bankruptcy proceedings that have fallen out after the bursting of the dot.com bubble in 2000/01. For example, when Egghead Software was sold to Fry’s Electronics in 2001, for example, its only major asset apart from some IP rights was acknowledged to be its database of 4 million customers and the price paid was $10 million. Furthermore, advanced technologies of ‘data mining’ increasingly allow new information, both about individuals and collective populations, to be generated from personal information databases.

Since consumers rarely appreciate the value of their personal information in aggregate, nor how websites collect, process and generate data, they are ill prepared either to protect their privacy or to bargain with it. They do, however, report unease around use of the Internet for commercial purposes, which can be connected to feelings of lack of knowledge and loss of control when they give information away on the Net. They have little or no confidence in either getting co-operation from companies who have collected the data or from courts in seeking redress. To make matters worse, consumers are by no means unaware that data supplied to a particular website may not only be used by that company, if only because they suspect the junk email or ‘spam’ they receive must somehow be connected. In mergers and acquisitions, databases of personal data may end up being shared with or passed to persons or companies who were never contemplated by the data subjects when the information was originally collected. Customer ‘profiles’ can be built up, which allow organisations such as DoubleClick, the leading supplier of on-line banner and pop-up advertisements in the world, to target specially-chosen advertisements at particular consumers as they surf particular pages of particular websites. When the type of data typically collected from website browsers, is combined with ‘real world’ information held in various databases, then not only can its value increase dramatically, but the risks to personal privacy increase correlatively. For such reasons, the contentious attempt in 1999 by DoubleClick to acquire Abacus, holder of the world’s largest conventional direct marketing database, was greeted with such hostility by privacy activists that the company was forced to deny any plans to merge the data in their respective databases. More recently, as a result of further investigation into privacy breaches, in August 2002, DoubleClick

---


7 Ibid, pp 26–29.


was forced to adopt new privacy related measures imposed by the Federal Trade Commission (FTC), and to pay $450,000 in settlement. Reports of scandals about data collection and database merger without knowledge or consent of the consumers involved continue to fill the pages of the online trade press, yet little or nothing seems to change despite various legal, regulatory, technical and rhetorical responses. Below we examine the various regulatory and technical solutions currently on offer to meet this ongoing crisis of confidence in on-line privacy.

Whenever we look at consumer privacy as an issue, the factor of consumer confidence or trust must be noted as a major driver in the growth – or failure – of e-commerce, especially in Europe where particular weight has been placed on it by the European Community. Surveys show again and again that consumer confidence in the electronic medium is weak. A major UK National Consumer Council report, e-commerce and consumer protection (hereafter ‘the NCC report’) found in August 2000 that 85% of UK consumers felt safest shopping on the High Street and over a third felt the Internet was the riskiest place to shop. Similar results have been consistently reported elsewhere. A survey on cross-border shopping by the Department of Trade and Industry (DTI)(not limited to Internet purchasers) in October 2002 similarly found that a third of those questioned would not purchase on the Web because of fears about credit card fraud while 20% also cited fears about disclosing personal information. Although a third of those questioned had bought goods from abroad in the past 12 months, over half (55%) said they would never use the Internet to buy goods or services from abroad.

This article, drawing on the theoretical structure suggested by Lawrence

---

10 ‘DoubleClick Loses Its Cookies’, Wired, August 26 2002.
11 Most recently at time of writing, claims are again being made that Microsoft Passport, Microsoft’s ‘wallet’ for holding personal information is insufficiently secure and thus threatens consumer privacy: see Associated Press report, May 9 2003.
13 See for example the May 2000 survey by the Federal Trade Commission, Privacy Online which found that 92% of US consumers were concerned about the possible misuse of their personal data when shopping on-line (‘FTC, 2000’). The Bertelsmann Foundation Internet User Survey, also 2000, covered Australia and the US as well as Europe and found that consumers considered loss of privacy ‘the major risk’ of using the Net. A later 2002 US survey (Pew Internet & American Life Project) found that ‘Americans overwhelmingly want the presumption of privacy of privacy when they go on-line.’ An extremely useful summary of survey findings on consumer privacy to 2002, confirming this general trend across multiple countries, can be found in Bennett and Raab, chapter 3, supra n 12.
14 Other issues however, it is worth noting, had little or nothing to do with information disclosure: not being able to touch the goods, for example, was cited by 22%. This is consistent with the findings of the 2000 NCC survey.
15 Cross Border Shopping, DTI/MORI, October 2002.
CONSUMER PRIVACY, ON-LINE BUSINESS AND THE INTERNET

Lessig16 discusses how effectively consumer privacy can be regulated and what conception of privacy current regulatory attempts are built upon.17

2 On-line collection of information about consumers

How is information collected about consumers in on-line transactions? Personal information collected falls broadly into two categories: ‘visibly’ collected data; and ‘invisibly’ collected data. ‘Visibly’ collected data, as the name suggests, information the consumer consciously supplies in a particular transaction, or at least has at some point consciously made public on the Internet. Many sites require some kind of registration, usually by form, before the consumer can start interacting with the site as opposed to passively browsing it for information. Such information is at least transparent in its collection, if not always in its subsequent use. But personal data may also be collected from other visible Internet sources, but without the consent or knowledge of consumers.18 It is common practice for example, for spammers to scour the public directories of large ISPs, or Usenet newsgroups, for names of subscribers and connected email addresses. Most of the recent controversy around data collection on the Net has, however, revolved around ‘invisible’ collection of data. By this we mean data which is collected when a surfer reads or accesses a particular web page, without that surfer necessarily either knowing data is collected, or consenting to that collection. Here both collection and use of data is non-transparent. Such data is often held via ‘cookies’, small text files placed on the hard disc of the consumer/surfer’s computer terminal. Payment also provides another opportunity for websites to collect personal information. Almost all transactions over the Web are paid for using identifying technologies such as credit and debit cards. Indeed, surveys show that consumer worries about privacy and disclosure of data are particularly intense around disclosure of credit card details. The NCC report, for example, found that when consumers were asked why they thought the Internet was the riskiest method of shopping, almost half – 46% – gave as their reason the need to disclose credit card numbers. Electronic or digital cash is available which in theory can be used with complete anonymity; however it has proved unpopular with consumers

17 Note that this paper is concerned only with how far anonymity on the Internet can be used to protect consumer privacy online and not with political/free speech uses of anonymity. It focuses on the relationship between consumer and commerce, rather than citizen and state.
and is almost unused in the UK consumer market at present. Finally ISPs can in theory collect complete data on every website a subscriber has visited (though retention is a controversial issue); and suppliers of third party cookies, such as Double Click, the on line advertiser, can also amass comprehensive profiles of consumer activity across multiple websites.

2.1 Pros and cons for the consumer of disclosing personal information

If consumers identify themselves to websites and allow them to collect and use data about them, the main potential advantage is that the shopping experience becomes more personalised, bespoke and efficient. A good example of such use of technology is the Amazon.com site, which retains a note of returning customer choices and preferences, can combine orders to save postage, can retain credit card details, past orders and delivery addresses, uses customer profiling and past orders to advise on new items for sale of possible interest, and offers a convenient ordering platform in the form of a ‘shopping cart’. More generally, it has been suggested that the voluntary disclosure and exchange of information between website and customer gives some semblance of a ‘trusted’ relationship which is good both for the consumer’s confidence and the enterprise’s profits. Organisations such as Yahoo! claim to have found ‘permission based marketing’, in which no information is collected (or email sent) without the prior consent or opt-in of the consumer, the best way forward to build a successful trading relationship. The down side of disclosure for consumers is, obviously, the loss of anonymity/privacy. Most obviously, information collected by websites leads to unwanted direct marketing by email or other means such as junk faxes and cold-calling: we shall generically call this the spam problem. Secondly, businesses holding personal information may disclose it to third parties, either deliberately or accidentally with unfortunate consequences. A famous example of this occurred when Eli Lilly, makers of Prozac, the anti-depressant drug, inadvertently revealed the names of all the subscribers of a mailing list it ran for users of Prozac to all the other list recipients – a matter of obvious sensitivity. Information disclosed may also be incorrect or partial when disclosed, and thus mislead. This may be termed the the disclosure problem. Thirdly, ‘spillover’ problems may arise when data is shared between different companies or agencies, and in particular when real and virtual identities are connected. Employers might find that

---

employers know they have applied to a job elsewhere; health insurers might learn the insured is checking out AIDS sites; lovers might discover their partner has signed up to an online dating agency.

All these disadvantages rest on the idea that some specific harm may result from the invasion of privacy: whether economic or dignitary (to steal a term from the language of copyright). At a more theoretical level however, some commentators believe that personal privacy is part of the inherent dignity of a person, one of the factors that constructs him or her as a human being, and hence as an actor with rights; in that sense, disclosure of personal information, without knowledge or consent, even where it causes no obvious, concrete ‘harm’, is an assault on the dignity of the person and a breach of human rights. This can be called the human dignity problem.21

3 Forms of regulation: markets, social norms, laws and ‘code’

Here we will draw on the influential theories put forward by Lawrence Lessig in his book Code and Other Laws of Cyberspace22. Lessig argues that actions are regulated, not just by law, but also by norms, the market and ‘architecture’.23 So for example, if we look at why people do not steal, then perhaps most obviously there are laws against theft, both statutory and common law. However there are also non legal social norms – for example, responsible parents tell their children not to pick the flowers in public parks, and to hand in money found in the street to the police. The market also influences patterns of theft: for example, diamonds, or video recorders, are more likely to be stolen than say, flowers, or old clothes, because there is a ready market for them, and they have enough value to be worth the risk of stealing. Finally, by ‘architecture’, Lessig says he means ‘how [something] is, how it is designed, how it is built – in a word its architecture.’24 So in the theft example, while cars are often stolen, skyscrapers rarely if ever are.

So when we seek to regulate a phenomenon, we are not limited to law as

---

21 See further L.Lessig, supra n 16, pp 147–150; R. Wacks ‘Privacy in Cyberspace: Personal Information, Free Speech and the Internet’ in P.Birks ed. Privacy and Loyalty (Clarendon Press, 1997). Wacks asserts that most supporters of privacy tend to depend on rights-based arguments such as fulfilment of personal autonomy, while supporters of free speech tend to rest more on harm-based arguments eg the consequences for democracy of censorship. On the Internet, it seems arguments mostly revolve around the latter even in relation to privacy.

22 Supra, n. 16.

23 Ibid, p 88.

24 Ibid, p 87.
Lilian Edwards

the only mode of regulation, nor is it always the most effective way. Speeding laws, for example, are routinely flouted; but speed bumps built into the road (‘architecture’) simply exist, and cannot be ignored.

Transferred to cyberspace, Lessig’s key insight is that while the architecture of the real world is often a given, in cyberspace, architecture has always been designed. Cyberspace is built of ‘code’, in the sense of programming code – ie, of software and hardware and protocols. But such ‘code’ also operates as ‘code’ in the sense of a legal constitution, in that it regulates and sets the values for cyberspace. Hence, the abbreviation, ‘code as code’. From this insight follows the second important point, that if ‘code as code’ regulates cyberspace – in that it constrains some behaviour and enables other types, embeds some values and excludes others – then those who write code are regulating activities in cyberspace, even though they are neither democratically elected nor generally accountable. So for example, Microsoft are currently explicitly choosing to build or not build privacy values into certain of their products25 – yet Microsoft are not the representatives of anyone other than their own shareholders, nor, generally, required to pursue anything other than their own commercial interests. Lessig finds this an issue of serious constitutional concern. As we will see below, this worry is germane when we come to consider ‘code’ as having a major role in regulating data privacy.

The democratic deficit of ‘code as code’ is accentuated by the fact that in cyberspace, law tends to be unenforceable, because of the diffuse and globalised nature of the medium, while code tends to be self-enforcing. Copyright laws against digital copying, as an example, are regularly ignored; however ‘digital fences’ or anti-copying technologies are extremely difficult to ‘crack’ or circumvent for most consumers, and hence very effective. In many areas needing regulation on the Internet, therefore, it is ‘code’ rather than law, norms or markets, which is often seen as the most hopefully effective solution.

3.1 Markets

The market is undoubtedly a powerful, if imperfect, actor in consumer policy.26 Therefore one would expect companies trading on the Internet to be influenced by the privacy concerns of consumers. There are many competing approaches to privacy and data collection which could be used as marketing advantages. The main way in which website businesses tend to

---

25 See ‘Microsoft puts privacy policy on display’, August 27 2002, at http://news.com.com/2100–1023-955514.html, which recounts how Microsoft have begun to incorporate better privacy policies and procedures into new products following a settlement with the FTC who had investigated them for making misleading statements as to the privacy of their products such as the Passport authentication system. See further the European Commission’s consideration of Microsoft Passport’s compliance with privacy law in Art 29 Data Protection Working Party Document on on-line authentication services, 10054/03/EN WP 68, 29 January 2003.

26 G. Howells and S. Weatherill, Consumer Protection Law, (Dartmouth, 1995) at 1.
advise consumers what privacy options they offer as opposed to their market competitors is via their ‘privacy policy’. However, firms do not seem to be marketing their privacy options as distinctive features – indeed, many firms, especially in the UK, have no privacy policy in place at all.27

Certain basic values about information collection have become internationally accepted in this area, and one might expect market forces to operate to embed them in company practice. There are five generally recognised Fair Information Principles or FIPs, including Notice, Choice/Consent, Access, Security and Enforcement.28 Empirical evidence shows that online businesses have been slow to produce privacy policies, and even slower to conform to the FIPs with more than lip service. In its report in 2000 on the subject, the FTC found that 97% of the random sample and 99% of the most frequently accessed websites group, collected e-mail addresses or some other type of personal identifying information. 41% of the random sample and 60% of the most frequently accessed group met the basic Notice and Choice standard, but when the additional principles of Access and Security were added in (which the FTC admitted were more difficult to implement) the figures fell to just 20% for the random sample and 42% for the most frequently accessed group. As noted below, this finally convinced the FTC of the need for legislation rather than leaving privacy to the market.

In the UK, until recently there was little hard data about the provision of privacy policies, or compliance with fair processing on web sites. Privacy policies have attained a fairly high profile in the USA in recent years, as a result of action by the FTC, who view the absence of a privacy policy as a pointer towards ‘unfair or deceptive practices’ under the Federal Trade Commission Act and other fair trading legislation.29 Without similar agency involvement, in the UK privacy policies have been slow to take off. The first survey by the Information Commissioner’s Office into compliance of UK websites with data protection (DP) laws in May 2002, found that 42% of their sample of 170 web sites did not provide any kind of privacy statement, even though all sites surveyed collected at least some kind of personal, demographic or sensitive information. Of those sites that did post policies, furthermore, only about 5% of privacy statements were

28 This term, which comes from the USA, was originally limited to the first four principles, but enforcement is seen as increasingly important (and is an intrinsic part of the European regimes).
29 Privacy policies have also become more popularly known as a result of the impact of the P3P technology. See below.
30 See n 27.
31 These sites were not chosen randomly, but to represent a range of different variable, including large and small web sites, and sites collecting certain types of information, eg, sensitive information, and information from children.
intelligible to the average reader. Only 18% of sites told surfers how to access data held about them, and only 27% of sites gave any information on how to complain about privacy or misuse of data. Perhaps most worryingly, less than 40% of sites even had procedures for recording what personal data they actually held. In terms of security, only 37% of small companies had any kind of data security policy, and less than half of all companies held a back up copy of their data off-site.

The fears frequently expressed by consumers as to their privacy on the Internet would suggest that the market is not responding to consumer preferences. Why is the market not working to support consumer demands for privacy and security? One explanation may lie in the fact that although consumers say they care about privacy, they do not care sufficiently about it to let it affect their choices. This is surprising as economic theory explains that businesses will respond to consumer demands even if they are shared by only a marginal number of consumers if they represent a loss worth avoiding. Consumers may not be a lobby for privacy however because they are not yet fully aware of what they are giving away. Another explanation may be that consumers simply do not have faith that any one company’s privacy policy is better than another’s. This resembles the problem of the lemon in consumer sales law. If consumers do not have confidence that they will get quality, they simply discount all products as being defective. The flip side of these explanations is that companies may simply feel they have more to gain by exploiting data than respecting privacy. It may also be increasingly the nature of profit making businesses, just as with state bureaucracies, to collect as much detailed personal information as they can, simply because they can. It seems therefore that some mechanism other than simple market forces has to be found to establish minimum privacy standards for participants in the online market place.

3.2 Norms

Although few spontaneous norms that have arisen to protect privacy from within the e-commerce community, there has been a growth in the development of codes of conduct and seal schemes in a bid both to restore consumer confidence and forestall government intervention. The difference between Europe and the US is marked in this regard. To some extent there was no need for European companies to develop data collection and privacy norms as there were already mandatory legal rules about this in most of Europe, in the form of data protection legislation that has now
been harmonised by the 1995 EC Data Protection Directive. Thus the importance of codes of practice and seal schemes in Europe is more about sending a signal that parties are serious about honouring their legal commitments, and implementing the laws in a meaningful manner. In the US, where there is only minimal or sector-specific legislation, the non-binding norms take on the role of providing the basic framework of protection.

In the US a large number of seal programmes and industry initiatives have been developed to promote good privacy practice. Indeed the number of schemes, whilst good for competition, may make consumer comprehension difficult as they are faced with a variety of seals many fulfilling different purposes and making it difficult to judge their value. In the UK, seal programs have also been launched such as TrustUK, and the Which? Webtrader seal programme. It is perhaps a measure of the value placed on these seal programs both by UK business, and the trust they inspire in UK consumers that the latter is no longer funded by its seal members and is effectively defunct. The problem of assessing what seals actually guarantee increases when the browsing shopper moves outside the home jurisdiction, as of course it is easy to do on the Internet. In an attempt to promote research into and exchange information about EU seal and trust programs, the European Union launched the e-confidence forum in 2000, which has set up a website with links to several of the Internet seal programmes around Europe and worked on establishing some Principles for e-commerce codes of conduct. This work is still at an embryonic stage however and, from its website, appears to be moving slowly. In the meantime other trans-national organisations such as the OECD are picking up the slack by coming out with their own guidelines for consumer protection in the context of e-commerce, which may prove to be either a harmonising or a diversifying influence.

In addition to seal programmes there are also industry sector initiatives to promote good Internet trading practices including privacy issues. To the forefront of these initiatives are trade associations like the Direct Marketing Association. The FEDMA (Federation of European Direct Marketing Associations), for example, issued its own code on e-commerce and interactive marketing which in June 2003 was the first code to be officially approved by the EU as compliant with data protection law under Art 27 of the 1995 Directive. However, it is well known that one of the problems with industry self regulation is what to do if members do not follow their

---

37 http://www.trustuk.org.uk/.
38 http://econfidence.jrc.it/default/.
own rules. Indeed Strauss and Rogerson have noted that industry associations aimed at developing self-regulation, like the Online Privacy Alliance, contain some members who have been frequently criticised for their information practices.40

Such self-regulatory developments must face the same questions that should be posed to determine the worth of all soft law consumer regulation: how extensive is the coverage of the codes, what incentives are there for compliance, and are there any effective sanctions against delinquent traders?41 The problem of coverage is clearly a serious one. In 1999, the privacy activism group EPIC found that only 20 of the 100 most popular shopping websites were part of an industry self-regulation programme.42 In 2000, at the peak of the dot-com bubble, the leading US seal programme, TRUSTe (which was founded in 1996) had 1200 sites accredited43; in 2003, its Annual Report states that three years on it now has only ‘over 1500’ signatory websites accredited, and admits that both membership, sponsors and revenues are falling following the dot-com implosion.44 TrustUK, the only major UK seal scheme still operating, has so far only accredited two industry codes covering around 4,000 UK web-traders. Furthermore, the profile of the Internet seal programmes that do exist is not yet very high among consumers. Although seeing a logo may inspire some confidence, consumers seem to need more convincing it has actual value.45 In a global market place, like the Internet, there is a strong argument for international criteria, somewhat akin to OECD guidelines, for what guarantees seal schemes should offer consumers, and for agreements on mutual recognition of codes. Having a multiplicity of code providers, as is the US situation, also reduces their effective sanction against members (ie, withdrawal of seal), as members know they can shop around for a new seal provider if their current association acts too rigorously against their misdemeanours. Dividing up codes by industry sectors is also a rather fragile process in an electronic world where familiar trading divisions are rubbing thin, eg, supermarkets are now offering on-line banking and credit card services. Finally, as hinted above, now that the e-commerce world is no longer seen as a bottomless well of profit, many web-traders may regard the cost of supporting or signing up to a seal scheme as unjustifiable given the relative lack of consumer seal brand recognition.

40 Supra n 36.
42 EPIC and Junkbusters, 1999, Pretty Poor Privacy, supra n 64.
43 FTC, 2000, supra n 12.
45 The UK NCC report found that consumers were generally unimpressed with seal schemes: few recognised the various logos (‘I have never heard of any of these frankly. They could have been made up by anybody.’ was one typical remark.)
This brings us to the well-aired issue of how effective seal organisations are in fact prepared to be in policing and punishing their members, given that their funding is usually dependent on said members. TRUSTe especially has been stringently criticised for soft peddling on the behaviour of some of its most prominent members such as GeoCities and Microsoft.46 As Bennett and Raab put it, ‘self-regulation will always suffer from the perception that self-regulation is more symbolic than real because those who are responsible for implementation are those who have a vested interest in the processing of personal data’47.

These weaknesses with self-regulation and seal programmes do not mean that they are worthless. They may serve a valuable function in at least partially supporting a higher level of consumer trust, especially where new technology has raised new fears about what are essentially old and well established forms of trade. Credit card transactions, for example, are generally as well protected against fraud on-line as off-line; yet, as we have seen, consumers find them extremely worrying to partake in on-line. As a confidence booster and ‘hand-holder’, trust seals have a valuable function. However, in practical terms of guaranteeing consumer privacy and providing adequate remedies for its breach, the lack of coverage, lack of meaningful sanctions and dubious funding basis of self regulatory trust seal schemes, mean they should be viewed only as a supplement and not a replacement for state-backed mandatory legislation.

3.3 Law

The European system of ‘hard’ data protection (DP) laws, as opposed to ‘soft’ law or self regulation, is perhaps well enough known not to need rehearsed again in detail here.48 The European legislation is comprehensive, or omnibus, in that it refers to the collection and processing of all types of data capable of identifying a living person and does not limit itself to data collected by the state. In theory, European DP law although conceived before the Internet should be flexible enough to regulate on line privacy. The practice has however been less satisfactory, and the rise of the Internet as a marketing medium has revealed dismaying gaps in the shield to privacy of DP law. The Privacy and Electronic Communications

---


47 Bennett and Raab, supra n 11, p 154.

48 Good accounts of the differences between the US and European regimes can be found in Charlesworth, A. supra n 46; Reidenberg J. (2000) 52 Stanford Law Review 1315; and P.Swire and Litan None of Your Business (Brookings Institution Press, 1998); Bygrave L. Data Protection Law: Approaching Its Rationale, Logic and Limits (Kluwer, 2002) is an excellent recent account of EU data protection law with particular reference to its application to on-line business and personal data collection.
Directive, passed on 12 July 2002, is an attempt to grapple with two main controversies which are central to the topic of consumer privacy protection and which have proved most immune to DP remedies: cookies and spam. At one point in the debates over the 2002 Directive, it looked as if the European Parliament might require the total banning of cookies without explicit prior consent by the consumer to their being set, to the utter consternation of European industry. As ever, a compromise was reached and the final version enshrined in Art 5(3) requires merely that cookies may only be set if the consumer is supplied with clear and comprehensive information...about the purposes of the processing, and is offered the right to refuse such processing by the data controller [italics added]. This is in many ways an extremely watered down version of the original intent which was to introduce an explicit opt-in requirement in relation to cookies. Instead, the provision retains an opt-out system, albeit with added requirements of clear information. It seems that in Europe, cookies may no longer be simply invisibly set and collected. But how will this information and opt-out opportunity be supplied? Will a hyperlink to a privacy policy be sufficient? What if the privacy policy is unintelligible? In the UMIST/UK Information Commissioner study of compliance of websites with data protection law, the study team found only 5% of privacy policies were intelligible to the average consumer, using recognised plain English indices. What if (as seems anecdotally to be the case) consumers never read privacy policies anyway? What if a tick box is supplied, already ticked, which gives permission to set cookies, unobtrusively tucked away at the bottom of the page? Or a box whose rubric reads ‘Tick this box if you don’t want us to set cookies’, so putting the onus on the unsuspecting consumer? Neither of these would surely have been acceptable under a requirement of explicit prior consent, but may well be in an opt-out regime. The recitals, from a consumer point of view, provide both bad and good news here. ‘Information and the right to refuse’, runs recital 25, ‘may be offered once...also covering any further use’. So it seems that if the consumer once has a tick box offered to her on her first visit to a particular web site, and fails to notice it and take the appropriate action (assuming she even knows what it means), she need never be offered it again; and meanwhile persistent cookies can be set which will continue to gather information every time she subsequently visits that site. On the other hand the recital goes on to require that ‘the method for giving information, offering a right to refuse or requesting consent should be made as user friendly as possible’. One

49 Directive 2002/58/EC.
51 Supra, n 27.
might hope that this might rule out the scenario described above. However, leaving such important detail to the recital part of the Directive will do little for European uniformity when the Directive is implemented, a glaring problem when websites largely operate without notice of or concern for national boundaries.

Another interesting point in Art 5(3) is that setting cookies is allowed without consent where ‘strictly necessary in order to provide an information society service explicitly requested by the subscriber or user’ [italics added]. Many web sites at present, whether by intent or laziness, are designed not to work without cookies. Some will work without cookies, but not as well; the Amazon site is a good example of this, as it (unusually) provides fairly good functionality without cookies, but popular features such as the ‘shopping cart’ disappear. So depending on the interpretation of ‘strictly necessary’, this provision may well be an open invitation to bypass the requirement of consent at all – in other words, to retain the status quo. What it should do, however, is clearly distinguish between the setting of site-specific cookies (eg when Amazon sets an Amazon cookie), and the setting of third party cookies by the likes of DoubleClick. Since such ad-server cookies are invariably set invisibly, and not at the request of the consumer (for who would explicitly request ads?) it seems these cannot be covered. Hence it appears European consumers will in future have to be persuaded at least not to opt out of receiving advertisements, at least once – an interesting opportunity if consumers are savvy enough to grasp it.

The UK government has indicated in its consultation document and in the Privacy and Electronic Communications EC Directive Regulations 2003 which implement the Privacy Directive an approach which is, in this writer’s opinion, disappointingly un-privacy friendly. On the question of how consumers should be offered the right to refuse cookies, the Regulations are entirely silent, except for asserting that the right to refuse cookies need not be offered more than once. The draft guidance suggested that the requirement to offer a way of refusing cookies would in fact be met if websites merely offered guidance on how consumers might use the facilities of their browser programme (eg Internet Explorer) to reject cookies. In this writer’s view this is entirely inadequate to provide most consumers with a ‘user friendly’ way to vindicate their legal right to refuse. The position is muddied further where the consumer is using a computer

---

52 The NCC survey Consumer Privacy in the Information Age (December 1999, PD65/L/99) spoke to focus groups of consumers about privacy, and one of their strongest resulting findings was that consumers did not like the current variation in how consent is sought by tick boxes, and felt opt-in was much more in the best interests of consumers than opt-out. The report attaches a model standardised tick box format.

53 Of course most consumers ads are served to US web sites from US ad servers and hence at least in practical terms outside EC jurisdiction. See below.

while at work; here it seemed the person with the right to refuse cookies might well be the employer, not the employee/consumer. Following consultation, rule 6 now provides that either the ‘subscriber or user’ must be given the right to refuse. On the question of what is ‘strictly necessary’ in response to a request by the consumer, the Regulations again say nothing, although the guidance notes did specify that the regulations would apply to all cookies, specifically including session specific cookies, but presumably including third party cookies.

On spam, the most significant change brought in by the Privacy Directive is, finally, following years of incremental struggle, the requirement of opt-in to receiving electronic junk mail or spam.55 Importantly the definition of ‘electronic mail’ in rule 2 is wide enough to cover not just email but also text, voice, sound and image messages sent over a public communication network and which can be stored until collected. The increasingly ubiquitous mobile phone txt spam is thus also subject to opt-in requirement. Again however, the banning of unsolicited spam is subject to a potentially damagingly wide exception. Prior consent according to the draft regulations, was not required if the details of the recipient were previously obtained ‘in the context of a sale of a product or service’ so long as (a) the recipient was given a clear, simple and free opportunity to opt-out of receiving spam each time a new communication is sent, and (b) the goods or services were ‘similar’ to those now being marketed. Privacy advocates might suggest that the correct way to interpret this provision is to regard the exception as only operating where an actual prior sale had occurred – i.e, not where the consumer had merely browsed the site to check out goods, decided not to buy, but perhaps inadvertently given away their details, eg, by registering to gain access to the website at all. The UK Regulations however again take a different approach. So long as the business has ‘legitimately’ obtained the contact details, no actual sale should be required. Details may be obtained ‘in the course of sale or negotiations for the sale’ (r. 22(3)(a) 2003 Regs). Furthermore, ‘similar’ goods or services, according to the DTI, should only be restricted by the reasonable expectations of the buyer at the time they gave their contact details. In other words, if a consumer buys baked beans on-line from Tesco’s, it is reasonable for Tesco’s to then market TVs and DVDs (say) to that consumer without prior consent, because the consumer could reasonably have known that Tescos sold all these types of goods at the time she first gave away her personal information; however if Tesco’s, subsequent to the baked bean purchase, acquired, say, a horse-riding stables business, it would not be reasonable for them to market horse-riding lessons to the

CONSUMER PRIVACY, ON-LINE BUSINESS AND THE INTERNET

consumer. Again, this seems a technical and privacy-minimising interpretation which is unlikely to be harmonious with several other member states which have already banned spam entirely and long ago – nor is it likely to instil the trust in consumers which is the whole object of the exercise.

Turning to the US, attitudes to regulation of privacy in the commercial sphere are notoriously very different than in Europe. Commercial invasion of privacy has largely been dealt with by piecemeal sector specific legislation, often passed in reaction against particular abuses: a good example being the Children’s Online Privacy Protection Act 1988 which limited the ability of websites to collect information from persons under thirteen. The slack is taken up – or is supposed to be taken up – by market norms, self-regulation and consumer pressure. In recent years, however, public concern has grown about the impact the Internet is having on personal privacy, spurred on by the campaigning of ‘electronic civil liberty’ pressure groups such as EPIC and Junkbusters, and frequent scandals relating to popular software products and sites such as Hotmail and Yahoo! The main state response has come from the Federal Trade Commission, which has made it a major part of its consumer protection remit to look into on-line data privacy abuses, and which, as we have already seen above, has on occasion been far more effective in curbing abuses than such industry bodies as TrustE. Significantly, in May 2000, after ten years of combating Internet industry data scandals, the FTC took the about-turn decision to move from its longstanding pro-self regulatory stance to a position supportive of enacting Federal privacy legislation, admittedly in conjunction with self regulatory programmes. Since then it has sought an increasingly active role as an ‘Internet cop’, particularly of late in relation to identity theft and spamming fraud.

But even if the US is pushed towards a more hands-on approach to privacy laws at least in the Internet medium, it is unlikely to ever accord to what are seen as the norms in Europe. This of course produces major difficulties in dealing with cyberspace. The Internet, tritely, is a global medium and the hub of the Internet industry is undoubtedly the US. What is the use of having effective DP laws in Europe if information is transferred to, or collected on the Internet by, US based companies? What is the use of the European Parliament regulating spam and cookies when most spam is sent from outside Europe and most cookies are set by US based websites? Even if jurisdictional rules attempt to deal with these problems,56 where are the resources and the political will to effectively enforce European rules outside Europe? There are the barest glimmers of a degree of real international co-operation in relation to spam emerging57 but even this is

likely to founder on the political difficulties of restricting US industry selling to US consumers to European privacy standards. This was the issue at the heart of the recent long running struggle over the EU/US ‘safe harbor’: which example does not give rise to great hopes that a global consensus on data protection law regimes will arrive anytime soon. Yet without a global solution, law is effectively helpless to provide realistic protection of consumer data as gathered and shared on trans-national websites.

The other major problem with law as a regulatory mechanism, as with ‘soft’ law already discussed, is compliance. The task of policing data collection on the web, is to say the least, not for the faint hearted. The search engine Google alone currently searches over 3,000 million web pages58 and this is of course known to be only a small percentage of the entire Web. Yet in general the resources so far devoted to web compliance with DP laws are puny.59 The UK Information Commissioner’s Office, for example, employs only a few hundred staff of whom not all are concerned with website compliance. The 2002 Annual Report reveals that although staff numbers increased by 40% during the year, requests for help also increased by a third. The new Information Commissioner, Richard Thomas, has announced, partly as a result of the dismal state revealed by the Study of Website Compliance that Internet compliance with DP standards will be one of the priorities of his term in office – yet there has been no significant increase in staffing substantial enough to even begin to meet this aim.50 Furthermore on line consumer privacy is a peculiarly difficult area for law to police, even looking beyond the sheer size of the Web. Consumers regularly report that they do not know what legal rights, if any, they have in cyberspace and suspect they have less rights in cyberspace than the ‘real’ world (usually erroneously). Thus they obviously have little reason to be concerned to know where or how to direct complaints. Only 42% of UK citizens even know they have data protection rights; a figure which itself has risen since 2002 from 27%.61 This is unfortunate, as given the resources allocated to website compliance, one can only imagine that

---

58 Noted at 23 July 2003.
60 Interestingly however, regional Information Commissioners have just been installed in Scotland, Wales and Northern Ireland as of April 2003.
61 Annual Report of the Information Commissioner, 2002. This actually compares well to the pan-European finding of the First European Commission Report on Implementation of the DP Directive, supra n. 50, which found that of its 10,000 respondents to consultation, 81% thought awareness of DP rights was insufficient, bad or very bad. The Report also indicted patchy compliance with DP law throughout Europe as based on the inter-locking problems of under-resourcing, lack of compliance by data controllers and low knowledge of rights among data subjects.
activity must be mainly complaint driven. On this gloomy note, we turn to
look at Lessig’s final mode of regulation: technology, or ‘code as code’.

3.4 Technology

If data collection on the Internet is enabled by software, then software
seems the obvious way to fight back. There are many products available
which can help consumers to stop their personal information being
collected in the first place. It is not hard or particularly expensive to
‘disappear’ entirely. 62 If you want to protect your e-mail address or URL,
then anonymous remailers can be used, which strip out the header
information from emails and so prevent the consumer’s ISP and IP address
being traced. Many of these are set up by privacy activists and provide
services for free. Proxy servers, which act as an intermediary for web traffic
between you and the website you want to visit, perform a similar function of
anonymisation in relation to web transactions and browsing. The truly
paranoid may want to use a string of remailers or equivalent, or better still,
an all-in product such as ZeroKnowledge 63 provides called Freedom. Such
products act effectively as ‘privacy firewalls’. The user can surf, transact and
send email without accepting cookies or having personal or traffic data
recorded except as they actually desire so to do. For the consumer who
does not wish to go all the way and buy a serious privacy product such as
Freedom there are still very cheap or free ways to avoid disclosing data. It is
easy to avoid accepting cookies, for example. All browsers have an option to
reject cookies. More sophisticated pieces of software which classify and
allow the consumer to manipulate and reject cookies selectively (‘cookie
killers’) can also be freely downloaded from the Net, such as Cookie
Cutter, CookieMaster and CookieCruncher, etc. These are usually avail-
able as freeware, but the downside of this is that they may not be easy for the
average Internet consumer to use. Indeed it is likely the average Internet
consumer still does not even know what cookies are, let alone how to find
the way to reject them in their browser preferences, or how to set up Cookie
Cutter. There is also the problem that turning off cookies still causes many
sites to turn away the user.

The alleged great white hope of technology providing better consumer
privacy protection, is P3P, or the Platform for Privacy Preferences. The first
release of P3P as a fully developed product, ready to be incorporated into
browsers and other software, was announced in April 2002. 64 It is integrated
into later versions of the world’s most popular Web browser, Internet
Explorer. It is important to note what P3P is not. It is not a ‘privacy firewall’
of any kind – it does not block cookies or anonymise transactions or hide
user data. It is not a law or a norm: it does not require a site to meet any

62 See for a comprehensive account of such practices, T. Greene ‘Do-it-yourself Internet anonymity’, 14
November 2001, at http://theregister.co.uk/content/6/22831.html
63 See http://www.zeroknowledge.com/
64 See http://www.w3.org/TR/P3P/
particular level of privacy, as the OECD privacy guidelines might for example. It is simply a standard or specification developed by the international research consortium the World Wide Web Consortium. What P3P does is to read the privacy policy a site already has (or may adopt), translated into a standardised machine-readable form, and to allow the consumer to use the version of P3P built into her browser to choose if sites measure up to her pre-determined privacy standards (determined via a multiple choice interface). The idea is that this protocol will allow users to take informed decisions about their web experiences and control the use of their personal information.

Some are convinced by this. Larry Lessig for example endorses P3P as the best way forward, at least at a theoretical level. His view is that given we live in a world where data is already a commodity, the best approach to protection is to grant control to those whom the data is about. Contrasting the European approach to DP as a subject for law, with technological protection by P3P, he prefers the P3P approach which gives the user effectively a property right in their personal information, which they can sell or choose not to sell. His view is that data protection laws merely create liability for the misuse of data, after the fact. ‘There is individual control or autonomy within a property regime, but not with a liability regime. Property protects choice; liability protects transfer.’ Thus he supports P3P, with the proviso that the law must grant individuals a property right in their data. (‘Laissez faire will not cut it.’)

Yet this solution is disingenuous. P3P supports bargaining about privacy, yes, but nothing more. It does not provide any enforcement or compliance mechanism of any kind. Any support for the disgruntled consumer must come from law (or perhaps seal schemes), exactly as in Europe. All the property right will allow the law to do is provide damages after the fact. Furthermore P3P does nothing to create a minimum privacy standard in the marketplace. It fails to set a bar below which sites cannot fall. If a site offers no privacy guarantees of any kind, and a consumer using P3P surfs the web with it at minimum level, then effectively she is saying to the world that she is prepared to give up any privacy protection of any kind, perhaps for consideration, perhaps for free. Whether this is seen as a problem is a basic problem of paternalism/socialist concern versus laissez faire capitalism. A free market advocate will argue that if a consumer wants to sell or give her privacy rights and personal data away then she is entitled to, even if it is ultimately likely to be harmful to her. But this fails wholly to

---


66 See Code and Other Laws of Cyberspace. Chapter 11. He stresses he is not endorsing the particular technical details of P3P but is supporting the idea of a free-choice system which supports consumers in making bargains about selling or giving away their personal information.

take into account the ignorance (and consonant lack of power) of the average consumer, not only as to the actual worth of her data (already commented on), not only as to the potential harms (also already commented on), but also as to how to alter the default settings on the version of P3P incorporated into her browser – how to use the technology to accurately represent her own wishes. It also fails to consider if allowing privacy to become another commodity which an uninformed consumer is free to give away on the open market is consonant with the ‘human dignity’ conception of privacy, or, to put it another way, if privacy should be an inalienable human right not an item of property.

P3P will also only work in a marketplace of different privacy policies for the consumer to choose between. It is fundamentally just an automated way of letting consumers choose between privacy policies. Without such a marketplace, any sense of choice or control it provides is illusory. Yet as we have seen above there is little evidence that such a market place is developing. P3P is in fact actively unhelpful because to the average consumer, it sounds like, but is not, what they want – a ‘privacy firewall’. Just as consumers have got used to the idea that email filters can keep out spam, and security firewalls keep out viruses and hackers, they are likely to think, if they grasp the idea of P3P at all, that it is a filter that keeps out cookies, or third party advertisers, or prying eyes. When they are disillusioned this will do nothing to help the already dismal level of consumer trust in the e-commerce marketplace.

For all these reasons the conclusions the European Commission came to when it examined P3P in 1998 still stand:

A technical platform for privacy protection will not in itself be sufficient to protect privacy on the web. It must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. Use of P3P in the absence of such a framework risks shifting the onus primarily onto the individual user to protect himself, a development which would undermine the internationally established principle that it is the ‘data controller’ who is responsible for complying with data protection principles.

This EC position has remained substantially unchanged since, despite technical developments in the P3P architecture. The latest review of implementation of the DP Directive, published in May 2003, formally embraces the use of technology to assist in the protection of privacy but is very careful to assert that the need is for products which are not only

--

69 See Privacy on the Internet, supra n 18, Chapter 9, Conclusions.
70 Supra, n 59.

246
privacy-compliant and privacy-friendly, but also privacy-enhancing and that products which are not transparent about what they do may in fact lose rather than engender the trust of users. The EC is quite clear that technologies such as P3P are, like trust seals, inadequate to protect privacy without a strong legal framework of legal DP rights to enable sanctions for non-compliance. They are also ineffective without considerable consumer education as to how they work and what their limits are. It is tempting to say, as EPIC do, that the efforts that have been put into P3P are at best misplaced, and at worst a diversion by the e-commerce marketplace from publicising and developing other forms of code freely available on the net which might better aid consumers; the ‘cookie killers’, proxy servers, anonymising software and other types of privacy enhancing technologies (PETs). Indeed in the European Commission report on consumer protection which preceded the new Privacy Directive, the overall conclusions do seem to echo these sentiments, in that they seem to regard P3P as at best only part of the solution and possibly even part of the problem. They suggest that (a) privacy compliant browsers should be produced with the most privacy-friendly default settings; (b) proxy servers could be offered as a free standard feature by every ISP; (c) websites should not deny access to users who do not want cookies set; and (d) individuals should be given more information about the existence and use of PETs. Only the third of these is however mandated (and that as we have seen, with caveats) in the Privacy Directive of 2002.

4 Conclusions

It is commonly said in electronic freedom circles in relation to the Internet pornography debate, that there is no reason why citizens should have less freedom of expression on-line than off-line. The axiomatic starting point for this writer was, similarly, that there was no reason why consumers should be forced to compromise their privacy when buying over the Internet, any further than they do when buying in the ‘real world’. Yet the reality of the debate turns out to be more complex than that. In some ways the consumer’s privacy is inevitably far more threatened on-line than it is when shopping on the high street due to the need to disclose the real world identity and location of the consumer in order to supply her with (non virtual) goods and services, and because of electronic footprints left by technologies such as cookies, the Web protocols and TCP/IP. Yet on the other hand, the Internet also offers the possibility in some cases to

---

72 This approach has been strongly backed by the UK Cyber Rights and Cyber Liberties campaigning organisation.
consumers to achieve near-perfect anonymity via technology, something which is simply never possible in the ‘real world’ environment. The obvious question to ask is, if law, norms and the market are inefficient at protecting privacy, why do all consumers not simply adopt technologies such as CookyCutter or P3P which appear to offer them the control they say in survey after survey they desire? Perhaps simply because of lack of knowledge of the technologies concerned. But even if that can be overcome, the next question is, should they be encouraged to adopt such strategies – or to rely instead, or as well, on their legal rights?

P3P, as noted above, is merely an automated bargaining mechanism. Currently customers cannot bargain efficiently with their personal data because few if any have any idea of its potential worth. Consumers are too easily lured into either giving away their data for nothing or, at best, by enticements which understate the value to the company of their data. They are also aware only of the information they give away themselves, and not of the aggregate value of their data combined with that of many other data subjects and possibly with other databases. In these circumstances, any consent given by consumers cannot be regarded as informed. In making choices about data disclosure it is also vital that consumers believe that their choices about their personal information will be respected and enforced post disclosure. Otherwise they will not take the issue seriously nor will their reasonable expectations of fair processing of data once collected be met. This is why the various techniques for regulation discussed above other than technology – law, norms and market forces – are important even if on the face of it not as efficient or as self-enforcing as technological means of privacy protection, such as P3P and PETs. There is no point in a consumer making the balanced decision to provide personal information to Expedia for the incentive of extra air miles, on the grounds Expedia will use the information but not share it, if Expedia then goes and gives that data to another organisation like (say) lastminute.com anyway.73 This point remains fundamentally the same whether the consumer decides by looking at privacy policies or other information (such as the detailed tick box the NCC has suggested74), or whether that choice is supported by automation as in a P3P architecture.

In order to encourage consumers to take their privacy choices seriously, it is important to remove from the range of outcomes they must have in mind instances where consumers cannot really benefit from sharing their data and losing privacy. Spamming is one clear example of a practice which benefits neither consumers nor legitimate commerce. It would give consumer’s confidence when considering what data they will release to know that whatever happens, they will not be inundated with spam. This of

73 The author hastens to add that this is a hypothetical example.
74 Supra, n 6.
course is an enormous problem only one part of which can be met by more stringent control of the sharing of personal data. However one useful starting point in Europe would be for the EC Privacy Directive to be implemented in the strongest possible form, so as to enforce the requirement of opt-in to unsolicited direct marketing as a matter of minimum harmonisation. Still more importantly, the attempts that are now being made to reach some kind of international, not just European, consensus on how to deal with spam must be continued and intensified. The DP Directive is due for wholesale review in 2005. Although light-years away in Internet years, this would be a good target for any process aimed at securing a genuine global law on spam and assent to mutual co-operation in at least this one limited area.

Cynically however, one might finally ask if consumers are simply getting the data privacy they deserve. Convenience today when surfing on-line seems a far more immediate prospect than the dim, un-quantified risks to privacy that might lurk tomorrow; and the effort of working out the pros and cons of data disclosure is perhaps simply one consumers do not want to make, especially on the Internet, where the typical purchase is low cost, low risk and rapid. As one respondent to the NCC Consumer Privacy report puts it, ‘You haven’t heard anything on the news that happened to anyone because somebody has got their personal data’. Although said in 1999, this comment still rings true today in the UK (although the idea of ‘identity theft’ as a serious crime has in fact begun to grab the occasional headline). Perhaps this fatalistic attitude explains the remarks of Esther Dyson, one of the major players of the IT industry and one of the original supporters of the TrustE initiative, which were quoted at the start of this article. Dyson recently gave an interview in which she admitted her disappointment that TrustE had slipped from consumer advocate to corporate apologist. But ‘I’ve also been disappointed in consumers’ she added, ‘in that they’ve not been proactive in protecting their own data. You do a survey and consumers say they are very concerned about their privacy. Then you offer them a discount on a book and they’ll tell you everything.’

The question is whether we are prepared to leave privacy to the efforts of individuals who are bloody minded or technologically literate enough to assert and enforce their own rights to privacy on-line; or whether the law (and to some extent, soft law) should still try to grapple with this problem. In the first scenario, a few informed, motivated and computer literate persons may be willing and able to expend the energy needed to protect their privacy preferences. However, most consumers are unlikely to fit into this category. Most Internet users rather have what they regard as a reasonable expectation of a certain degree of privacy which they should
enjoy undisturbed without having to expend ingenuity or effort in protecting it. They wish also not to sacrifice the advantages of some data disclosure on the Internet such as speedy, cheap, personalised and convenient access to goods and services by the more extreme approaches such as never accepting cookies. This is why the argument here is not for the banning of data collection online, which would in any case be political and commercially unworkable, nor for accepting that the onus is on individuals to protect their own privacy via P3P, the rejection of cookies, et al. Instead, the effective enforcement of certain basic privacy standards needs to be enshrined in legal regulation in the US and elsewhere, as well as enforced in Europe, and not simply left to market forces. Many European jurists would argue that such a framework already exists in the shape of DP law; but while it is not universally adopted, not well harmonised (another major criticism made in the 2003 EU Commission report on implementation), has significant gaps in protection, and above all, is unenforceable on-line without huge input of resources, it cannot be regarded as adequate. The quest for scholars and policy makers then is to look for what new legal solutions may replace, or more likely, bolster DP law on the Internet. 77 Such legal regulation should ideally not limit the effectiveness of on-line web-trading, nor interfere with the growing tendency of businesses to operate globally and in conglomerates. But it must allow consumers to gain confidence in the global Internet as a safe place to shop, learn, play and work.

77 A preliminary attempt to look beyond DP law to new forms of legal solutions can be found in Edwards L. ‘The Problem With Privacy: A Modest Proposal’ (2003) 3 Privacy & Data Protection 6. See also the suggestions for reform of DP law made by Bygrave L., supra n 48, who draws particular attention to the need to regulate data ‘profiling’ and to extend DP law to protect juristic as well as living persons; and the conclusions of Bennett and Raab, supra n. 12, who argue that while globalisation is leading to the general ‘trading up’ of states to a minimum level of privacy protection, there is also one or multiple balancing ‘races to the bottom’ in terms of state and commercial surveillance.
Web Services and the Law: A Sketch of the Potential Issues

ASSAFA ENDESHAW

Abstract

The function of the World Wide Web (the ‘Web’) has passed through stages. The first stage, often known as ‘web publishing’, represented the provision of static information. The second stage, ‘Web application’, was the provision of computing applications on the Web. The latest stage, ‘Web Services’, promises to integrate business applications via the Internet regardless of differences in platforms.

The promises of Web Services have yet to materialise. Operational and security issues still dog its adoption by individuals, businesses and other organisations. This paper confines itself to an examination of the possible range of new and old legal issues that Web Services might throw up. It concentrates on ‘network contracts’ (among multiparty partners) for the supply of goods (as well as information) and services, end-to-end security, data and privacy protection, intellectual property and dispute resolution.

The paper argues that, whilst Web Services extend current capabilities towards the ubiquitous network, they nevertheless do not prompt a radical departure from the currently evolving legal framework. The likely impacts of Web Services on the law in general and the attendant risks and responsibilities of all participants in particular will appear to be linked with the breadth of their reach. Yet, one cannot say exactly how the legal response will shape out finally. It may be hazarded that the nature of

1 Assafa Endeshaw PhD, Associate Professor of Law, Nanyang Business School, Singapore 639798 Email: Aendeshawntu.edu.sg
contracts and jurisdictional issues will be the most extensively impacted, consequently too dispute resolution.

1 Introduction

Until recently, it had seemed that the broad frameworks for electronic commerce (e-commerce) and the corresponding legal infrastructure had become settled. The general understanding was that application systems would continue to evolve together with the entry of new devices as additional media for e-commerce. After all, e-commerce has transited from a stage, in the 1970s, when certain transactions began to use computer media to the current period (form 1994 onwards) of full-fledged trading in goods, services and information.

The earliest form of e-commerce (in the 1970s) was Electronic Funds Transfer (EFT) that facilitated movements of money between financial institutions. In the 1980s, Automatic Teller Machines (ATMs) enabled individual bank customers to conduct withdrawals and other retail banking activities through a computer network. At the same time, Electronic Data Interchange (EDI) began to take hold among business entities that sought to exchange transactional documents such as contracts, purchase orders and bills, again via computer networks.

Then emerged the Internet with its original purpose of facilitating exchange and sharing of research data and computing power among different people at varied places. The Internet has since evolved into a means of business operations. The mode of communication between the connected computers and networks was established by a protocol known as the 'Transmission Control Protocol/Internet Protocol (TCP/IP)’. This allows messages between networks regardless of the differences in operating systems that they use. The addressing system also enables exchanges from virtually anywhere so long as the network or computer is connected to the Internet.

Until the early 1990s, the Internet was only useful for exchanging text. The possibility of exchanging graphics and other forms of content was made possible after the protocol known as the ‘World Wide Web’ (WWW) was invented. As an interconnection of networks of computers equipped with previously agreed sets of rules or standards (‘protocols’) for communications and transfer or exchange of information among those networks, the Web-enabled Internet has already created a space for interactions of all forms that parallel terrestrial transactions and social and political activities. The potential of the Web to turn the Internet into a

---

2 The major ones are the HyperText Transport Protocol (HTTP), the Uniform resource Locator (URL) and the HyperText Markup Language (HTML).
medium with all forms of relationships replicating real life situations has lately taken the shape of ‘Web Services’.

*Businessweek* has described Web Services simply as ‘the next big phase of the Internet . . . when the Web’s infrastructure becomes so advanced that people no longer have to find their way through a maze of software applications and Web sites to get things done. Instead, computers stuffed with different kinds of information, run by different companies and hooked to different Web sites, can chatter between themselves behind the scenes to accomplish tasks.’

A great deal of promise (or hype?) accompanies any mention of Web Services, particularly by those engaged in its development and use. Web Services are regarded as the ‘silver bullet’ that will solve the problem of integration of business applications through cross-platform interoperability. Web Services are supposed to be able to provide universal access for global trading as well as the application of content and management solutions in heterogeneous environments. Furthermore, Web Services will arguably simplify business to business (B2B) transactions, drive down costs and facilitate collaborative relations. The argument is that, by bringing online businesses closer to consumers, those businesses will generate the huge demand that has been eluding them to date.

A few studies have been conducted to test the above claims. A 2001 study by InfoWorld surveyed 500 people involved in determining technology strategy and technology-buying decision makers: 85% expressed familiarity with Web Services; 74% ranked them as moderate, high, or critical priority in next two years; 66% indicated they would be developing a strategy within the next year; 30% disclosed that they were already realising benefits from Web Services within their company or expect to do so within the next quarter.

A Borland Software Corporation 2002 survey found that ‘80 percent of respondents are either currently using Web Services or are planning to use them in the very near future.’ A similar study found that ‘98% of IT

---

5 See for instance, Daryl Plummer and Whit Andrews, ‘The hype is right: Web services will deliver immediate benefits’, October 9, 2001. (A report of a Gartner research presented at Gartner Symposium ITxpo 2001.) Available at http://www.gartner.com/resources/101500/101571/101571.html; accessed on November 4, 2002. The authors predict: ‘The financial-services industry will be among the first to adopt Web services, due to this industry’s ready-made network of authentication and reputation systems. Other early-adopter industries will include transportation, energy, high-tech and small businesses that have little or no investment in installed software.’
managers will be developing web services-enabled applications within two years, while 75% are already incorporating some level of web services functionality into applications today.\[9\] The same study reportedly found ‘internal enterprise applications is the most prevalent area of deployment.’\[10\] On the other hand, it cited security and authentication as being ‘one of the biggest concerns surrounding the web services model’.\[11\]

Still another survey projected the adoption of Web services to jump to 87 percent next year at the same time pointing to ‘security, ambiguity in Web services standards’ and other technical issues as obstacles for deploying Web services.\[12\] A further survey commissioned by BEA Systems showed 54 percent of European companies to have adopted Web services, though 48 per cent cite security concerns as preventing their implementation.\[13\]

Earlier misconceptions about the potentials and capabilities of Web Services have come under scrutiny. It has thus been contended,\[14\] despite the claims, that Web services will not be able to foster indiscriminate and anonymous business partner selection over the Internet; Internet businesses will need to negotiate partner agreements themselves. On the positive side, Web Services help existing partners to work better together by enabling them to integrate their systems more easily. On another level, Web Services will not eliminate the need for application integration because integration remains a key challenge for almost every enterprise. Newcomer notes ‘Web [S]ervices are not executable things in and of themselves; they rely on executable programs written using programming languages and scripts.’\[15\] Nor will they eliminate the need for decision makers.\[16\] Just like any other technology, they create new opportunities for business to transform themselves. Finally, commentators warned: “The idea that Web services will foster a revolution in self-aware software that makes all decisions without human intervention is mostly a pipe dream.”\[17\]

Whilst the touted promises of Web Services might remain unfulfilled and it might yet take a few more years before Web Services become a dominant feature of business transactions on the Internet, their legal
implications have still to be worked out. For one thing, the law is a reactive discipline.18 Secondly, the full picture of the workings of Web Services has yet to emerge – not to mention that other technologies might evolve and transform Web applications.19 This paper therefore limits itself to an examination of the potential problems that Web Services might throw up for the law to grapple with.

Section 1 of the paper sets the stage by defining the nature of Web Services and the functional changes they promise. Sections 2 to 6 take up specific areas of law that might face challenges. Section 2 explores contractual agreements (among multiparty partners) on supply of goods (as well as information) and services. Section 3 examines the potential increase in exposure of businesses to liability for development or protection of content. Section 4 addresses the paramount problem of end-to-end security for Web Services and issues of data and privacy protection. Section 5 looks at the increased potential difficulties for protection of intellectual property. Section 6 peruses the likely impact of the implementation of Web Services on forms of online dispute resolution. The conclusion underlines that the potential impacts of Web Services on the law are linked to the breadth of the emerging ubiquitous network, the diversity and complexity in the nature of transactions as well as the multitudinous number of participants.

2 The Nature of Web Services

Web Services represent a major change in the architecture of computing. In the early stage of computing, the process, data and user interface for a software application were all kept in the mainframe computer.20 Thus computing during that period was centralised and users shared the facilities. Later, the interface began to appear on the client/user’s desktop

---

18 The author has made a summary of the relationship between law and technology in Internet and E-Commerce Law: with a focus on Asia-Pacific, Prentice Hall, Pearson Education Asia, 2001, Chapter 1, pp. 3–39.

19 One example is the developing work on the ‘Semantic Web’ – ‘a smart network that will finally understand human languages and make computers virtually as easy to work with as other humans.’ See, Otis Port, ‘Special Report: The Next Web’, Businessweek 95, March 4, 2002, at 95. The expected outcome is a technology that ‘would understand not only the meaning of words and concepts but also the logical relationships among them.’ Ibid., at 96. This will enable summarising, translating and ordering of existing knowledge as well as analytical work to be handled by computers and shifting the relevant tasks from people to machines. Ibid.

20 To all intents and purposes, there are three principal components in computing; an interface which the user employs and manipulates to get to the application (software) she needs to run; data (raw facts and files as well as databases); and a process whereby the application turns the data into information. See James Branchecau and Shi Nansi, Essential technologies for e-commerce: developing professional Web applications, Singapore: Prentice Hall, 2001, at 5.
computer. Accordingly, the client software, often running on a personal computer (PC), would send a request (through a standardised communication protocol) to the server software (a high-performance computer). Thus emerged client/server computing comprising of a network of computers where most of the data, interface and process were handled by a main frame (the server) while limited number of applications ran on the client (desktop PC or laptop). Gradually, some applications began to run on clients and more and more of the service capabilities were extended to PCs. Mainframes could become depositories for data (databases) and some applications while clients accommodate processing and some data too.21 The trend has been towards moving more software applications and data to the client computer.

The Internet was built on the client/server architecture and, because of the open (non-proprietary) standards it adopted,22 it has spawned linkages between diverse computers across the world, running different operating systems and applications. The Internet has been transformed since the introduction of the World Wide Web (the Web) and the open standards set by the WWW Consortium (W3C).

The function of the Web has again passed through stages or generations. The first stage, often known as ‘web publishing’, represented the provision of static information such as contact numbers, addresses and description of businesses as well as the goods or services they offer to their customers. Such content was generated with the help of the HyperText Markup Language (HTML) and uploaded on the Web to be accessible to surfers. The HTML regulates how documents look when displayed on the Web; it also enables graphics and linkages with other documents. The supply of static information on the Web effectively turned the Web into online Yellow Pages for listing a business or individual under some category.23 The first-generation approach did not prove effective. According to Gianforte, ‘this approach drives customers off your Web site and back to less efficient and more expensive media such as the telephone.’24 This called for further development in the function of the Web.

The second stage, ‘Web application’, was the provision or distribution of computing applications on the Web. Web application development consists of both system design and programming skills. As soon as a

---

21 Ibid., at 4–6.
22 The Internet open standards set by the Internet Engineering Task Force (IETF) control core transport protocols TCP/IP, SMTP (Simple Mail Transport Protocol for ASCII email), MIME (Multipurpose Internet Messaging Email), SSL (Secure Sockets Layer for Web security). The technical aspects of operations are managed by the Internet Architecture Board comprising of the IETF and the Internet Research Task Force and the W3C developing protocols for common use.
23 Brancheau and Nanni, note 20, above, said, at 3.
business determines its requirements for solutions to specific tasks (such as order handling), an application is built by employees with the appropriate skills and installed on the client/server for the use of operation employees. If the business intends to make the application available to customers it must provide them a Web front-end. Should the business decide to create a front-end for its partners, it can do the same.

Each face of the application system (residing on the application server) needs connections, and must communicate, with the integration server. The persons at the different front-ends prompt additional functional requirements: personalisation (identification), management of content, security, workflow and possibility of wire-less communication capability. The resulting complexity demands standards for universal integration.

Yet, the quest for interoperability (making computers exchange information with one another) and integration (providing human interface across computers) remained a major challenge. One the one hand, the closed or legacy systems in place (developed by proprietary hardware and software interests) may be platform or software dependent and lock end-users to specific products or services. The standards or protocols produced by such proprietary interests and deployed on the Internet may not necessarily interoperate either. Secondly, security and reliability issues deter systems operators from opening up to other organisations.

Before the advent of Web Services, both consumers and businesses would have to access the ‘application services’ on the business’s server and transact accordingly. It was therefore inevitable that ‘Web Services’ were earlier used interchangeably with ‘application services’. That was because the services that were made available from a business’s Web server relied on programs placed on that server, regardless of the medium of communication used by outsiders to access those programs. Moreover, the access could only be done by those in possession of compatible programs.

‘Web Services’ are expected to eliminate the necessity of having compatible programs between business to business (B2B) and business to consumer (B2C) transaction parties. Web Services operate as a means of integrating applications via the Internet regardless of the computing platforms and programming languages of the respective businesses. Web

---

25 Branchseau and Nansi, note 20, above, ibid., at 6.
Services therefore usher in the era of ‘federated commerce’.26 Web Services can also be referred to as pay-per-view application consumption.27 Users just look through a directory for details of a business, dial up the interface and plug the service into their web page or application.

The use of the same designation for two different stages in the evolution of Web applications creates an unfortunate confusion.28 One would therefore exercise caution in using ‘Web Services’ as it has not yet gained a distinct recognition among broader sections of the industry. In this paper, the term ‘Web Services’ refer consistently to the third stage of Web development.

The concept behind the operation of Web Services is relatively straightforward. Providers of Web Services register with a directory or repository, supply a description of themselves and the services as well as the links for interfacing with each. There are thus three main components of a Web Services platform: ‘Discovery’—how availability of services can become known and discovered; ‘Description’—how information getting into and out of a service can be specified; and ‘Transport’—method of communication between a user and the service.

The discovery is accomplished through the Universal Description, Discovery and Integration (UDDI) protocol. The UDDI serves as a registry of companies (the Internet equivalent of the Yellow Pages), detailing their products and addresses as well as other particulars in three parts. The ’white pages’ pertain to the general information about a business and its contact details. The ’yellow pages’ provide classified listings of businesses according to industrial standards and custom. The ’green pages’ show technical details of a business’s Web Services and the interface to access them.29

The interface is described in Web Services Description Language (WSDL). WSDL describes message contents and defines where the service...
is available and what communication protocol is used to talk to the service. The transport or communication is managed using the Simple Object Access Protocol (SOAP). SOAP allows companies to communicate with outside applications regardless of differences in platforms or programs.

The language for defining all these is the eExtensible Markup Language (XML). The XML is ‘a set of rules, guidelines or conventions for designing common information formats such that it produces files that are easy for a computer to generate and read via the Internet, intranets and extranets.’ The essential function of the XML is to facilitate ‘loosely coupled components to interact across organisations, server platforms and programming languages.’ XML therefore goes beyond ‘defining and maintaining static content’ (as HTML does) and enables defining ‘the elements that associate meaning with the data’ such that content is ‘generated and digested dynamically.’

To summarise, Web Services promise to allow the use of any application regardless of any company’s platform and provide integration capabilities for all applications. Some, however, see Web Services as no more than a ‘useful and somewhat evolutionary trend, which is a natural development of the long-running trend toward service-oriented architectures.’ Currently, companies such as Microsoft, Sun Microsystems and IBM are developing technologies (respectively called .Net, Sun ONE and Web services) to harness the potentials of Web Services for business and individual applications.

3 Web Services and Contract Law

Contracts remain the bedrock of what and how parties may enforce their online expectations or claims from each other. The mechanisms for concluding contracts on the Internet are also becoming more and more familiar to all. Given the technological advances in ensuring identification and authentication of parties and reliability of electronic documents, contractual agreements between two parties on the Internet may be considered straightforward. Still, the nature of online contracts, as well as

---

30 An extended discussion is available at http://www.w3.org/TR/wsdl.html.
33 Ibid., at 49.
34 Newcomer, note 4, ibid., at 21.
the contents (or terms) that the respective parties agree upon, continue to be critical aspects requiring scrutiny.

3.1 ‘Network Contracts’

Inter-organisation transactions via the Internet are complex, whether or not the organizations have established ongoing relations or find their partners as and when necessary. It can be conjectured that where various parties hailing from diverse networks interlink behind the façade of one party to supply the goods or services desired by another party, the resulting relationships can be extremely complicated.

Web Services will further deepen and extend the inherently interlocking nature of online services and transactions. Activities that may generally be considered self-contained in the realspace environment will converge or merge to generate a seamless flow of goods, information and data. The treatment of different layers of the Internet as one ‘Superhighway’ criss-crossing the globe will therefore become a concrete reality with the spread of Web Services.

The consequence is that, unless one slices up the layers of the Internet in terms of their functions and characterises the legal impacts depending on the restricted functions alone, any mishap at any level may have repercussions on levels higher than where it occurs. The interdependent nature of the functions will imply that defects or shortfalls at the foundations (the backbone and other infrastructures) can have a direct bearing on all activities throughout the Internet. The same consequence can be expected for the varying levels above them. It is therefore apposite to consider the complex relationships that Web Services are bound to spawn further in terms of ‘network contracts’, instead of the traditional notion of bilateral contracts.

The concept of network contracts has yet to find full support in English common law36 and the jurisdictions that adhere to it. The pointers towards recognition of such a concept have sprung from the analysis of problems associated with the standing, or lack thereof, of third party beneficiaries of bilateral contracts. However, the common law courts have steadfastly upheld the doctrine of privity and rejected any notion of contractual nexus with a third party even where specific benefits may have been conferred on that party.37 There is growing support for limiting the applicability of the doctrine of privity38 in the context of the parties’ intentions and ‘a fair allocation of the risk’ between them.39 Beatson contends that ‘The

37 This was affirmed by the House of Lords in Scrittons Ltd v Midland Silicones Ltd, [1962] AC 446.
39 Collins, note 36, above, ibid., at 126.
recognition of the right of third parties to enforce contracts made for their benefit would reduce uncertainty by allowing contracting parties to abandon an array of elaborate devices they must now use and giving them the facility to achieve what they intend directly.40

Calls for recognition of the right of third parties have been made by reference to ‘through-carriage’ cases and carriage by rail.41 Explicit mention of ‘network contracts’ has occurred in connection with construction and manufacturing,42 credit and commercial financing arrangements.43 Adams and Brownsword have attempted to conceptualise ‘network contracts’ in a general way. They define a ‘network contract’ as follows.

1. A network contract is a contract forming part of a set of contracts.
2. The set of contracts has the following characteristics:
   (a) there is a principal contract (or, there are a number of principal contracts) within the set giving the set an overall objective;
   (b) other contracts (secondary and tertiary contracts, and so on) are entered into, an object of which is – directly or indirectly – to further the attainment of this overall objective; and,
   (c) the network of contracts expands until a sufficiency of contractors are obligated, whether to the parties to the principal contractor or to other contracts within the set, to attain the overall objective.44

There are several advantages of encapsulating chains of contracts involving complex circumstances that underlie Web Services. Firstly, failure in performance at any level (or layer) could expose the potential defendants to liability for parties expecting a diversity of services. As the performance of any party would be a precondition for the fulfillment of particular obligations by other parties, it would only be proper to hold them liable for any shortfalls. Secondly, claimants who would otherwise have to climb up the chain of contracts to reach the party ultimately responsible for the mishap would have the choice of seeking remedy from the immediate party. Thirdly, the possibility of seeking remedy from any (‘proximate’) party in the network would enable bypassing jurisdictional problems; a party claiming in its own jurisdiction against another party (for instance, a Service Provider) could thus save itself from various inconveniences and costs. Finally, parties would know that they cannot shield

---

40 See Beatson, note 38, above, ibid., at 9.
41 Battersby, note 38, ibid., at 383.
42 Collins, note 36, above, ibid.
44 Ibid., at 27–28.
themselves from liability for malfeasance and proceed to make arrange-
ments for risk allocation and some form of protection (chiefly, insurance).

The upshot of introducing the notion of network contracts into online
transactions will be to lay open the responsibilities of all participants under
the complex conditions that defy jurisdictional delimitation. The inade-
quacy of apportionment of risks that ordinary contract rules provide for
under the rubric of consent and privity will be overcome. Still specific rules
will need to be worked out to turn the concept of networks contracts into a
viable tool.45

3.2 The Place of Standard Forms of Contracts

In spite of the growing popularity of standard form contracts, particularly
in B2C transactions, their relevance in the B2B context is not readily
apparent. Moreover, the contents (terms) of contracts will vary depending
on the matter they cover. B2C sale transactions relating to software and
digital goods have been based on shrink-wrap or click-through contracts.
On the other hand, relationships or partnerships, for instance businesses
committed in an Electronic Data Interchange (EDI), spell out their
expectations in advance of any transactions. They generally focus on a host
of concerns ranging from communication protocol to message format and
effectiveness, to security arrangements (eg. encoding), division or limi-
tation of liability for error/ disaster or third parties to payment.46

The coming into existence of a diversity of businesses with the ready
tools to communicate and transact without being hindered by interoper-
ability problems or cross-platform differences have the potential to
transform the manner in which contents of contracts will be arrived upon.
While it is conceivable that sellers of goods (as well as information) and
services would work out their terms well in advance of any offerings made
to them via their Web Services, their acceptability to offerors may not be a
forgone conclusion. The same conditions that have created a diversity of
businesses will entail a diversity of standard terms and conditions, each
business seeking to offer the most attractive proposition or package to
potential buyers. However, unless the parties have an ongoing relationship
or been tied to a pre-existing formula (such as in the EDI arrangement),
the likelihood of parallel offers being available to the same buyers is
obvious. Under the circumstances, it would not be proper business practice
for buyers to settle for a standard set of terms they chance upon. Neither
could sellers assume that they can dictate the terms and believe that the

45 Adams and Brownsword suggest ‘three criteria which would need to be satisfied’ in addressing privity
issues that stand in the way of third party claims: ‘First, the law should be clear, coherent, and predictable in
its application. Secondly, it should avoid commercial inconvenience…Finally, it should avoid injustice and
46 See, for instance, Dennis J. Gallitano, ‘Trading Partner Agreements: Avoiding the Pitfalls’, 19 (3) The
Computer & Internet Lawyer 10, March 2002.
buyers would turn to them. Nothing could be further from the scenario that Web Services are heralded to generate. The possibility opened for buyers to scour the entire Internet before making their decisions will translate into so many hits and misses by individual sellers unless they become willing to adopt flexibility in their terms and conditions.

The arguments against setting standards will therefore eventually outweigh those for. In the end, in the constant search for buyers, the winners will invariably be those adopting an absolute flexibility which is another name for abandoning set standards. The common denominator operating in the market will be that favouring the buyers, in other words, the lowest and permanently tending to fall. Sellers who publish their particular standard terms and strive to shove them on buyers will lose to others who undercut their terms or abandon them altogether and provide much favourable ones. The information asymmetry proverbially denying the buyers the best choices from a global market will no longer have relevance to an Internet driven by Web Services. Ultimately, the shift in power to the buyers/consumers may effectively impede any form of control or manipulation of market forces by sellers.

In the absence of standard terms, how are businesses likely to operate? It would appear logical that online transactions will still need various terms that buyers would expect to rely on against the sellers, particularly in cases of breach. One can always apply the various headings that the EDI arrangement has evolved. Recent developments in online contracting need also to be into consideration when businesses work out their modus operandi.

### 3.3 Compliance with Self-regulatory Rules

Any agreement that online parties conclude will have to comply with the relevant codes of conduct. These codes have not yet been reduced to any authorititative form, nor do they appear in a single document. Whole industries, or sections of them, have adopted various types of codes aimed at general or specific objectives such as the protection of privacy, the promotion of best business practices and the like. Then there are Netiquette rules that have evolved over time to indicate the manner of use or prohibit abuse of Internet resources.\(^{47}\)

While there may be no sanctions against those who violate the codes, the implications for offending businesses may be catastrophic. Consumers in particular are prone to attack and expose offending businesses to the multitude in cyberspace creating a deluge of email which might inundate the business’s network and ultimately shut it down.\(^{48}\) Moreover, the loss of


customers might ultimately drive the business into bankruptcy. The fear of customer retaliation is a factor that no business engaging in online transactions can ignore. Many businesses have indeed attempted to open feedback channels on the Net to get to hear complaints and nip them in the bud.

3.4 Performance Standards

The performance standards expected of the parties are subject to a number of factors. The main factor is the level of advance of technology and its reliability and availability. It has become a rule of thumb that the more available the technology is, the higher the expectation that the respective party would use it. Without this link between the availability and progress in technology and general expectations of transacting parties, reliance on the performance of any party could not be easily established.

To prove that the performance by any party has been in conformity with the contract, particularly with the implied term of meeting the relevant level of expectation of the other party, the agreement may introduce testing or acceptance procedures. The supplier of goods and services will generally assume responsibility for exercising best efforts in its performance of obligations. ‘Best efforts’ again depend on the state of technological advance and the capabilities of the supplier.

Issues may however arise as to whether other parties which team up with the supplier in performing aspects or parts of the contract should not shoulder responsibility, at least to the extent of their share of the tasks? Different parties may be responsible for system congestion, transactional delay, loss of communications or failure of delivery. Would not the Web Service provider, the Internet Service Provider (ISP) and other intermediaries or business partners of the supplier be responsible in some capacity? The identification of who exactly bears responsibility for any shortfalls is important because the deployment of Web Services would arm every participant with the possibility of disrupting the fulfilment of the transaction through failure to perform its portion of the general bargain.

It goes without saying that, in every situation where the interlinkages and transactions between diverse parties on the global network have not been placed on a contractual footing, tort law will step in. Thus negligence with respect to use of a proper system or infrastructure, safeguarding transactional data, prevention of unauthorised access, protection of intellectual property and content might become a subject matter of such tort. Yet, whether and to what extent, any party in the chain will become tortiously liable to another on the same network is not easy to predict. Apart from the inevitably dissimilar approaches and remedies offered by the multiplicity of jurisdictions to which the parties might seek to resort in their claims, the ubiquitous nature of computing that Web Services usher in will expand the
The capability that Web Services provide to suppliers of goods and services to make these available to indeterminate customers might not be a subject of scrutiny until it throws up a deluge of claims when things go wrong. Wrongs committed at any of the layers of computing and interconnections may give rise to claims by all parties that could have been affected by the specific hazard. A software solution installed on a machine which receives constant updates online will prompt claims by many parties, should an update on patching a discovered lethal bug fail to arrive because of a system failure. Not only will the machine operators proceed against the sellers and the software house for any accidents or defective operations, they may sue the relevant service providers (which could be their ISP, ASP or any number of Web Services providers), including others in charge of one system or another. The potential defendants of the machine operator’s action might also engage in claiming against each other for whichever aspect of the failure they might feel entitled to recovery.

3.5 *Apportioning Risks*

Although suppliers of goods or services will generally be in charge of the front-ends of a series of processes that are undertaken in their back-office, those suppliers cannot assume that the party in default of its bit of the overall task will automatically bear the burden. Moreover, according to traditional rules of privity, back-office operations may not lead to any contractual nexus between the buyer and those operators. Hence, it would be prudent for the supplier to work out the exact nature of the responsibility of the back-office participant, lest it shoulders the entire responsibility by itself.  

It may of course be possible for the supplier to pre-arrange the extent of responsibility among the back-office operators and transfers such into terms of the contract with the buyer. This would enable the buyer to make direct claims for breach against the specific party in default rather than the overall supplier. Whether this becomes acceptable to the buyer is another matter. The prudent buyer might seek to spread the risks of breach to more than one party in spite of the ease of pursuing the main supplier. The advantages of such segmentation of risks to the benefit of the buyer will

---

49 Matsuura notes, regarding the ‘security’ aspect, ‘In the world of the ubiquitous network, the parties facing legal responsibilities for protection of security will include many players who currently face no such requirements.’ See, Jeffrey H. Matsuura, *Security, rights, and liabilities in e-commerce*, Boston : Artech House, 2002, at 220. Matsuura also cites the increased onus on manufacturers of ‘Web-enabled’ consumers products to make sure that such products are ‘compatible with system-security standards and requirements’ *Ibid*.

definitely have to be weighed against the disadvantages of pursing different parties. However, this is an area that will need practical resolution as much as judicial (legislative) conceptualisation, as discussed above under ‘network contracts’.

Regardless of whether the supplier decides on apportioning risks to other parties, the parties might resort to the use of liquidated damages for breach.\textsuperscript{51} This has the benefit to both parties of circumventing disparity in laws and jurisdiction that apply to contractual breaches and allowing them to resort to a ready path for settlement of their dispute instead of waiting for the courts. Finally, the parties may also agree on warranties and indemnities for any likely infringement of third party rights (such as intellectual property).\textsuperscript{52}

4 Liability Arising from Development and Protection of Content

Suppliers of goods (as well as information) and services deploying Web Services will have more onerous obligations than ordinary (realspace) businesses as regards development, delivery and protection of content. For one thing, they must ensure the currency and accuracy of information (eg. price lists, sales performance) they supply to potential customers. Otherwise they run the risk of legal claims, even prosecution, for misleading the user of such information. Secondly, they need to ensure that information made available to their customers (particularly in B2B transactions) is adequately protected from copying and unauthorised distribution. They must clearly define permitted uses of information as well as proprietary material such as trademarks. Thirdly, in using third party materials (information or other work), they need to set out the perimeters of authorisation by the proprietor, the manner of use or display, duration and any payments, as well as responsibility for content.

The global presence that Web Services allow such businesses will also bring about exposure to potential liability under a multiplicity of laws and jurisdictions across the world. The choice of businesses to go global and offer their goods and services to other businesses and customers will necessitate an adoption of the highest standards encapsulating at least the obligations of any business in the major jurisdictions. One would therefore be operating at one’s peril if one did not subsume, for instance, the European Union’s Data Protection Directive and the measures introduced for consumer protection on the Internet.

A consequence of such an approach is that Web Services will pave the way

\textsuperscript{51} Ibid., at 1–7.
\textsuperscript{52} Ibid., at 1–7.
for an approximation of legal rules on a world level. However, such a process will not stop at the adoption of minimal standards—as has been the customary process in treaty formation. The urge, on the part of businesses, to save themselves from liability under disparate laws and jurisdiction coupled with the competition for customers who seek better protection of their rights will drive up the standards ever higher. The result will be the adoption of the highest common denominator by all businesses with ambitions to match their capabilities.

Similarly, the impact of measures that businesses routinely publish to offset their burdens, such as limitations of liability for defects or errors, may be significantly reduced. Again, this is because of the inherently competitive outcome that Web Services inject into business operations. Insistence on limiting liability towards customers will have to give way to apportioning risks to back-office parties if the supplier is to continue to retain the trust of customers and not be displaced by other offerors at better terms and conditions. This does not necessarily mean that the use of limitations will disappear altogether; rather, that their frequency will diminish in proportion to, among other things, the number of competitors in the respective market.

It should not be forgotten either that back-office operators with roles of mere carriers or conduit have generally become exempt from any liability for content. Yet, in the wake of increasing mergers and convergence among Internet service and content providers, the beneficiaries of the exemption may not be that many. Where such businesses engage in value-added services, therefore, the possibility of an extension in their liability arises. A US case in point is *Southwestern Bell Telephone Co. v Delaney*.

### 5 Security, Protection of Data and Privacy

The integrity and security of transactional data or information have been the most important concerns for e-commerce and remain so. Both consumers and businesses do not trust that online processes and transactions may be free from tampering by unauthorised parties; on the contrary, they fear that they might incur losses. The use of digital signatures, the establishment of trust creation bodies such as certification authorities (CAs), improvements on securing payment systems (particularly encryption through the Secure Sockets Layer, or SSL) have allayed somewhat the fears of consumers from hacking and other surreptitious intrusions.

Security issues are even more paramount for the success of Web Services simply because the potential problems of misuse will go up. The very design

---

54 809 S.W.2d 493 (Tex. 1991).
of an open, federated network, with the possibility of a single sign-on identity solution for every participant (business or individual), multiplies the risks of misuse. While the deployment of Web Services on networks across the world may safeguard interoperability between all kinds of providers of goods and services, the same process will open up new vistas for hackers and intruders of all types. Matsuura comments,

As more content and transactions are processed by the network, incentives for unauthorised activities will increase. The breadth of the overall public network also provides more access points and more tools for those with intentions to misuse the equipment. The ubiquitous network thus increases both the motives for malefeasance and the means to breach the security of the network. In addition, the ubiquitous network makes the potential adverse effects of security breaches greater than they are today. When the network is fully integrated into more functions used by more people in more parts of the world, breaches of network security carry far greater potential for harm than they do with a more limited network.55

Current approaches of differentiating and dealing with disparate types of users of information in granting varying levels of authorisation (to computer networks, file directories, application programs) and ascertaining (authenticating) compliance in an appropriate manner may not be totally relevant in the context of Web Services. It is therefore understandable if the inadequacy of security is perceived as the most important factor in holding back the adoption of Web Services.56

One might interject that the adoption of technological solutions will resolve this problem. Yet, even companies such as IBM and Microsoft are reportedly ‘just starting to make serious security recommendations for Web service technologies like SOAP.’57 The advice given to businesses hence is ‘until a solid base of technologists and a reliable security framework materialize, they should play a limited role within your Internet applications.’58 Microsoft has recognised this openly: ‘Because there are no broadly-adopted specifications for security, routing, reliable messaging, and transactions, developers today either have to go without these capabilities or they develop ad-hoc solutions that they must resolve separately with each partner or customer. Going without these capabilities

55 Matsuura, note 49, above, ibid, at 220.
58 See Plummer and Andrews, note 5, above, ibid.
can expose a company to risks and degrade the value of its XML Web services.\textsuperscript{59}

5.1 Personal data protection

The legal parameters for the collection, management and use of data will face similar problems from increased use of Web Services. As the range, availability and dispersal of computing devices and their integration increase, the frequency of abuse might climb thereby impacting hugely on legal obligations relating to data/privacy protection. Judging by the negative experiences in efforts to prevent unauthorised access to, or theft of, data on the Internet,\textsuperscript{60} the open network that Web Services permit will present an insurmountable task. Although devising an open, safe protocol that protects consumers' private financial and other data may be critical in gaining consumer trust, such a solution is still either lacking or has not found broad acceptance.

Microsoft's Passport was meant to provide a reliable authentication service on the Web, thus enabling businesses to resolve longstanding problems of requiring customers to log on at every site they accessed. By offering Passport, Microsoft was hoping that businesses will not have to devise their own solution as well as that customers will reap the benefits of saving time and efforts from having to sign on at diverse sites on each of their visits. Nevertheless, Passport has not gained popularity. The reluctance to divulge one's particulars to an application still not perceived to be secure from intrusion accounts for the limited success.\textsuperscript{61}

Indeed, Microsoft had to retreat from its ambitious plan to develop a


\textsuperscript{61}One commentator contended, 'It does not allow for sufficient control over the use of authentication information by a user and, where current technologies fall short of the ideal, it trades off security in favor of convenience in a way that leaves users vulnerable.' See Marc Slemko, 'Microsoft Passport to Trouble', November 5, 2001. Available at http://alive.znep.com/markspassport/. A Microsoft's .NET UK marketing manager, reportedly admitted, 'We recognise that currently Passport isn't fit for doing banking transactions, right now there are certain applications it's not suited to. But this is why we are working with people like Egg to get it up to that level.' See, J Gardiner, 'Microsoft admits "Passport not secure enough"', November 6, 2001, Silicon.com. The same official stated 'We found some strange tweaks in the My Wallet part of Passport, which is currently being moved and totally re-architected anyway, and responded immediately. We can confirm that no data was compromised.' See 'Microsoft Passport flaw revealed – Wallet insecure', November 5, 2001; available at http://www.silicon.com/a48874. According to a report summarising a Jupiter Consumer Survey, 'just three percent of consumers would trust Microsoft to store their personal data. Banks were found to be the most trusted identity repositories, chosen by 27 percent of consumers'. See, David Schatsky, James Van Dyke and Rob Leatherman, 'Identity Services: Assessing the Benefits and Timing Investment – Concept Report', May 22, 2002, available at http://www.jupiter.com. The same writers added 'Merchants, and especially financial institutions and other players with large, established customer bases, are extremely wary of inserting a third party between them and their customers for the purposes of online identity management.' Ibid.
single central consumer database as part of its .Net My Services.\(^6^2\) The idea was to store consumers’ personal information including private financial data and make it available to them and the relevant businesses for a fee. Both consumers and business did not warm to the proposal; the former because of repeated reports of security glitches at Microsoft and the latter in view of their fear of passing access and control over their customer database to Microsoft.\(^6^3\) Microsoft has since shifted its strategy towards selling the software to businesses that will then develop their own database.\(^6^4\)

Meanwhile, the fate of the proposal by the Liberty Alliance for a ‘federated identity’, instead of those proposed by single companies, is still pending. The scheme has been described in these terms: ‘In a federated scheme, multiple parties are empowered to manage identity information and to authenticate users. Consumers might select their bank as their identity manager, for example, or their credit card company, or several trusted companies with which they work. They might, then, grant permission to those companies to authenticate them to other online services with which they don’t yet have a relationship.’\(^6^5\) Yet, according to the same commentators, ‘these applications will not be widespread for at least two years, until 2004 at the earliest. The Liberty Alliance is developing a specification, not a tangible technology; it’s not yet possible to predict which company will deploy it or when.’\(^6^6\)

6 Intellectual Property

Web Services will probably not generate entirely new problems to intellectual property (IP) that have not already been posed by the Internet.\(^6^7\) Problems relating to linking, framing, caching, metatags and content-sharing\(^6^8\) of proprietary stuff without the authority of the proprietors will continue to trouble businesses. The potentially increased access to trade secrets, business method patents, trademarks and copyright matter that Web Services open up through interconnections spanning all kinds of industries will be fraught with more difficulties for proprietors to
maintain their control and continue to reap benefits.\textsuperscript{69} Trademarks could also be diluted or infringed if their use by unauthorised third parties implies a commercial relationship with the proprietor.

Current strategies of managing IP online through, for instance, safeguarding copyright or trademark matter in the process of hyperlinking, framing or in the use of keywords or banners may not be totally suitable to the expanse of the global network that Web Services create. Digital rights management systems might not suffice in the conditions of diversity and complexity of the network.

The potential issues that confront proprietors in licensing their software might become more intricate through Web Services. Fort starters, it opens up further possibility of reverse-engineering of software. It may also impinge severely on open source software, particularly through increased fragmentation\textsuperscript{70} by the multitude of end-users in cyberspace. In situations where adapting Web content or text is permissible to third parties, the question of whether such adaptation stays within the limits set by the proprietor/licensor will be hard to establish. Moreover, what level of adaptation amounts to an infringement will not be easy to establish.\textsuperscript{71}

In all these cases, what is the best form of protection that proprietors/licensors could hope to adopt? Even if licence restrictions could be imposed on potential licensees, would there be any chance of enforcing such restrictions against the recalcitrant? Added to this is the concern that undue restrictions could curtail the free flow of information.\textsuperscript{72} In any case, whatever licensor/ee obligations may be assumed in contract or through legal requirements, the susceptibility of the network to enable non-proprietors to subvert any restraints may have overriding significance. It is not easy to conjecture what forms and methods of protection would be necessary to stop what might otherwise be a free for all in as much as online IP is concerned. Again, past practice suggests that the odds are set against proprietors who might seek to rely on current forms.

7 Dispute Resolution

The resolution of disputes arising from online transactions has yet to find an agreed approach and procedures. The dread for the unknown (in terms of the laws of the other contracting party and the impartiality of their courts) hangs over all transactions. Unless the parties handle it in specific clauses, the incidence of many national laws on a transaction may prove to

\textsuperscript{69} Matsuura observes, ‘Increased use of distributed-computing systems poses one of the greatest challenges for effective enforcement of legal rights in the future.’ Matsuura, note 49, above, \textit{ibid.}, at 222.

\textsuperscript{70} \textit{Ibid.}, at 146–7.

\textsuperscript{71} \textit{Ibid.}

be daunting for both parties. A case in point is the diversity in consumer protection laws across the world. Moreover, the appropriateness, or otherwise, of the regular courts notwithstanding, the parties may nevertheless end up having to resort to them. As a matter of fact, most standard contracts concluded online routinely include clauses on the applicable law and jurisdiction. Consequently, dispute resolution might become subject to the choice of the supplier of goods or services.

Nevertheless, as pointed out above, the relevance of standard terms of contracts might be severely eroded, if not eliminated, by the growing closure of the information gap between suppliers and buyers. In that sense, it could be hazarded that a more neutral dispute resolution mechanism might be called for by the widespread implementation of Web Services. The use of arbitration or other alternative dispute resolution (ADR) forms may thus save both parties from the uncertainties that characterise their transactions. A possible way out could be the rise of third party dispute resolution services, whether endorsed by governments or operating independently. Perhaps the shortcut to the complexity that Web Services introduce in online transactions, particularly in the proliferation of legal requirements of different jurisdictions and the manner of resolving disputes arising, is removing the problem altogether through some form of treaty. It is proposed that the Internet be declared a single jurisdiction subject to rules custom-made for its purposes. These rules could also be the foundations for the emergence of universal (in the sense of non-national) laws applicable to all businesses operating online.

In the meantime, whatever venue or form of dispute resolution is adopted, the parties will need to adopt certain house keeping measures such as maintaining accurate electronic records and evidence. In any case, some transactions must be preserved in view of tax or other government regulations. Keeping such records may be a daunting task for smaller businesses to undertake on their own. However, the task could be outsourced. Indeed, the storage and maintenance of records has already started to become an activity left to third parties. Web Services will hence only speed up its further development.

8 Conclusion

This paper has demonstrated that Web Services will not prompt a radical departure from the currently evolving legal framework for the Internet. For one thing, Web Services are only extending existing capabilities towards the ubiquitous network. Yet, one cannot say exactly how the legal response will shape out finally.

73 For an extended discussion and tips, see Matsuura, note 49, above, ibid, at 9–46.
74 Ibid.
The likely general impacts of Web Services on the law are linked to the breadth of their reach and the attendant risks and responsibilities of all participants whether jointly or alone. As Matsuura rightly comments, ‘the range of legal requirements applicable to the digital marketplace is currently complex and is virtually certain to be substantially more complex in the future. The digital marketplace is a major part of the global economy. As the number of participants in that marketplace increases, and the variety of their transactions and relationships expands, more legal requirements will be applied to the marketplace.’\textsuperscript{75} It may therefore be hazarded that the nature of contracts and jurisdictional matters and consequently means of dispute resolution will be the most extensively impacted.

Many of the problems emanating from emerging complexities prompted by Web Services can be tackled through developments of new standards or extension of existing capabilities. Thus, the problem of end-to-end security is reportedly being addressed by Microsoft, Hewlett-Packard and Sun as part of their ongoing work in developing ‘standards for interoperability and building support for Web Services into their existing offerings’.\textsuperscript{76} Toolkits for building interfaces and creating implementation codes are also maturing.\textsuperscript{77}

Yet, Web Services are still very far from becoming the general industry standard. It is generally recommended\textsuperscript{78} that, where security and complex interactions between services are not urgent requirements, businesses can begin using Web Services today. Borck adds, ‘At the very least, businesses can begin experimenting with in-house Web Services and private repositories to address interoperability flash points within company walls.’\textsuperscript{79} The underlying hope is that such an approach will prepare them for the promised future of quick and cost-effective application integration across the Internet.

\textsuperscript{70} \textit{Ibid.}, at 227.
\textsuperscript{71} See Borck, at note 7, above, \textit{ibid.}
\textsuperscript{72} \textit{Ibid.}
\textsuperscript{73} See, for instance, Plummer and Andrews, note 5, above, \textit{ibid.}
\textsuperscript{74} See Borck, at note 7, above, \textit{ibid.}
XML E-Contracts: Documents that Describe Themselves

DARRYL MOUNTAIN

Abstract
This article discusses how XML will facilitate and drive the transformation of contracts from paper documents to electronic legal documents. It contrasts XML-based contracts with conventional contracts, summarizes the benefits of storing contracts in XML, and analyzes the impact of Microsoft’s forthcoming release of a version of Word that will allow documents to be saved as XML. The article then sets out the current state of the LegalXML eContracts committee and concludes by suggesting a plan of action for law firms.

1 Introduction
XML (extensible Markup Language) is an acronym that evokes blank stares from most lawyers, yet lawyers have been involved in its evolution from the very beginning. XML is a simplified version of SGML (Standard Generalized Markup Language), the original markup language that was invented by an American lawyer named Charles Goldfarb in the early 1970s. It is a W3C standard, meaning that it is supported by the World Wide Web Consortium, which leads the technical development of the Web. In the past five years, XML has moved out of the early adopter phase and into the mainstream. The ‘tipping point’ for XML may very well be

---

1 512 East 12th Street, North Vancouver, BC, V7L 2K4 Canada. Telephone: 01.604.771.9424. E-mail: darryl.mountain@ontago.com

Microsoft’s release of Word 2003 (see http://www.microsoft.com/office/developer/preview). This version of Word is an XML editor and allows users to save their documents as XML. It demonstrates that Microsoft is open to the prospect that XML eventually will supplant both its proprietary binary Word .doc format and its ‘rich text’ format. If Microsoft is successful in this transition, users of all older versions of Word (i.e. 97, 2000, XP) will have to upgrade.

LegalXML is a new family of standards under development that eventually will dominate the electronic exchange of legal data. LegalXML has been given short shrift to date in discussions of the future of law and it is time it was given more exposure. It is tailor-made for the online world toward which legal applications are migrating. It has a place with respect to online advisors, which deliver interactive legal advice over the Internet, and almost any application that involves the exchange of legal information. XML standards for common law contracts are being created within a body called OASIS http://www.oasis-open.org/.

XML is both facilitating and driving the transformation of contracts from paper documents to electronic legal documents. This transformation involves more than simply replicating what we have on paper in an electronic medium. As we transfer contracts from the two-dimensional world of paper to the multi-dimensional world of cyberspace, we are, in effect, adding other dimensions to their existence. As Ethan Katsh points out, this may alter our thinking such that ‘a contract might be viewed not as a piece of paper or as an agreement made at a particular time and place but as a continuing and ongoing process of collaboration.’³ Electronic contracts will be ‘dynamic, modular, multimedia entities’ that will involve interactions between people and people, people and machines, and machines and machines. One legal issue that will have to be resolved is to what extent the XML tags themselves become a part of the contract.

2 What is XML?

XML is not a programming language but rather a non-proprietary standard for creating markup languages for information exchange. A markup language is ‘a set of conventions for annotating texts for editorial, publishing, or other purposes.’ As LegalXML ‘guru’ Winchel ‘Todd’ Vincent III has stated,

The power of XML is that it is a tool that can change data to information. XML does this by making it possible for software to capture identifiable pieces of information, place the information into documents, and then ‘parse’ (extract) information from documents automatically.⁴

3 How will XML-enabled Word be different from today’s Word?

Microsoft Word’s proprietary .doc format is the current standard for legal documents, with a dominant share of the legal market. When you create a precedent using Word, you type in free flowing text, using formatting as a proxy for structure in the document. For example, you use headings and subheadings to guide the reader through the document. Commentary to the text is also indicated through the use of formatting, typically by bolding it and enclosing it in square brackets. The document is stored in Microsoft’s proprietary format.

XML-enabled Word documents will differ from current Word documents in two principal ways: they will be structured and open.

3.1 Documents will be structured

With XML, a rigorous underlying structure operates to standardize the document so that it can be manipulated by computer programs as a tree of data. This is accomplished through the use of machine-readable tags that are invisible to the user and stylesheets that allow the user to format the same information in a number of ways. The purpose of the tags is to identify the information contained within the tags: for example, `<date>` January 16, 2003 `</date>`. The effect is similar to activating ‘reveal codes’ in WordPerfect, except that XML tags don’t describe the formatting; they make explicit the structure of the documents.

Everything in a contract fits into a hierarchy. At one extreme, structural markup constructs a hierarchy of clauses, subclauses, paragraphs, and subparagraphs. Non-structural markup, on the other hand, is more complex because it involves making legal interpretations as to whether a particular provision is, for example, a condition or a warranty. Some markup examples fall between these two poles.

Because XML documents are structured, internal check mechanisms are able to monitor the creation of each document. For example, you can set rules that don’t allow you to refer to a party unless it has been created or to use a term unless the term has been defined in the contract. The structured nature of XML documents also allows lawyers to identify, extract, and manipulate specific chunks of information.

3.2 Documents will be open

XML documents adhere to an open standard, which means that there are no proprietary limitations on who can use the standard. There is a wide choice of tools that manipulate XML documents. Because XML is independent of any operating system, these tools are available for Windows, Linux, Macintosh, and other operating systems.

In his recent book *The Future of Ideas*, Stanford law professor Lawrence
Lessig describes how communications systems can be divided into three distinct layers, each of which is either controlled or free. This analysis can be applied to legal documents.

At the bottom is the physical layer, the computer and the wires that link it to the Internet. The middle layer is the code layer, which consists of the software that makes the hardware run. That code includes operating system software, document management software, word processing software, and document assembly software, macros, or templates that sit on top of the word processing software. The top layer is the content layer, the traditional free-flowing text of law that is read by humans and is represented via document formats such as doc, rtf, html, pdf, and xml. Currently, all three layers are controlled through property law and intellectual property law. The code layer, though currently the domain of Microsoft by virtue of its control over Windows and Word, has the potential to be free.

There are several disadvantages to Microsoft’s current control of the code layer. First, any wholesale redesign of Windows or Word would disable the rest of the code layer and would affect the other layers. For example, the upcoming changes to Word will require document assembly software that piggybacks on Word to be altered and the documents themselves to be converted. Second, because only Microsoft can ‘muck about with its code,’ Microsoft controls the pace of innovation. For example, there is a demonstrated market need to open and save fragments of content smaller than a ‘document’. Word is ill-suited to doing this. If the code layer were free, many innovators would be addressing this need. Because the code layer is controlled, innovation in this field will take place according to Microsoft’s timetable. This is expected to change once XML becomes the native file format.

Open code such as XML has the advantage that it does not permit strategic behaviour. Because the source code is free, there is the perpetual possibility that an open code project will ‘fork’, with development splitting into different directions. This possibility operates as a check on the power of any particular clique within the project and pressures development to proceed in the interests of the broadest range of users.

The open nature of XML documents also reduces the effort required to achieve interoperability among various pieces of software. First, an XML document is a text document, not an unreadable binary format like Word’s .doc format. It can be manipulated by XML aware tools. Second, different communities typically create XML grammars to describe the documents they need. XML-encoded data contained in a contract can be sent from

---


6 Ibid at 67.

7 Ibid.
one piece of software to another, and manipulated as a contract (as opposed to a generic collection of words) so long as each piece of software knows the contract XML grammar. For example, it can be traded among precedent systems, word processors, case management systems, deal rooms, and contract management systems. The receiving software will automatically discover and understand the function of the data.

At this point, it is reasonable to ask why law firms, even those that are large and technologically advanced, would be interested in putting money into an open standard. Wouldn’t they be doing the groundwork for their competitors?

To a certain extent, yes. The first company to exploit a new technology idea is not always the one to create a market out of it. For example, Charles Schwab was able to dominate the online brokerage business despite starting late in the business behind a joint venture called Net Investor that was launched in January of 1995.\(^8\)

However, Lessig argues that the return from deploying a new idea is high, even if others get the benefit of the new idea, as well.\(^9\) The market produces enough incentive on its own, so the fact that others can free-ride doesn’t kill innovation. He gives the example of IBM, which reportedly has invested over US$1 billion in the development of Linux and Apache, thereby spending its money on something it might otherwise get for free. IBM’s incentive is that it sells more equipment and services if the software that runs that equipment is improved. If law firms could use a LegalXML contracts standard to increase the speed of their transactions and thereby do more transactions that were previously uneconomical, then the same argument for increased revenues would apply.

4 Why store contracts in XML?

Previous attempts at standardization in the field of contracts mostly have involved the language of the contracts themselves (see http://www.commonaccord.org/, for example). When agreements of the International Swap Dealers Association (ISDA) are negotiated, parties start with boilerplate language and set out any deviations from that language in schedules. The boilerplate, which forms the bulk of the agreement, never changes. While XML will facilitate the use of boilerplate information within a contract, use of XML does not require lawyers, judges, or legislators to standardize document appearance or language.


\(^9\) Ibid at 69.
Storing contracts in XML will bring some benefits that can be predicted and others that cannot. As with many technologies, LegalXML will have unforeseen benefits as creative people experiment with the new tools.

4.1 Accurate, focused searching
First, you can use software to search through a group of contracts. Searches can be limited to words within particular tag contexts. For example, when conducting due diligence, a lawyer would be able to quickly scan the governing laws of all agreements in the data room or to search for all contracts dated after January 1, 2000 that involve a particular party. This is achieved without using natural language technology. Even a powerful search engine such as google is unable to do such context-based searching at the moment. In addition, the lawyer will be able to browse and manipulate each contract in a collapsible outline mode.10

4.2 Divorcing content from presentation
Because XML divorces content from presentation, lawyers will be able to rearrange presentation of contracts into various preferred formats, depending on the reader’s tastes and circumstances. For example, law firms could easily implement a change to the firm standard font or even develop client-specific styles for their precedents. In addition, people who use XML tools to create documents do not need to spend any time fiddling with the format (ie changing margins, paragraph spacing, heading styles, etc.).

The openness of XML documents allows for multichannel publishing. Lawyers can view their documents in Word or PDF or using a Web browser, or even via a handheld device such as a Palm or Blackberry. In the future, there may be provisions for electronic filing of XML contracts with securities regulators, tax authorities, and property and corporate registries. Alternatively, the regulators could ‘plug in’ to the contract itself:

One can imagine a financial intermediary as a patient in the hospital’s intensive care ward. Electronic ‘nodes’ would be attached to all of the financial intermediary’s ‘vital organs.’ The regulators would monitor the intermediary’s ‘vital signs’ on a ‘real time’ basis. They could immediately (or almost immediately) discover changes (such as withdrawals of capital or shortfalls of customer securities). Indeed, the complete financial condition of the intermediary would be continuously exposed.11

4.3 XML facilitates reuse
Information relevant to contracts and transactions needs to be captured

---


11 Supra note ii at 132.
only once. Content can be collected before the method of presentation is even known. For example, lawyers will be able to tag information that is input via extranet by a party to a transaction and then ‘explode’ it through the deal documents, even if those documents are drafted at a later point in time. In the words of Eddie O’Brien, President and CEO of Ringtail Solutions Inc., ‘an enormous amount of work, consumed in traditional legal practice by finding, losing, misinterpreting, correcting, and simply re-typing legal data, will be avoided, once XML standards have been created and put to use throughout the legal industry.’

Where a number of precedents share one clause, any changes to that clause will be able to be made in all precedents at once.

4.4 Collaboration and negotiation
XML will make it easier for knowledge to travel between organizations. It will be possible to send a marked-up contract drafted by one law firm to another law firm for review and negotiation. For example, many documents are currently exchanged in online dealrooms, such as IntraLinks http://www.intralinks.com/. XML will improve the functionality of these dealrooms by allowing online collaborative authoring. Transaction documents often represent various stages of negotiation with respect to complex sets of terms. If significant terms and passages were tagged, all parties could quickly generate a filtered view of the documents in progress showing the current state of such terms and passages (eg ‘agreed, still under negotiation, worked on by Bloggs’), rather than having to slog through the entire text. The documents could even be summarized automatically.

4.5 Better management of contract portfolios
XML will automate the processing of contract content for use in contract management applications. Once a contract has been signed, it passes downstream from the document creation phase of its lifecycle to the contract management phase. There is a discontinuity at this stage because the contract is unable to monitor its own implementation. Human intervention is required to manually input information from the contract into a tracking system that flags relevant information, such as the renewal date. By way of contrast, XML tagging largely eliminates this discontinuity. Information that is tagged in XML can be captured automatically when the contract is fed into a contract management system.

The portability of tagged information will also allow the linking of contracts and subcontracts. Loan agreements will become ‘living’ docu-

---

13 Personal e-mail from Marc Lauritsen dated August 21, 2002.
ments, linked to software that monitors compliance to financial thresholds and triggering warning alerts when covenants have been breached.\textsuperscript{14}

Law firms and legal departments will be able to keep statistics on their portfolios of contracts. They could audit their portfolios to determine how many contracts have a particular clause.

4.6 \textit{Precedent Asset Management}

Today when lawyers create documents, they determine the value of these documents by the billable hours that go into their creation. They try to charge as much as possible to the original client and then reuse the documents with subsequent clients. This is an artificial measure of value creation. In the future, law firms will be able to keep track of each clause that is created and how many times it is used. This will enable the document creator to be compensated for documents created in terms of profitability and number of times used rather than creation time. It will also enable law firms to value their precedent assets (and thus their firms) more accurately, by the net present value of the actual income the assets will generate in the future, less their maintenance costs.\textsuperscript{15}

5 \textbf{E-Contracts Committee}

XML standards for common law contracts are being created within a body called LegalXML. Founded in 1998, LegalXML is now a collection of technical committees within OASIS, a global, not-for-profit consortium that drives the development of e-business standards. OASIS includes groups that work on XML standards for everything from auto repair to business transactions.

LegalXML is developing open technical standards for the electronic exchange of legal data. Members are in private industry, academia, non-profit organizations, and government. The idea is that companies will cooperate in setting license-free standards and then will compete on adding value that benefits from the adoption of these standards. Sponsors include publishing giants Thomson and Reed Elsevier.

A separate organization, LEXML, is the forum for XML standardization in the legal domain in Europe. LEXML is focused mainly on civil law jurisdictions. The two organizations are partnered.

LegalXML is comprised of eight technical committees. These are Court Filing, eNotary (self-proving electronic legal information), IntJustice (data exchange among justice system branches and agencies), Lawful Intercept (global sharing of criminal evidence), Legislative, ODR (online dispute resolution), Transcripts, and eContracts. These committees aim to develop

\textsuperscript{14} Conversation with Dr. Lawrence Leff, May 21, 2001.
\textsuperscript{15} Personal e-mail from Jason Harrop dated September 25, 2002.
Document Type Definitions (DTDs) or Schemas within their respective arenas. Of these committees, the Court Filing Group is the most advanced, having developed Court Filing 1.1 Proposed Standard DTD and the Court Document 1.1 DTD.

DTDs and Schemas are alternate means for specifying the ‘grammar’ or rules that the hierarchy of tags in a particular document must follow. A document can be compared against the DTD or Schema to ensure that all mandatory information has been tagged for that document. Although there are some well known DTDs in widespread use, the newer Schema standard is gradually supplanting DTDs for new work.

The EContracts committee likely will have the biggest impact with respect to non-litigious areas of law. It exists to develop open XML standards for the markup of contract documents in the Anglo-American legal domain. The core scope of this activity will be to create DTDs or schemas that can be used by parties (a) to negotiate and finalize contracts in an application neutral format; (b) to exchange contract contents as valid XML; (c) to automate processing of contract content; for example, for use in contract management applications; (d) to support the production of human readable output documents; and (e) to facilitate the use of reusable or boilerplate information within a contract [http://www.oasis-open.org/committees/legalxml-econtracts/charter.shtml].

The EContracts committee is working toward the goal of devising a Schema for representing contracts that meets the business requirements of participants. This Schema, like any other Schema, will be supported by the new Microsoft Word 2003 for formatting and validation. The group is concentrating first on the structural markup, a hierarchy of clauses. The group has developed a statement of requirements for a clause model and is now completing work on a solution that meets those requirements. At the same time, it is seeking to understand what non-structural markup is necessary. The structural and non-structural efforts are conceptually independent.

As different industries design their own XML protocols, one challenge will be to manage overlap with other professional initiatives. For example, FpML (Financial products Markup Language, see [http://www.fpml.org/]) is an XML-based protocol for complex financial products. FpML standards may influence the markup of contracts in the banking and finance field. Other standards include Australia’s residential Lending Industry XML Initiative, see [http://www.lixi.org.au/] and ACORD [http://www.acord.org/], an initiative of the insurance and reinsurance industries. The difference between these initiatives and the eContracts project is that these initiatives create standards for data contained within contracts while the eContracts group focuses on creating standards for structure and markup applicable to all contracts.

Daniel Greenwood, an American e-commerce consultant and MIT lecturer, is Chair of the eContracts committee. One Co-Vice chair, Jason
Harrop, is an Australian employed by the Melbourne-based legal technology firm SpeedLegal Pty Ltd. The other Co-Vice chair, Dave Marvit, is a specialist in automated negotiation at Fujitsu Labs America. Decisions on specifications of a standard are subject to a 2/3 majority vote by all members of the technical committee.

Jason Harrop is Chief Technology Officer of SpeedLegal, which is partly owned by business and legal publisher CCH Australia Inc. SpeedLegal has developed SmartPrecedent, an XML-based document assembly system that uses XML standards and a Web browser interface. Document assembly is a branch of expert systems that generates a document by having the software ask questions of the user.

XML adds a new dimension to document assembly, which traditionally has been about moving information from a word processor template into a word processor document. This new stage of evolution enables the sharing of information among many different products, irrespective of platform.

XML-based document assembly is more than a matter of enhancing speed and accuracy: it is part of a knowledge management solution that avoids proprietary word processing formats. Eventually, says CEO Jamie Wodetzki, the document creation world will revolve around collaborating on an online document to which central access is provided, not iteratively exchanging entire word processor drafts.

Current SpeedLegal customers include legal publisher CCH and various corporate legal departments and law firms, including some in non-English speaking jurisdictions.

6 What do law firms need to do?

Clients are beginning to understand the benefits they will accrue by being able to manage their portfolios of contracts more efficiently. Just as client pressure has led to law firm use of extranets, it will lead to their adoption of XML. Many Fortune 500 companies already have embraced the XML standard and some leading law firms are beginning to store their documents in XML format. Here is what law firms need to do:

- Understand the contracts life cycle. What do your clients do with a contract once it has been negotiated? Could your firm profitably take over any contract management functions on behalf of clients?
- Understand how the drafting process can be improved to meet client needs for transparency and efficiency.
- Address XML in your strategic plan. Plan your migration to Word 2003 based on when you plan to migrate to XML. Re-evaluate any non XML-based development projects.
Consider establishing a pilot project, storing the documents in XML. This will help you to understand the benefits and issues and will prepare you for using XML in a project with a client.

Consider storing your precedents in XML format. By putting your knowledge base in XML, you can reduce your exposure to proprietary binary formats, interoperate more easily, and stop wasting time formatting documents. You can start by using the structural markup envisaged by the eContracts Technical Committee.

Even if you choose not to move forward with any XML projects at present, seek to understand how XML will affect your clients and their competitive advantage in their particular industry. In a matter of time, clients will require law firms to deliver XML formatted documents or to help them tailor their own documents. When that time comes, at least you will know what they are talking about.

Consider participating in the eContracts committee or closely monitor the OASIS website. The best way to create standards is by experimenting with real world documents and problems, doing what makes sense from a lawyer’s perspective rather than a computer scientist’s perspective. By becoming involved before the standards are finished, you can influence them yourself and ensure that they meet your needs.

7 Cites


Invention in Patent Law: A Review and a Modest Proposal

DAVID VAVER

Abstract

This paper considers how the notion of invention is presently conceived of under the patent laws, and what changes to that conception may be desirable for the future.

1 Preliminary

The patent system is based on the theory that people should be granted an exclusive time-limited right to encourage them to produce, or to reward them for having produced, certain results that are thought to be socially beneficial. The results typically stem from experiments and research to solve a problem in the industrial sphere, and produce some new and unobvious solution to that problem – be it a new article, substance or method, or an improvement on previous technology. Without the prospect of such a grant of rights, fewer people and resources would, it is generally believed, be attracted to such activities, and consequently fewer solutions

1 Reuters Professor of Intellectual Property & Information Technology Law, University of Oxford; Director, Oxford Intellectual Property Research Centre, St Peter’s College, Oxford. An earlier version of this paper was written in the context of a wider project on patentability in the light of current technological innovation (‘La brevetabilité face à l’innovation technique contemporaine’), directed by Professor Michel Vivant at the Université de Montpellier, France. An updated version similar to this one was published in Peter Mirfield & Roger Smith (eds.), Essays for Colin Tapper (Lexis/Nexis, 2003), 182.
would be sought or discovered. A lower rate of social progress and less social well-being would ensue – at least, so the standard story goes.\(^2\)

The beneficial results for which society rewards such researchers with a patent are called inventions. The important question is, of course, what results should be so classified. Anything outside that category will not be patentable and so will fall into the public domain once it is marketed or becomes otherwise publicly available. The product or process can then be freely copied (or independently created) without tribute to the patent holder – at least, unless some other intellectual property or unfair competition law, or binding obligation of confidentiality, intervenes.

The question of what subject-matter falls under the concept of invention can be conveniently separated from other qualities the invention must have. Analytically, this proposition exemplifies the familiar Aristotelian dichotomy between essence/kind on the one hand, and attributes/quality on the other, also reflected in other intellectual property laws. Thus, in copyright law, what qualifies as an artistic work (its ‘essence’ or ‘kind’) is analytically distinct from the question whether the work is ‘original’ or not (its ‘attribute’ or ‘quality’). Similarly, in patent law, what qualifies as an invention – the ‘subject-matter’ of the grant – is distinguishable from other criteria of patentability, i.e., that the invention must be (1) new, (2) not obvious, (3) useful, and (4) adequately disclosed in the specification.\(^3\)

These preliminary observations bring us to the question: ‘what is an invention’?

2 The definition of invention

(a) **Who defines ‘invention’?**

‘Invention’ is not a self-defining concept. Etymologically, the modern verb ‘invent’ comes via Middle English from the Latin *invenire*, meaning to find or contrive. *Inventio* is the noun form. According to English language dictionaries, ‘to invent’ tends to be defined as to create by thought, to devise or originate (e.g., a new method or an instrument). ‘Invention’

---

2 How much activity is spurred by the patent system, and in what spheres, are empirical questions on which research is sparse and on which opinions accordingly differ. This study notes, but does not enter, that debate.

3 The distinction between kind and quality cannot be pressed too far. For example, one might fairly argue that novelty and non-obviousness are part of an invention’s essence. It is unnecessary to pursue that point here. Rather, we shall assume, safely, that the essence or quality of a thing is not established *a priori* but is the product of common social understandings and practices. Since it is universal practice and understanding (including within the European Patent Office and its boards of appeal) to treat the elements of novelty, non-obviousness, utility and adequate disclosure separately from the element of subject-matter, that convention will be followed here.

287
correspondingly means ‘thing invented’, and is often accompanied by the
further explanation: ‘especially something for which a patent is granted’.

Neither the etymology of the word ‘invention’ nor its modern usage
reveals the precise parameters of the concept – nor should we expect them
to, for the notion of invention is a legal term of art. It is defined by
legislatures, and the legislative definitions are interpreted according to
legal criteria by courts, tribunals and officials such as patent examiners and
patent office appeal boards. Like other terms of art, the definition and
interpretative contours of ‘invention’ are not immutable: they have
changed over time and have often differed – and may still differ, at least
marginally – among jurisdictions. The term of art meaning of ‘invention’
has naturally affected, and continues to affect, the concept’s popular
meaning, but popular meaning cannot determine the meaning of a legal
term of art.

It is entirely proper for ‘invention’ to be considered as a legal term of art,
for the purposes of the patent law. In that way, its definition may be shaped
by the policies espoused from time to time by the patent legislation as
interpreted by courts and tribunals. The difficulty is that invention is
something which, by its nature, cannot be fully known or defined in
advance. The concept is dynamic, not static. Were the same legislators who
voted for a piece of patent legislation 20 years ago now faced with the
question whether or not a newly emergent technology should be patented,
their views might very well differ today from those they may have held 20
years ago. Of course, their world view may have progressed meanwhile. But,
just as likely, the new technology may present them with issues which were
barely perceptible or not conceived of at all earlier.

This truism is evident worldwide from recent disputes about whether any
and, if so, which biotechnologies should be patented. Part of the dispute
revolved around the ontology and teleology of ‘invention’: for the
purposes of the patent law, can some or all of the products of genetic
engineering properly be classed as ‘inventions’ rather than ‘discoveries’?
But the perhaps more important part of the debate has been deontolog-
ical: ought this result, patentable in law, be patentable in fact? As
importantly, who decides?

Currently such decisions are made by patent offices, patent office appeal
boards, and courts. Legislators may become involved, but a long period of
uncertainty often ensues as they debate the issues and their involvement
ceases once the legislation is passed. The result may not prove particularly
satisfactory and may need to be revisited: the technology or public opinion
may have shifted even during the period of the legislators’ debate. The
legislation may well look obsolete as soon as it is passed; but thereafter
patentability is treated as a technical question for specialists in patent law.
The public has no continuing input on the point. Moreover, once the
specialists have interpreted the legislation to encompass a new technology,
it proves hard to go back. The courts rarely ‘disrupt the settled expectations
of the inventing community’ by reducing extensions to patent scope4; nor will legislatures.

Public input here is critical if the patent system is to command public respect. Patenting is not just a matter between a particular industry (or industry in general) and the patent office, nor even between an industry and the government ministries responsible for patents and innovation policy. How to provide such input is an issue which will be considered in the concluding section of this paper.

(b) International usage
The legal definition of invention is not left solely to the discretion of national legislatures or of supranational law-making institutions such as those of the European Union.

(i) TRIPs and ‘invention’
Since 1994, ‘invention’ has acquired an international dimension through article 27.1 of the TRIPs Agreement.5 That provision requires member states of the World Trade Organization (‘WTO’) to make patents available ‘for any inventions, whether products or processes, in all fields of technology’, if they are ‘new, involve an inventive step and are capable of industrial application.’ The proposed European Patent Convention of 2000 (‘proposed EPC’) virtually repeats this definition, with the immaterial substitution of ‘susceptible’ for ‘capable’.6 The same article of TRIPs emphasises that patents should be available ‘without discrimination . . . as to the field of technology’.

The TRIPs language reveals little else about what qualifies or should qualify as an ‘invention’. The phrase in article 27.1 – ‘any inventions, whether products or processes’ – includes the main examples of invention, seemingly without attempting to be exhaustive. European patent law has long treated both products and processes as patentable, and this position undoubtedly will continue under the proposed EPC.7 Similarly, inventions must fall within a field of ‘technology’ but this advances thought very little: ‘technology’ as a concept seems as elusive as ‘invention’. The main idea behind including ‘all fields of technology’ in the TRIPs language is to prevent states from excluding any area of human endeavour – e.g.,

---

4 Festo Corp. v Shoketsu Kinzoku Kogyo Kabushiki Co. Ltd. 122 S. Ct. 1831, 1841 (2002), rejecting a rule of patent interpretation which had been proposed by the lower court for the sake of greater certainty, but which reduced the breadth of patent claims.
5 i.e., Agreement on Trade-Related Aspects of Intellectual Property Rights (‘TRIPs’), annexed to the World Trade Organization Agreement 1994 (‘WTO Agreement’).
6 Proposed EPC, art. 52(1). This version of the EPC, rather than the EPC 1973, is often referred to in this paper on the basis that it is likely to be adopted in the near future.
7 Neither the present nor the proposed EPC refers explicitly to ‘products or processes’ but the omission is unimportant. To have expressly included the TRIPs language in the proposed EPC would have been not only tautologous, but may also have cast doubt on previously well-established European jurisprudence.
agriculture or medicine – from patentability for national sectoral public policy or economic reasons. What constitutes the outer limits of ‘technology’ is left open for discussion or interpretation.

(ii) TRIPs and exceptions to patentability

The obligation under TRIPs article 27.1 is qualified in three ways:

(A) Public order exceptions

First, TRIPs recognises that states may wish to discourage certain activities because of their perceived adverse social consequences. It may seem inconsistent, on the one hand, to discourage such matters by a state’s social laws while, on the other, encouraging new forms or means of producing or exploiting them by offering the opportunity of reward through the patent law. TRIPs article 27.2 therefore allows states to exclude certain inventions from patentability, namely, those

the prevention within their territory of the commercial exploitation of which is necessary to protect ordre public or morality, including to protect human, animal or plant life or health or to avoid serious prejudice to the environment, provided that such exclusion is not made merely because the exploitation is prohibited by their law.

This provision reflects a similar provision in the present and proposed EPC, but is not always present or explicit in other laws.

(B) Social or ethical exceptions

Secondly, TRIPs recognises that states have historically excluded certain categories of things from patentability for a variety of social or ethical reasons. States may wish to continue these exclusions until a different social or ethical consensus emerges in their territory. Article 27.3 accordingly provides a closed list of permitted exclusions: diagnostic, therapeutic and surgical methods for treating humans or animals; plants and animals other than micro-organisms; and essentially biological processes for the production of plants or animals.

The reasons for excluding these items are not always the same. One may infer that the items are all capable of being classified as ‘inventions’ but that some other reason may dictate their exclusion. Thus, the present EPC excludes medical and diagnostic treatments because these are considered not to be ‘inventions which are susceptible of industrial application’. In other words, a new treatment may involve invention but surgery, diagnosis and the like are professional individual skills that are, or should, not be ‘susceptible of industrial application.’

8 Proposed EPC, art. 53(a). Art. 53(a) omits the inclusory examples found in TRIPs art. 27.2, again essentially for the reasons mentioned in the previous footnote.
The proposed EPC continues the exclusion, but this time without providing any specific reason\(^9\) – as is permissible, since TRIPs lets states choose how to implement its provisions.\(^10\) The proposed EPC does confirm the patentability of ‘products, in particular substances or compositions, for use in any of these methods’,\(^11\) i.e., the current European practice (sometimes followed outside Europe) of allowing Swiss-type claims for new or old substances for use in medical treatment where the inventiveness lies in their particular medical application.

Other states apply the TRIPs medical treatment exception in different ways. Thus, in Canada, surgical treatment is not specifically excluded from patentability but Canadian courts have interpreted ‘invention’ in the Canadian Patent Act to apply only to inventions in the field of trade and industry, not for professional skills. Such skills are to be exercised in the interests of a particular client or patient and not traded as a commodity. Thus, advocacy is among the skills that are unpatentable: ‘a barrister who has devised a particular method of cross-examination [cannot] obtain a monopoly thereof so as to require imitators or followers of his methods to obtain a licence from him.’\(^12\)

‘Cannot’ in this quotation imports a legal decision, but one partly influenced by a mixture of ethical and public policy reasons. These include the fact that professionals, often already benefiting from a state-granted monopoly to practise their skills for the public benefit, should not seek to enclose their skills through monopoly or other means, but should rather share them as widely as possible for the public benefit. Professionals, moreover, do not need the spur of a patent to do their best for their clients; professional codes of conduct require that of them in any event. Nor should they be prevented by a patent from acting in the best interests of the client or patient – particularly important when life-saving surgery is being undertaken.

(C) Plants and seeds

Thirdly, TRIPs article 27.3(b) lets WTO members choose how they wish to protect plant varieties: ‘either by patents or by an effective sui generis system or by any combination thereof’. The provision reflects the fact that many states have passed plant breeders’ rights legislation pursuant to a version of the international plant variety protection treaty, UPOV. Article 27.3(b) does not mandate UPOV-style legislation: any sui generis system that protects plant varieties effectively in a non-discriminatory way suffices under TRIPs.

\(^9\) EPC, art.51(4); proposed EPC, art. 53(c).

\(^{10}\) TRIPS, art. 1.1: ‘... Members shall be free to determine the appropriate method of implementing the provisions of this Agreement within their own legal system and practice.’

\(^{11}\) Proposed EPC, art. 53(c).

Developed states may let plant breeders acquire patent and plant breeder rights cumulatively if they wish, so long as the product may be described in a way that falls within the subject-matter definition of both statutes. Alternatively, they may (as in the EU) allow partial cumulation: a patent if the technology applies to more than one variety, a plant breeder right where the technology produces only a single new variety of plant.

More recently, the TRIPs review at Doha, Qatar, in November 2001 produced a ministerial declaration requiring a broader consideration of plant variety protection issues that would take into account the concerns relating to biodiversity and the protection of traditional knowledge and folklore particularly for developing countries.

(D) EPC exceptions not repeated in TRIPs

Exceptions in the present and proposed EPC, not mirrored specifically in TRIPs, are the following:

(a) discoveries, scientific theories and mathematical methods;
(b) aesthetic creations;
(c) schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers;
(d) presentations of information ... only to the extent to which a European patent application or European patent relates to such subject-matter or activities as such.

These things may presumably be excluded, consistently with TRIPs article 27.1, as being neither ‘inventions’ nor concerned with some ‘field of technology’. Whether business methods and computer programs, now patentable in the United States, may properly be excluded under the EPC for such reasons is a question currently under debate.

(c) Teleology of ‘invention’

Historically, the concept of invention has been inextricably tied to the purpose of the patent legislation as it has developed and been perceived over time.

---

16 Taken from articles 52(2) & (3) as amended by the proposed EPC 2000.
DAVID VEVER

(i) Old UK law: ‘any manner of new manufacture’

In 1624, the English parliament passed the Statute of Monopolies to curb profligacy in the exercise of the royal power in granting monopolies. An exception was, however, made by section 6 of the Statute for 14-year grants of the sole working or making of any manner of new manufactures within the realm, to the true and first inventor and inventors of such manufactures, which others at the time of making such letters patent and grant shall not use, so as also they be not contrary to the law nor mischievous to the state, by raising prices of commodities at home, or hurt of trade, or generally inconvenient . . .

This language of ‘any manner of new manufactures’ remained part of the British patent law as a de facto definition of invention until the United Kingdom enacted the Patent Act 1977 to implement the EPC of 1973. We may note that, right from the start, British patent legislation accepted that not all manufactures were thought worthy of patenting. Those that were ‘mischievous to the state’ in the three stipulated ways, including broadly being ‘generally inconvenient’, would not be patented.

(ii) Other countries continue old UK law

Even today, some countries maintain the 1624 formula. Australia’s completely remodelled and revamped Patent Act 1990 provides that ‘invention’ means ‘any manner of new manufacture the subject of letters patent and grant of privilege within section 6 of the Statute of Monopolies . . .’ Australia’s deliberate retention of a formula introduced in its early days as a British colony reflects its relative satisfaction with the way in which the courts had treated the term over the years.

The leading Australian decision is that of its High Court in 1959. The Court unanimously reversed the Patent Office’s refusal to accept claims for a method of deploying a known chemical for a new use as a selective herbicide. The Court held that it was wrong to conduct, as the Patent Office had, a purely linguistic analysis into whether or not the claimed method was a ‘manner of manufacture’. The Office should have delved ‘not into the meaning of the word[s] so much as into the breadth of the concept which the law has developed by its consideration of the text and purpose of the Statute of Monopolies.’ In a much quoted passage, the Court observed:

The purpose of s. 6 [of the Statute of Monopolies], it must be remembered, was to allow the use of the prerogative to encourage national development in a field which already, in 1623,17 was seen to be excitingly

17 1623 was the year when the bill which led to the passage of the Statute of Monopolies was introduced; 1624 was when it passed. – My comment.
unpredictable. To attempt to place upon the idea the fetters of an exact verbal formula could never have been sound. It would be unsound to the point of folly to attempt to do so now, when science has made such advances that the concrete applications of the notion which were familiar in 1623 can be seen to provide only the more obvious, not to say the more primitive, illustrations of the broad sweep of the concept.18

Since then, the Australian courts have accepted that computer programs, methods of medical treatment, and possibly even business methods may qualify as patentable subject-matter.19 At one time, patenting any of these inventions might have been considered ‘generally inconvenient’. The New Zealand Court of Appeal thought this to be so for medical treatment, which, after a full review of the Commonwealth jurisprudence, it held to be unpatentable in 1982.20 More recently, Australian courts have taken a different view, holding that it is not ‘generally inconvenient’ to patent medical treatments.21

The recent trend, both in Australia and New Zealand, is to read this exception narrowly.22 In short, the courts themselves now find the qualification itself to be generally inconvenient. Previously, Australian and New Zealand courts tended to retain judicially created exceptions to patentability, saying that any change to long-established exceptions should be made only by Parliament. The contrary presumption now seems more prevalent: the courts can and do eliminate exceptions for which they claim to see no justification, saying that Parliament can always correct them if they are wrong.23
(iii) **US and Canadian definitions of ‘invention’**

United States courts and the US patent office have similarly taken the view that ‘anything under the sun that is made by man’\(^{24}\) is patentable. The case in which that somewhat hyperbolic statement (from the *travaux préparatoires* of the 1952 US patent amendments) was approved involved the grant of a patent for a genetically modified bacterium which degraded fuel oil.\(^{25}\) Computer programs, business methods and genetically modified animals (excluding humans) have progressively been swept within the language of ‘anything under the sun that is made by man’. This process has occurred even though the wording of the US patent law, in this respect little changed from the early 19th century, is rather different. The US *Patent Act* allows inventors to patent only ‘any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof’.

Canada has a provision similar to that of the United States, except that the US wording, with the addition of ‘art’, appears as a definition of ‘invention’ in the Canadian *Patent Act*:

‘invention’ means any new and useful art, process, machine, manufacture or composition of matter, or any new and useful improvement in any art, process, machine, manufacture or composition of matter.

Canadian courts have, however, until very recently, been more reluctant than their US counterparts to allow patenting particularly for more contentious new technologies. Thus, computer programs, computerized business methods, cross-bred plants, and methods of medical treatment have not been accepted as falling within the definition of invention.\(^{26}\)

Signs of change seemed possible when a majority of the Canadian federal Court of Appeal in 2000 allowed the Harvard onco-mouse to be patented. Indeed – contrary to the European Patent Office’s 2001 decision in opposition proceedings on the corresponding European patent – the court allowed the claims to covers all transgenic non-human mammals and all oncogenes, even though the disclosure related only to a mouse and one class of oncogene. But the Canadian Supreme Court, in a 5:4 decision, reversed the Court of Appeal: it was for Parliament, not the courts, to extend the notion of invention to encompass higher life forms. The majority thought that the technology was categorically different from

\(^{24}\) The only exceptions are ‘laws of nature, natural phenomena, and abstract ideas’: *Diamond v Diehr* 450 U.S. 175, 185 (1981).


3 Different approaches to patentability

It is useful to compare the United States and European approaches to deciding whether or not an invention is patentable as a prelude to considering the difficulties arising from each approach and possible reforms. The US approach embodies one end of the spectrum; the European is towards the other. The operation of these two approaches may then be conveniently considered by reference to two technologies: genetically modified animals and business methods.

(a) Current differences between US and European approaches

The United States patent system, in accepting that anything under the sun that is made by man is patentable, firmly takes the view that any advance, good or bad, deserves the reward of a patent. The patent system is there to grant property rights. Property is thought to be good in itself and therefore deserving of encouragement: the more property there is, the greater the incentive to use and profit from it, and the better off society will be as a whole (ignoring distributive effects – which is to ignore a lot). Under this conception, the grant of property is sharply distinguished from its use. Just as a gun can be used for good or ill, so may a property right. Just as any quantity of guns can freely be made, so may any quantity of patents be created. Just as it is the job of other laws – tort or criminal law – to regulate the use of guns, so it is the job of such other laws – including competition law – to regulate the use of patent rights.

Patent law in Europe has developed differently. Patents are indeed property rights but their grant is not automatic. Technology may be good or bad; if bad, it should be discouraged at the earliest point. Certainly, there should be no incentive to develop anti-social technologies by offering the prospect of a patent, or indeed any other privilege or subsidy.

The European sentiment is deeply-rooted. In the UK, patents started off as monopolistic privileges that were granted at the discretion of the

---

28 The Australian-New Zealand approach, with its broad exception for ‘generally inconvenient’ inventions, ought theoretically to be at the complete opposite end of the spectrum, compared to the United States. However, as has been noted, this exception is little applied today, partly under the influence of TRIPs art. 27.
monarch. They were not available as of right. That view prevailed in its strongest form before the passage of the Statute of Monopolies in 1624. Battles in the 17th century before the courts and in Parliament led to curbs, contained in that Statute, on both the type of monopoly granted and also the circumstances in which that type could be legitimately refused. Patents thenceforth could be granted by the Crown for, inter alia, manners of new manufacture but only if the patent would not, in the words of the Statute, be ‘mischievous to the state by raising prices of commodities at home, or hurt of trade, or generally inconvenient.’

The first and second of these grounds were probably always thought of as window-dressing: monopolies inevitably raised prices and, by suppressing competition, hurt someone’s trade. The third was potentially more significant. It signalled that the decision to patent could take into account contemporary economic and social policies. In the 16th century, for example, the social disorder which high unemployment might bring was widely feared; it was therefore deemed ‘inconvenient’ to patent machines that would throw workers out of jobs. This view fell into desuetude: progress, not employment, was a right; social disorder could be repressed in progress’s name. The proviso in the Statute was reinterpreted with the times, without completely losing force. Thus, in the 20th century, as noted earlier, the question whether medical or surgical treatments can be patented has been decided partly by reference to whether patenting them would be ‘generally inconvenient.’

The current references in European law, reflected in TRIPs, to refusing patents where the exploitation of an invention would be ‘contrary to ordre public or morality’29, continue to emphasise that patenting is not a morally neutral act. Patents may no longer be refused in the state’s general discretion, nor are the EPC/TRIPs grounds potentially as wide as the old ‘generally inconvenient’ ground. Nevertheless, as Cornish puts it: ‘The state, as granting authority, cannot disclaim responsibility for the inventions for which it grants protection.’30 Inventors can claim no natural right to benefit from immoral or socially disruptive activity, however ingenious.

(b) Patenting animals

The differences between the United States and Europe are well exemplified in the case of the Harvard onco-mouse. When the application to patent this genetically engineered animal came before the EPO, the EPO explicitly weighed the benefits and burdens of patenting the animal to determine whether the grant would be against ordre public or morality.31

29 Present and proposed EPC, art. 53(a).
INVENTION IN PATENT LAW

The reasoning used by the EPO to decide in favour of patentability may not be to everyone’s inclination, but at least the morality of exploiting animals as research tools to improve the quality of human life was considered – and will continue similarly to be considered under the EU Biotechnological Inventions directive.\(^{32}\)

In the United States, on the other hand, once a man-made bacterium was accepted as a ‘manufacture’ even though it was a living thing, the patenting of man-made multicellular life forms (excluding, supposedly for constitutional reasons, humans) seemed to follow inexorably.\(^{33}\) The US Supreme Court said that courts deciding issues of patentability had no mandate to weigh the potential hazards involved in genetic engineering, including such risks as that ‘its practice may tend to depreciate the value of human life.’\(^{34}\) The US patenting of the Harvard onco-mouse in 1988 was thus treated as a relatively routine matter.

This is not to say that the EPC ‘ordre public and morality’ exception operates satisfactorily. It does not. Patent examiners and the technical boards of appeal which review their decisions are little equipped by training or inclination to give the exclusion much substance.\(^{35}\) A different body to deal with such matters is suggested below in the concluding section of this paper.

(c) Business methods

It is also instructive to look at a case where the patent application does not apparently raise any issue of *ordre public* or morality: the patenting of business methods.

Just five years ago, few people would have predicted that a new method of doing business method, whether computerised or not, might qualify as a patentable invention. Presumably, it was thought that such methods were more mental than technological, were in large enough supply without needing the incentive of a patent, and could unduly inhibit ordinary business competition.

But once the US Court of Appeals for the Federal Circuit directly admitted a computer program as patentable subject-matter (‘any new . . . machine’) in 1994,\(^{36}\) it was only a matter of time — *viz.*, 1998 — before it also admitted a computerised business method on the same basis and suggested

\(^{32}\) This 1998 directive (above note 14) continues the EPC’s *ordre public* or morality’ exception and explicitly deems various genetic engineering practices to be unpatentable under this head, including modifying an animal’s genetic identity if that is likely to cause it suffering without any substantial medical benefit to man or animal: art.6.2(d).


\(^{34}\) *Diamond v Chakrabarty*, above note 25.


\(^{36}\) *Re Alappat* 33 F.3d 1526 (Fed. Cir. in banc, 1994).
that an uncomputerised business method was equally admissible (‘any new ... process’). Australian courts took a similar line. Technically, both countries could act this way without fanfare because their courts treat potential constraints on patentable subject-matter as flowing from the language of their patent legislation and the prior judicial interpretations of it. In the US Patent Act, any subject-matter that is ‘any new and useful process, machine, manufacture or composition of matter, or any new and useful improvement thereof’ is patentable; in Australia, it is ‘any manner of new manufacture etc.’ tracking, as we have seen, the language of the old Statute of Monopolies. Neither country needs to follow the European preoccupation with finding a workable modus vivendi between patentability and exceptions to patentability – because (apart from a ban on patenting human beings) there are virtually no exceptions written into either Patent Act. US and Australian courts and their patent offices thus welcome virtually anything into the patent fold today.

It was not always so. The US patentability of a computerized method of running a machine remained in doubt until 1981 when the US Supreme Court (by a slender 5:4 majority) accepted it as ‘any new ... process’. It then took over a decade more for a new computer program as such to be accepted as a patentable machine, but thereafter only four more years for business methods to be similarly admitted. As previously noted, ‘anything under the sun that is made by man’ has become the paraphrastic rallying-cry of patentability in the US courts and patent office. The actual language of the Patent Act seems now relevant mainly when the scope of the invention is considered: a technical issue of how the claims are drafted and on what acts later may infringe the patent.

In Europe, the question seemed closed by the present and proposed EPC’s ban on patenting ‘methods for ... doing business [and] programs for computers ... as such’. An application claiming a computerised business method should therefore fail before the EPO on two grounds, not merely one. Such is the view taken in the UK, under which claims which are ‘in substance’ for a method of doing business or for a computer program must be rejected even though they ‘in form’ cover an apparatus programmed to execute a defined task. Under the UK approach, the exceptions are treated seriously as statements of legislative policy.

---

37 State Street Bank & Trust Co. v Signature Financial Group Inc. 149 F.3d 1369 (Fed. Cir. 1998).
38 See the pre-Alappat Australian decision in IBM in 1991, followed by Welcome, both above note 19.
40 EPC, art. 52(1)(c). Similarly proposed EPC, art. 52(2)(c).
41 Merrill Lynch’s Appn. [1989] R.P.C. 561 (C.A.). The UK Patent Office, faced with the apparent conflict between Controlling pension benefits and Merrill Lynch, initially followed Merrill Lynch in Pinto Global Services Ltd’s Appn. (April 6, 2001) and then threw in the towel in a Practice Notice issued on 24 April 2002: ‘inventions which involve a technical contribution will not be refused a patent merely because they relate to business methods and mental acts.’ How this practice will fare in the UK courts remains to be seen.
The EPO, on the other hand, seems to find the EPC’s exceptions to patentability embarrassing to its perceived task of rewarding inventiveness through the patent system, and seems willing to accept any superficially plausible theory to avoid them. Thus, a recent EPO board of appeal was willing to accept a claim for a programmed computer as a patentable invention, even though the computer was designed and used to execute a business method. In the board’s view, the computer, being a concrete apparatus, had the ‘technical character’ necessary for an invention. Since exceptions to patentability are interpreted narrowly, the finding that a piece of hardware is neither a method for doing business nor a program for a computer inexorably follows on the EPO’s reasoning. Thus, the EPC exceptions can be avoided simply by clever (though uninventive) drafting.43

This approach echoes that taken in the US since 1994 and in the UK pre-EPC.44 It assumes that patents, being property, should be encouraged and that disallowing them interferes with the right to acquire property. The use of property language here stultifies rather than advances clear thinking. An equally plausible, possibly preferable, approach is to say that it is as important not to patent anything on [the EPC’s list] as it is to patent things that are off it. On this approach, any doubts about whether or not a patent application claims a mere ‘discovery’ rather than a true ‘invention’ – something found in the natural order rather than man-made change to the natural order – should be resolved by dismissing the application. [The opposite approach assumes that] when in doubt, create and reinforce property; do not deny or cut it back.45

This heresy has not yet struck the European Commission. In February, 2002, it proposed a directive that admitted all computer-related inventions (except those for business methods) to patentability and that allowed both process and product claims for them. Since harmonization EU-style inevitably means harmonizing in favour of more protection, the Commission unsurprisingly preferred the approach taken by the EPO (endorsed by the German courts) over that taken by the UK courts. The usual flim-flam about legal certainty and more jobs for Europe was trotted out, with about as much conviction as for prior directives in the intellectual property field.46 One is reminded of the EC’s Copyright Term Directive, which extended the standard period of copyright protection by 20 years, to 70 years after the death of the author. The reasoning underpinning this

4 Some further trends

The foregoing discussion reveals that the form of wording used to signal what items are patentable inventions varies among states. Nevertheless what is or is not a patentable invention is today remarkably quite similar worldwide. Perhaps paradoxically, newly emerging activities with potential economic significance – e.g., business methods, genetic engineering, computer programs – are more readily classified as inventions in states whose legislation is couched in terms of 17th and 18th century concepts of invention, than in states using 20th and 21st century definitions such as those found in the present and proposed EPC.

(a) **International control of the meaning of ‘invention’**

International homogeneity is less surprising as a phenomenon today than it may have been even a decade ago. TRIPs has effectively imposed a worldwide standard under which the availability of patents for inventions in all fields of technology has become the norm. States may choose what exceptions to make from a short closed list. They may expand the range of items for which patents are granted – for example, to include discoveries or pure mathematical ideas – in which case, they must make such patents available on identical terms to other WTO states. They cannot, however, unilaterally add to the list of exceptions that TRIPs allows. Nor may they, through legislation or judicial decision, restrict the meaning of invention – at least, not for long. If another WTO member state complains, the WTO may, through its dispute resolution procedures, require the offender to discard any unacceptably narrow meaning of invention or any unacceptably broad interpretation of a permissible exception. WTO trade panels have found states in breach of other patent obligations under TRIPs (e.g., India, 1999; Canada, 2000) and would no doubt police with equal vigour attempts to avoid TRIPs obligations on patentable subject-matter.

(b) **Reduction of exceptions to patentability**

A further development that should be noted is the clear trend since TRIPs towards the progressive elimination of many, perhaps even all, exceptions from TRIPs article 27.1. Apart from the common tendency in human

---

47 TRIPs, art. 1.1: ‘...Members may, but shall not be obliged to, implement in their law more extensive protection than is required by this Agreement, provided that such protection does not contravene the provisions of this Agreement.’

48 TRIPs, art. 4.
affairs towards simplification and generalisation, two specific phenomena contribute to this trend.

(i) **Bilateral ‘TRIPs-plus’ treaties**
First, the United States has embarked on a programme of bilateral negotiations, particularly with developing countries, under which the contracting parties undertake obligations beyond those required by TRIPs – so-called ‘TRIPs-plus’ treaties. Thus, the *US-Jordan Free Trade Agreement* of 2000 eliminates all the exceptions mentioned in TRIPs article 27.3(b), imposes UPOV obligations for plant variety protection, and commits Jordan to granting patents for business methods and computer-related inventions by ensuring that these items are not caught by the ‘mathematical methods’ exception in Jordan’s patent law.\(^{49}\) The EC is also not immune from this form of bilateralism in its dealings with non-EC states.

Treaties such as the *US-Jordan Free Trade Agreement*, while nominally bilateral, have multilateral effects because TRIPs requires any advantage extended by one WTO member to another to be extended to all.\(^{50}\) States that are bound to extend special advantages to others may fairly demand reciprocal treatment from them. Moreover, the more bilateral agreements impose obligations on states to grant patents for, say, business methods, the more likely it is that a WTO panel may interpret TRIPs itself as requiring business methods to be treated as an ‘invention’ and a ‘technology’: state practice may ‘clarify’ the meaning of TRIPs art. 27.1. A nominally bilateral obligation may thus become quickly multilateral in practice, and gradually universal in tendency.

(ii) **Common law trend towards more patenting**
Secondly, common law courts have shown themselves willing to follow the trend towards wider patentability spearheaded by United States courts and the European Patent Office. It is not surprising that European (including UK) courts have followed the EPO’s lead, given the pressure towards harmonisation exercised by the EPC and the centrality of the EPO in the EPC’s scheme. Less inevitable has been the trend of common law courts in jurisdictions such as Canada, Australia and New Zealand to reverse or whittle away at long-standing exceptions to patentability created by earlier courts in interpreting their respective patent statutes. The recent allowance of a patent in Australia for computer programs and medical treatment, and in New Zealand for Swiss-type claims covering the use of

---

\(^{49}\) Agreement Between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Area, art. 4.18; Agreement Between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Area, art. 5. Both documents were signed on October 24, 2000, and took effect on December 17, 2001.

\(^{50}\) TRIPs, art. 4, so-called ‘most-favoured-nation treatment’.
known compounds to produce pharmaceuticals for medical treatment,\footnote{See notes 25, 19 \& 21 above; \textit{Pharmaceutical Management Agency Ltd \textit{v} Commissioner of Patents,} above note 22, deliberately avoiding the medical treatment exception affirmed in \textit{Wellcome Trust} case, above note 20. } are examples of this phenomenon. In each case, the courts followed United States or European developments, ostensibly in the desire to keep their innovation policy up-to-date and not to let their country feel left behind in the technological race.\footnote{Such moves may prompt civilian lawyers to reconsider their preconceptions of what precedent and \textit{stare decisis} mean in practice in modern common law jurisdictions.}  

\begin{enumerate}[\textit{c}]  
\item \textbf{Cumulative protection} 
\end{enumerate}  

As intellectual property rights have proliferated and expanded, instances of multiple intellectual property protection have increased.\footnote{See the US and Canadian cases cited in note 13 above. Thus, in \textit{Monsanto Canada Inc. \textit{v} Schmeiser,} above note 13, the court enforced a patent for genetically modified seed against a farmer who had saved seed, holding that the exemptions for saving seed under the \textit{Plant Breeders Rights Act} was irrelevant to a patent infringement action. } For example, a firm’s logo may be registered or protected at common law as a trademark, a textile pattern may be registered as an industrial design, a computer program can be protected by a patent; yet copyright protection for all three is often cumulatively available. Patent and design right holders also strive to create trademark rights over aspects of their product and so to lessen free competition on expiry of the patent or design registration. As noted earlier, in some jurisdictions plant breeders may acquire both patents and plant breeder rights over their new seeds and enforce the rights cumulatively, thereby circumventing any inconvenient user exemptions found in one Act but not the other.\footnote{Proposed \textit{EPC,} art. 52(2)(b) \& (c).}  

Sometimes intellectual property legislation itself partly discourages multiple protection. Thus, the \textit{EPC} excepts, \textit{inter alia,} aesthetic creations and computer programs ‘as such’ from cumulative patent protection, largely because these items are adequately protected by copyright automatically without any formality or registration.\footnote{This section draws on Vaver, \textit{Copyright Law} (Irwin Law, Toronto: 2000), pp. 16–18. } Yet, as earlier noted, the EPO has undercut the full force of the computer program exception by interpreting it narrowly and has allowed patents for a wide range of computer programs. A copier may therefore be liable for either or both patent and copyright infringement as a rightholder decides. Indeed, the rights may be transferred and held by different entities, subjecting the copier to double liability and double damages.  

Intellectual property rights are here treated like products in a supermarket: a shopper with enough money and information can acquire as many items as she wishes. Innovation levels are hardly enhanced by the prospect of adventitious multiple protection. Whether the rule of ‘take as many as you can carry’ could be replaced by a rule of ‘only one per customer’ is
worth investigating further. If an ‘only one per customer’ rule were adopted, then seeking or obtaining a patent for a technology could bar reliance on any right which attaches without registration (e.g., copyright or common law trademark) and which substantially corresponds with the registered right, both during the pendency of the registration and also on its expiry.

Current common law jurisprudence shows some tendency in this direction, but the rule that cumulative protection may be obtained unless legislation positively forbids it is more prevalent.

One may also look at the matter from the patents end. Patents should be awarded to encourage desirable inventiveness. Therefore, where the activity is adequately encouraged and would occur even without the prospect of a patent, patenting is unjustified. This consideration suggests that the EPC exceptions to patentability for aesthetic creations, computer programs and presentations of information should be interpreted more broadly than they are now by the EPO. Indeed, a more general exception may be warranted to exclude all material that is susceptible of being adequately protected by copyright, database or design rights.

5 Reform suggestions

The foregoing discussion suggests a pressing need to reform the notion of patentable invention. The conflict between the UK courts and the EPO on how exclusions from patentability should be interpreted is serious and basic. The growing irrelevance of the ‘ordre public and morality’ exception, as applied by the EPO and national patent offices, is troublesome. The propensity of the EPO, in common with other patent offices, is to grant patents, not reject them; it is not institutionally equipped to make judgments on whether, in the public interest, a patent should be issued or continued. The point is tentatively recognized in article 7 of the EU Biotechnological Inventions directive, which states neutrally – without imposing any obligation on the EPO or national patent offices – that the EC’s European Group on Ethics in Science and Technology ‘evaluates all ethical aspects of biotechnology.’ Other jurisdictions also implicitly recognize that intellectual property offices do not necessarily possess

56 E.g., TrafFix Devices Inc. v Marketing Displays Inc. 120 S. Ct. 2715 (2001), barring trade dress protection for a functional design feature covered by the claims of an expired patent.


58 Above note 14.
in institutional competence to deal with broader public policy issues. With growing public concern about new technologies and the pace of their introduction and dissemination; it is increasingly important for the public to be involved on an operational level in the grant of patents and not merely to be consigned to a sideline role.

Patents should work manifestly in the public benefit – the ultimate justification for the system. The public pays a high price for patents. It must get, and be convinced that it is getting, correspondingly high value from it. Greater public involvement and hence understanding would help attain this goal. Without such involvement, the system may not muster the public support it needs to survive.

Public input, to be meaningful, requires a broader ability than currently exists to decide on which inventions deserve a patent. The old idea of patenting as a privilege rather than a right has much to commend it. The idea lost currency through being too intermeshed with royal patronage and, later, bureaucratic discretion. But these objections would lose force if the body that granted patents were more representative of the public, and if the grounds for grant or rejection were more firmly linked to the perceived benefits the invention would potentially confer on the public. In short, a ‘generally inconvenient’ invention should not be patented, but the question of general inconvenience should be resolved by a more widely representative body than one comprising merely lawyers or technical experts.

The following suggestions, focussing on the European system but easily adaptable (at least in theory) to other systems, are therefore proffered for consideration:

1. The European practice of not defining ‘invention’ in legislation is sound.
2. The practice of excluding firm categories of items is unsound except for categories that, on any view, fall outside the concept of ‘invention’. So ‘discoveries . . . as such’ may reasonably continue to be excluded, because any decision to expand the patent legislation to include discoveries is a major structural decision – akin to the

---

59 Consider, e.g., the Trade Marks Bill introduced into the New Zealand Parliament in 2001. In the Bill as reported out of Committee on March 1, 2002, the Commissioner of Trade Marks must reject an application if he ‘considers that, on reasonable grounds, its use or registration would be likely to offend a significant section of the community, including Maori’: Bill, s. 17(1) (b) (ii). A committee will advise the Commissioner on such issues. Originally, the advisory committee’s role was limited to advising whether a registration ‘that is, or appears to be, derivative of Maori imagery or text is, or is likely to be, offensive to Maori’, but this clause was struck out during Committee consideration of the bill. The new committee would have a general advisory role on all matters: Bill, s. 178. Presumably the Commissioner may accept or reject the committee’s advice. Adverse advice would constitute ‘reasonable grounds’ on which the Commissioner could refuse registration under s. 17(1) (b) (ii) of the Bill.

60 The suggestions take no account of political or other possible obstacles to implementation such as those presented by international conventions, e.g., TRIPs or the EPC.
decision to establish a *sui generis* database right – that would require legislation. The line between discovery and invention would still need to be continually policed and clarified.

3. The EPO practice of construing patentability exceptions narrowly and allowing their avoidance through simple drafting means is unsound. The UK practice of treating the exceptions as embodying expressions of substantive policy is preferable.

4. A technology should not be protected under more than one intellectual property law. Thus, if the technology is protectable by copyright, no patent should be awarded. All plant technologies should be protected under more precisely targeted plant breeder laws, rather than by patents.

5. The decision to award or refuse a patent requires greater flexibility than presently exists. Unforeseen technologies and issues may require broader consideration than technically-oriented patent examiners are equipped to give them. Therefore the legislation should be amended to exclude inventions that it would not be in the public interest to patent – in effect, a return to the principle of excluding ‘generally inconvenient’ patents, but one where the issue of ‘convenience’ or ‘public interest’ is seriously weighed and considered. Inventions could be excluded by categories but, more importantly, there should also be a general discretion to exclude any particular invention whether or not it presently falls within a specific category.

6. Among the non-exhaustive reasons of public interest to exclude an invention might be that:
   (a) its production was already adequately encouraged (i.e., supply was sufficient);
   (b) it was already adequately protected under another intellectual property law or by the general law (e.g., by unfair competition or trade secret law);
   (c) its patenting would discourage biodiversity, contrary to the Convention on Biological Diversity 1990;
   (d) current ethical concerns rendered it, on balance, inadvisable to patent. This view could be modified from time to time to render patentable what currently is not, and unpatentable what currently is.

7. A special Ethics and Public Interest Panel should be established independently of the patent offices.\(^6\) The Panel would comprise both experts in law, ethics and technology, and also ordinary

---

\(^6\) This suggestion builds on one contained in the Westminster Institute for Ethics and Human Values & McGill Centre for Medicine, Ethics and Law, Ethical Issues Associated with the Patenting of Higher Life Forms, (London, Ont., 1994) at 103ff.
members of the public, with power to co-opt other persons (including experts) from time to time as it thought fit.

8. The Panel would:
   (a) decide what categories of inventions should not, in the public interest, be patentable;
   (b) add to or subtract from those categories from time to time;
   (c) exclude a particular invention in the Panel’s discretion;
   (d) issue advance rulings on potential patentability of particular new technologies, and repeal or amend those rulings from time to time;
   (e) decide issues of ordre public or morality – a subset of public interest – currently decided by the EPO and national courts;
   (f) advise the EPO and national patent offices on what categories of applications should be referred to the Panel. (An examiner could always refer any application to the Panel for its opinion, whether it fell within a stipulated category or not.);
   (g) request the referral of any application to it at any time;
   (h) revoke, after a hearing, any patent on the ground that its grant was against the public interest, or that its continued exploitation was against the public interest, ordre public or morality;
   (i) commission studies on any patent issue (including patentability) to assist it in its decision-making.

Charles de Gaulle is reputed to have said that politics were too serious a matter to be left to politicians. A similar sentiment holds true for patent law. It is too important to be turned over to the specialists, be they patent lawyers, patent judges, or even patent law professors. Patent laws are there for the whole of society. Not every member of the public may read patent laws or patents as avidly as they read literature, but they are nevertheless touched by those laws at least as significantly, whether they know it or not. They therefore deserve a greater role in the way patent laws operate than the laws currently allow them. The modest proposal of this essay is that the public be allowed that greater role.
Review Article


Review Article by DENIS N. MAGNUSSON

1 The Book

This book was published in 1999 in anticipation of the March 1, 2000 coming into force of the main provisions of the UK Competition Act, 1998. That Act has been described as ‘the most radical change ever to competition law in the U.K.’ It replaced UK competition law ‘complex to the point of being indecipherable’ which ‘ha[d] been regarded as an irrelevance by most small and medium sized businesses’. The book has not as yet reached a second edition.

The publishers present this book as a ‘readable [guide to] U.K. and E.C. competition law for non-competition law specialists’. The Foreword states that ‘[m]ore and more undertakings are adopting in-house procedures to ensure compliance with competition law’, implying that the anticipated non-specialist readership will include in-house business managers and legal advisers, as well as external legal advisors, who are not competition law specialists.

Of interest to readers of this Journal, the author’s Preface notes:

[A] strong emphasis has been placed on intellectual property agreements and the exploitation of intellectual property rights given the increased importance of intellectual property to businesses . . .

Paul M. Taylor is a seasoned specialist in the field. This book ought to

---

1 Professor Emeritus, Faculty of Law, Queen’s University, Kingston, Canada. Email: magnussdqsilver.queensu.ca.
3 Ibid.
have a wide readership, including specialists in competition law as well as non-specialists.5

Dual Competition Law Regimes
In his concise and helpful Ch. 1, Introduction, Taylor gives an overview of UK and EC competition law and demonstrates why all UK businesses must be alert to competition law issues. Taylor notes that ‘[t]he thrust of the 1998 Act is to introduce into the English law an absolute prohibition against a range of anti-competitive activities which affect trade within the United Kingdom’ [emphasis added]. Taylor also indicates that EC law will ‘continue, in parallel, to prohibit anti-competitive activities which affect trade between Member States of the Community.’ He further explains that UK business leaders and legal advisers are saved from having to master two divergent systems of competition law by Parliament’s modeling of the 1998 Act on EC competition law, strengthened by the explicit direction of s. 60 of the 1998 Act that regulators and interpreters of the Act are to treat:

questions arising under this [Act] in relation to competition within the United Kingdom ... in a manner which is consistent with the treatment of corresponding questions arising in Community law in relation to competition within the Community.

Extended Scope of the 1998 Competition Law: Information Technology
Industries
Prior to the 1998 Act, at least those businesses whose trade was confined largely to the UK may have been safely oblivious to the then ineffectual UK competition law. The new Act, Taylor maintains, ought to cause a radical shift in that attitude. Nevertheless, smaller UK businesses might still regard competition law as primarily a matter of concern to big business. Taylor’s book explains why this is a mistaken view.

The first of the two main categories of competition law regulation applies to ‘a broad range of agreements and concerted practices’, notes Taylor. The prohibition in s. 2(1) of the 1998 Act applies to any agreements or concerted practices which ‘have as their object or effect the prevention, restriction or distortion of competition within the United Kingdom’. The interpretational limitation on this prohibition of most interest to smaller businesses is the requirement that the agreements or practices must have an ‘appreciable’ anti-competitive effect. EC interpretational guidelines

---

5 The syllabus for the University of Cambridge LLM. Competition Law paper includes this book as one of ten listed readings in the field. http://www.law.ac.uk/faculty-paper14.htm visited July 31, 2002.
indicate that horizontal restrictions affecting 5% of the Community market and vertical restrictions affecting 10% of the Community market are \textit{prima facie} of ‘appreciable’ effect. Office of Fair Trading (‘OFT’))\textsuperscript{6} guidelines provide that agreements or practices affecting 25% of the U.K market are \textit{prima facie} of ‘appreciable’ effect. However, the effective scope of the prohibition is even wider given the warning that some agreements or practices affecting smaller market shares may still be found to have an appreciable effect. Further, any agreement or practice which ‘directly or indirectly fixes prices or shares markets’ or ‘imposes minimum resale prices’ is generally regarded as having an appreciable effect regardless of market share, and so is absolutely prohibited.

Of particular relevance to readers in information technology businesses, Taylor devotes a very useful Ch. 9 to the application of this first category of competition law regulation to ‘Intellectual Property Agreements’, including patent and know-how licences, copyright licences, trade mark licences, joint ventures, and other R&D agreements.\textsuperscript{7} Taylor notes the somewhat anomalous position of intellectual property under EU competition law:

It is striking that the EC Treaty itself makes no mention of intellectual property other than in Article 36 which permits restrictions on free movement of goods if justified on the grounds of protection of ‘industrial and commercial property’. The principle of free movement of goods ostensibly conflicts with the national protection afforded to goods protected by intellectual property against ‘importation’ as an infringing act, and Article 30 \textit{[sic]} resolves the conflict. The interpretation of Article 36 has given rise to considerable case law from the E.C.J. to determine the extent to which intellectual property rights may be exempt from the free movement principle of Article 36.

Much the same can be said of the 1998 Act,\textsuperscript{8} in which the only express mention of intellectual property is the repeal by s. 60 of ss. 44 and 45 of the Patents Act, 1977, apparently on the ground that the Patents Act sections became redundant with the enactment of the Competition Act, 1998, despite the lack of other express references to patents or other intellectual property in the 1998 Act.\textsuperscript{9}

The second of the two main categories of competition law regulation prohibits abuses of competition by dominant firms. While this category is

\textsuperscript{6} The OFT Director General is chief regulator under the 1998 Act. See the OFT site: \texttt{http://www.oft.gov.uk/default.htm}. Click on ‘Business Information’ and then click on ‘Competition Act 1998’ under ‘More Business Information – Legal Powers’. The references and quotes which follow are to documents on this site. Visited 31 July, 2002.

\textsuperscript{7} This chapter should now be read in conjunction with the OFT document: \textit{Intellectual Property Rights: A draft Competition Act 1998 guideline}, November 2001.

\textsuperscript{8} In his Preface Taylor noted his inclusion of competition law application to intellectual property agreements and to the exploitation of intellectual property rights, ‘even though the new Act makes little reference to intellectual property’. Taylor, \textit{op. cit.}, p. vii.

primarily of concern to larger firms relative to the EC and UK markets for EC and UK law respectively, Taylor warns that dominance is defined in relation to a particular product market, and the potential for defining innovative new product technologies as individual markets may catch even smaller product innovator firms as dominant within such markets.10 Taylor devotes Ch. 4 of his book to ‘Definition of Relevant Market and Assessment of Market Share’. Of course, mere dominance in a market is not a competition law wrong, but a dominant firm must be alert as to whether any of its business practices might be seen as abusively anti-competitive.

Of further particular interest to readers of this Journal, and to the intellectual property engaged information technology businesses with which they are associated, this book includes a chapter on ‘Exhaustion of Intellectual Property Rights’.11 Taylor explains that the various national intellectual property laws provide for the point at which the further exercise under national law of an intellectual property right, by the owner of such right or by such owner’s agent, stopped. However, the national laws of the various EC states differ in defining this point, particularly in international contexts.

For example in the United Kingdom, once a patented product is sold, the purchaser could deal with it anywhere in the world subject only to restrictions of which the purchaser is given notice.12 … By contrast, many continental European countries (such as Germany) have resisted any concept of international exhaustion of patents, preferring instead to entitle the patentee to resist imports of products first sold outside their borders.13

EC member states’ laws which might restrict the movement of goods among member states became a matter for concern under Article 3(c) the EC Treaty, mandating the elimination of ‘obstacles to the free movement

10 Taylor, op. cit. p. 176. Since the prohibited agreements and practices under the first category of competition law regulation apply only in relation to their anti-competitive effect within a defined product market, the market definition jurisprudence has a similar broadening potential for the first category prohibition of anti-competitive agreements and practices in new technology markets.

11 Ch. 10.

12 Taylor cites Betts v Wilmott, [1870] L.R. 6 Ch. App. 239. Thus the purchaser in France of a patented product (tyres) from the business (Dunlop) who also happened to be the UK patentee, without notice of any restriction on the purchaser’s use of the product, is free of any finding of patent infringement under the UK patent with respect to importation into, and sale and use in the UK of such products.

13 Taylor, op. cit., pp. 188–189. Hypothetically, a purchaser of patented tyres in France from a seller, who happened to be the patentee in Germany, would not be free of infringement claims under the German patent if the purchaser exported the tyres to Germany for sale and use there. The motive for using intellectual property to control the movement of goods among different national markets is most often the intellectual property owner’s determination to exploit the profit maximization potential in price discriminating among the various markets. See, for example, the controversies over price differentials among EC states with respect to automobiles. European Parliament Fact Sheets, The automobile industry, http://www.europarl.eu.int/factsheets/4–7–4–en.htm, visited 31 July, 2002.
of goods...as between Member States'. Exhaustion jurisprudence has an EC competition law dimension when the owners of national intellectual property rights make agreements or adopt practices, shaped by the topography of the various national laws on exhaustion, with the purpose or effect of restricting the flow of intellectual property covered goods across EC state borders. A further EC competition law dimension would arise if a firm in a dominant market position sought to assert its national intellectual property rights to block the movement of intellectual property protected products across EC state borders.

2 A Useful Book: But Caution

This reviewer found that this book succeeded in the objectives set out by the publisher, Foreword and author’s preface. However, the intended users of this book should be cautioned about the limitations inherent in any such use of such a work.

The Foreword to the book may intimate that readers other than competition law specialists can readily dip into the book to deal with particular competition law compliance issues. The caution is that few, if any, such issues could be dealt with by consulting a few pages or even a whole chapter of this book. For example, an information technology firm manager wanting to check on the competition law status of a desired clause in a proposed agreement for licensing its technology would consult Ch. 9 'Intellectual Property Agreements'. However, that chapter cannot be properly understood without absorbing Ch 2, concerning the general competition law applicable to anti-competitive agreements. To be safe, it would be desirable also to scan Ch. 3 on potentially abusive practices of dominant firms. Of course Chs. 2 and 3 are not understood unless the law of market definition in Ch. 4 is understood. If the business is keen, as most businesses would be, to escape the application of the competition law to its agreement, it might often be necessary to review Chs. 8 (on the types of agreements given automatic block exemptions from the law’s prohibitions) and 9 (on agreements commonly eligible for specific exemption). As the purpose in such an exercise is to comply with the law, Ch. 15 on compliance programs, with its helpful questionnaire to guide the user in compliance efforts, ought also to be carefully read.

This reviewer does not suggest that the book’s objective is impractical, but only cautions that effective use of this tool will require some care and real effort. Indeed, with the adoption in 1998 of an effective competition

---

14 Under the first category of competition law regulation, see Article 85 (now 81) of the EC Treaty. For example, under UK law, the seller of patented tyres in France might do so under an agreement in which the purchaser accepted that nothing in such sale granted the French purchaser any immunity from being found to infringe under the UK patent should the purchaser cause those tyres to enter the UK market.

15 Under the second category of competition law regulation, see Article 86 (now 82) of the EC Treaty.
In April 1999 the OFT expressed concern about evidence it had gathered of the ‘low awareness of the new Competition Act’ among UK business people and announced an extensive program of education for business to address the problem. http://www.oft.uk/News/Press+Releases/1999PN+12–99htm.

Currently, the OFT has published 10 Information Leaflets ['basic guides to particular aspects of the Act'], 19 Guidelines and 3 draft Guidelines ['detailed guides as to how the OFT and sector regulators intend to enforce the Act']. The discussion draft form available to Taylor has since been modified and promulgated together with new Director’s rules indicating 'the procedures that the Director General of Fair Trading and the regulators will follow when taking a decision or giving guidance' Statutory Instrument 2000 No. 293. Further, a Lexis search for ‘Competition /1 Act /1 1998’ in the UK case law database showed a total of 18 reported decisions of the Competition Commission Appeal Tribunal and the trial and appellate courts interpreting the 1998 Act on 12 different case matters.

In considering consulting or purchasing this book, readers may question whether a book published 4 years ago, before the 1998 Act had even been finally enacted, might be substantially less useful in the light of intervening competition law developments. Subject to the limited cautions below, this reviewer believes this book is still a useful aid. At writing Taylor did have access to the text of the 1998 Act and to additional material such as a discussion draft of a key form under the Act, and to a final draft of the form for requesting regulator guidance on issues arising in the period of the transition from the old law to the 1998 Act. He also had access to drafts of at least some of the material produced by the OFT to guide business with respect to the new competition law. Most importantly, at writing Taylor had access to the body of EC competition law developed under Articles 85 and 86 of the Rome Treaty of 1958. That law is applicable to UK businesses engaged in trade among EC member states, and Taylor deals extensively with that law in this book. Further, the UK 1998 Act is based closely on that EC law which must be used in understanding the content and operation of the new UK law. While EC law has developed further in the three years from Taylor’s writing, that law is an ‘iceberg’. The law prior to Taylor’s publication in 1999 is the big part under water, the post-1999 developments are only the above-water tip of the ‘berg. Particularly for the book’s intended non-specialist in competition law readers, the fact that the book does not include the latest nuances of the law is not a fatal deficiency.

There are pending competition law reform projects affecting both the EC law and the UK law which may render the book somewhat less useful in

---

16 In April 1999 the OFT expressed concern about evidence it had gathered of the ‘low awareness of the new Competition Act’ among UK business people and announced an extensive program of education for business to address the problem. http://www.oft.uk/News/Press+Releases/1999PN+12–99htm.

17 Currently, the OFT has published 10 Information Leaflets ['basic guides to particular aspects of the Act'], 19 Guidelines and 3 draft Guidelines ['detailed guides as to how the OFT and sector regulators intend to enforce the Act']. The discussion draft form available to Taylor has since been modified and promulgated together with new Director’s rules indicating ‘the procedures that the Director General of Fair Trading and the regulators will follow when taking a decision or giving guidance’ Statutory Instrument 2000 No. 293. Further, a Lexis search for ‘Competition /1 Act /1 1998’ in the UK case law database showed a total of 18 reported decisions of the Competition Commission Appeal Tribunal and the trial and appellate courts interpreting the 1998 Act on 12 different case matters.

18 These articles have subsequently, though fairly recently, been renumbered 81 and 82. Taylor consciously decides to continue to refer to these articles as ‘85’ and ‘86’, Taylor, op. cit. p. 1. Consistently with Taylor’s usage, though with less justification, in this review those articles are referred to as 85 and 86, rather than 81 and 82.
the future. In September 2000 the European Competition Commission published a draft revised Regulation 17 which implements Articles 85 and 86 of the EC Treaty. The proposed changes are largely procedural, but are significant. Such changes would primarily affect the material in this book’s Ch. 6 ‘Notification, Exemption and Guidance’. Further, and of particular interest to intellectual property attuned information technology businesses, a European Competition Commission review appears to suggest immanent changes in the content of the Block Exemption of Transfer of Technology Agreements from competition law prohibitions.

Such changes could affect the material in this book’s Ch. 9 ‘Intellectual Property Agreements’. In March, 2002, the UK government introduced the Enterprise Bill into Parliament which makes some changes in UK competition law. The major competition law changes in the Enterprise Act affect merger law, an area of UK competition law that was not changed by the 1998 Act. Such changes will have had a substantial effect on the material in Ch. 11 of this book, ‘United Kingdom Monopoly and Merger Control’. Other Enterprise Act changes include introducing criminal sanctions (imprisonment) for ‘hard core’ cartels (cf. book Ch. 2 ‘Infringement by Coordination’) and facilitating private remedies for injury suffered through competition law violations.

3 A Rant

This reviewer has a final observation which, as he luxuriates in reading this Journal’s free copy of this work, will cast him as both hypocritical and ungrateful – but this is a work on competition law. I refer to what seems a too common practice of British law book publishers, including the publisher of this book. This book has 602 pages. Of these 602 pages, 262 pages, 43.5%, are composed of appendices of UK and EC statutes and regulations. This book’s intended readership of other than competition law specialists may justify the inclusion of this otherwise readily available material. That justification may have been even stronger in 1999, before the expanded access to statute and regulatory material on the Internet.

19 See http://www.dti.gov.uk/cp.eccompreform.htm. The changes would largely eliminate the present procedures for Commission administrative rulings in non-merger cases, and would expand the role of national courts in enforcing the EC competition law.

20 See http://europa.eu.int/comm./competition/antitrust/technology-transfer.


22 Taylor noted the unsatisfactory state of the law under the 1998 Act on private actions seeking compensation for injuries suffered by others competition law violations. Taylor, op. cit. p. 20.

23 Not counting 50 pages of Foreword, Preface, Table of Contents, Table of E.C. Cases, Table of E.C. Legislation, Table of United Kingdom Cases, Table of United Kingdom Statutes, Table of United Kingdom Statutory Instruments.

24 In competition law this practice is referred to as ‘tying’ – the purchaser must buy the unwanted product (statutes and regulations the buyer already owns or can get elsewhere much cheaper) as a condition of being able to purchase the wanted product, the text of the book.
Nevertheless, this reviewer stresses, perhaps for the publisher’s consideration with respect to a hoped-for revised edition of this useful book, that the appendices do make the book significantly bigger, somewhat costlier to produce, and may seem to justify a substantially higher price for a bigger book. This reviewer can testify that, particularly for would-be readers of British legal materials located outside the UK, this practice compounds the reduced accessibility of British legal materials created by the otherwise aggressive pricing policies of British law publishers.

---

25 The UK list price was £105 but it can be bought for £75 as of August 2003 on Amazon.co.uk. While this tactic is common to many legal publishers, this reviewer’s impression is that British publishers are especially fond of the tactic.

26 Where ‘aggressive’ does not mean ‘low’. Perhaps British publishers are determined to profit maximize in the UK market for which they assume a relatively inelastic demand curve – if you are a Briton with a local legal problem you must have the local law. This foreigner’s demand curve for British legal texts is quite elastic as is that of many of his colleagues. Certainly price gouging is not unknown among US and other countries’ legal publishers – especially in an era of much increased concentration in the market (cf. OFI, ‘The Market for Scientific Journals – Invitation to Comment’, 5 July, 2001, noting ‘the continual rise in prices of Scientific, Technical and Medical Journals’ at http://oft.gov.uk/News/Pressreleases/2001/PN+30–01.htm). However, in addition to often being better, US legal publications are often cheaper, even much cheaper, for foreigners (and Americans too). Understandably, whether Canadians and other foreigners have easier access to UK legal materials is a trivial matter for Britons. And the relative costs of legal materials is a small factor in the widespread and rapidly accelerating displacement of UK legal thought and precedent in, at least, Canadian legal education and practice. Perhaps I’m just musing on the obvious – the ubiquitousness of the present Empire and its utter vanquishing of the old empire, and the on relative efficacy of cheap literature over guns in legal cultural imperialism. Salve lex Americana!
Book Reviews


Review by MARK PERRY†

Whilst looking for a shared theme amongst these three works it struck me that perhaps the only commonality between them was the likely lack of enthusiasm from at least the academic readers of this journal for any of the books under review here. However, there are gems to be found by even the most theoretical of academics within these works. Each work also presented its own reviewer’s challenge of a practical nature, appositely for such practical books.

Rennie’s Computer and Internet Contracts and Law is the only work of the three that is directly aimed at legal practice. In addition to the editor, there are contributions by distinguished scholars from Europe, Japan, Australia and the United States. The 68 contracts in the looseleaf work (though curiously the Sweet and Maxwell site says there are 60) have been drafted ‘to reflect that universality which is the nature of the computer industry’. An introductory note prefaces each precedent, and within each precedent there are alternative wordings to reflect the requirements of Australia, Japan and the U.S.A. with footnotes mostly referencing other precedents. The introductory notes give explanation as to the use of the precedent following, and in the main they are useful and clear. Occasionally, such as in Precedent 10, the note reads like a complex clause in the precedent with one sentence exceeding 100 words, but this is a small gripe: if you intend to use the precedent you should follow the notes. The precedents are also supplied on floppy disk (a challenge to the non-Intel box user with no floppy drive) in WordPerfect format. The looseleaf also includes a short (a little over 100 pages) but dense commentary on Computer Program and

† Faculty of Law and Department of Computer Science, The University of Western Ontario.
Database Protection in the EU, USA, Japan and Australia, and the Internet and Electronic Commerce. The commentary is pithy and to the point, as to be expected in a practice oriented work. Following the commentary there are the sample contracts, divided into five main groupings, Software, Databases, Systems/Hardware, Miscellaneous Agreements (including disclaimers, consultancy, supply of software authors, non-disclosure, disclosure, copyright legends, evaluation, option, guaranty, beta testing, facilities management, and telecommunications agreements) and Internet. One omission noted in this revision was the lack of a privacy precedent in the reviewed release, and this brought attention to a small error. The index listing for Privacy refers the reader to E-51 in the commentary, where you will find discussion of WIPO and ICANN, whereas Privacy is discussed in E-55. Hopefully, later revisions avoid such irritations. Business method patents are promised for commentary discussion in Revision 8.

The floppy disk accompanying Computer and Internet Contracts and Law is unexceptional, but serves its purpose. It simply contains a compressed archive of the precedents in the looseleaf, that, when expanded, are WordPerfect files. This makes it much easier for the contract writer to 'tweak' any contract, in addition to simply entering the names of the parties or choosing the country specific wording. Ironically, the shrinkwrap licence agreement accompanying the floppy is different to the precedent example in the looseleaf, perhaps illustrative of the need for constructing different licences in different circumstances. A practice that deals extensively with the computer industry will no doubt have its own database of standard contracts covering many of the situations envisaged in the precedents. However, for those that are being drawn into this field, or those firms that wish to extend their precedent tool collection, Computer and Internet Contracts is a valuable resource.

The Harris book (Digital Property: Currency of the 21st Century) claims to be targeted at the 'businessperson, educator, librarian, writer, researcher, artist, publisher, investor, new media entrepreneur, or just someone who is fascinated with the digital world'. Such an audience was probably a lot larger in 1998, and less aware of intellectual property rights, than today post dot-bust.

Readers of this review who are interested in checking out Digital Property can see the first chapter at http://www.mcgrawhill.ca/digitalproperty/chapter1.html and get a feel for the style of the book. The author addresses her readers in a chatty, congenial style, reflecting the enthusiasm that powered the dot-com boom. There are many personal references, questions and even a quiz, reminiscent of the self-improvement genre of books. This may be comfortable for some readers, but for me became irksome after a while. This book is a fast read, not so much because you cannot put it down, but rather because it has large type and is typeset with plenty of space, which I consider a bonus. The book is festooned with pertinent, often chipper, quotes. One of my favourites, from Lord
Evershed, caught my eye on p.70, although it does seem to be a misquote. The quote, according to Megarry, *A Second Miscellany-at-Law* runs ‘This contract is so one-sided that I am astonished to find it written on both sides of the paper’. In *Digital Property* the word ‘astonished’ is replaced by ‘surprised’. It may be that the *Digital Property* quote is the more correct, or perhaps this is just a minor error. However, even if it is the only such error in the work, it is hard to establish authenticity of quotes, and for the interested reader without research experience it is difficult to follow up items that tweak interest with further reading, as the book lacks comprehensive references. My challenge was to track down a trustworthy reference to the quote in as little time as possible (it took a few minutes online to find one reference to a book that was not on shelf in the library, and another an hour amongst the stacks before checking out Megarry).

On a positive note, *Digital Property* is a book that, though an unlikely hit for readers of this journal, may make a nice gift as an introduction to the area of the rights surrounding digital materials. It is clearly written, and will bring to the fore issues surrounding intellectual property in the computer age for the neophyte. Perhaps for someone who has a stirring of interest in the area, or who needs a basic backgrounder on intellectual property issues surrounding digitally created materials. Even though dated by the dot-hype (in a mere four years), the key topics are as important as they ever were. For example, everyone should be aware that digital content is a different kettle of fish to content that is fixed on paper, or that the paradigm governing operation of the Internet has changed from inception, and so forth. Although clearly aimed at the layperson, curiously the work includes in Appendices the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty that may give most laypersons a headache. In short, if you know anyone who does not have a clue about intellectual property or any of the issues around digital materials, this is a book that most could read in a day or so.

For a complete change of pace, try Masterson’s looseleaf (*IT Policies & Procedures*), though you should be warned that this is again not a book directed towards lawyers. The target audience here is managers of the information technology sections of a business. *IT Policies* is very clearly organised into 10 chapters, covering the gamut of IT management areas from Planning the IT Infrastructure in chapter 1 to IT Support in chapter 10. The chapters between cover IT Quality, Project Management, Purchasing, Outsourcing and Contracting out, Using IT Tools and Techniques, Security, Health and Safety, and Data Protection. Each chapter is divided into sections; at the head of each section is a ‘Policy Statement’ for that issue. These are in the form of a short statement summarising the policy behind the ‘how to’ content. For example, chapter 6 contains a section on Design Techniques (6:4) ‘The organisation is committed to developing and operating high quality IT systems. Where design work is required as part of system implementation, appropriate design techniques and
representations must be adopted. These should be used to clarify interactions between those performing development work, discussion with end users and in negotiation with external suppliers.’ Straightforward comments that belie the complexity of the topics that follow. In short, this is a manual for running the IT section of a firm.

As is becoming more common with reference works, a CD is included with the package. In addition to the looseleaf and the CD supplied, subscribers are promised six-monthly updates in the form of replacement CDs and pages as well as four bulletins per year and access to a monthly email newsletter. With the CD is a manual for installation and running instructions for Microsoft Windows and NT, with a software requirement of Windows 3.1 or later. As these are operating systems that some readers may not be familiar with, or even avoid, I called the Customer Service Team at the number given in the book to see if other platforms were supported. The representative was friendly and attentive, but unfortunately did not ‘know much about CDs’, but did seem to think that there was only a CD for Windows users. This is probably because of the proprietary format used for the document viewer. My plea is for publishers to move to a more standardised distribution format for content that will allow Unix, Macintosh and other platforms easy access to such useful tools and content. Here, my practical challenge was to reinstall the Windows emulation on my laptop to check out the CD, admittedly this was probably something not anticipated by the publisher. The CD viewer, once I enabled the compatible operating system, worked flawlessly, although it is not very slick. It reminded me of very early versions of FolioViews. There is little reason why the materials could not be supplied simply as HTML for simple access, or Adobe Acrobat files, if it was felt that more sophistication was needed to give pop up comments and easy searching as well as the hot links.

Lawyers as well as IT managers may be drawn to chapter 9, as it deals with Data Protection and the reviewed version was updated at the end of 1999 requiring consideration of both the 1984 and the 1998 Acts. However, as this is primarily a management text, do not expect to find references to case law or any in-depth study of legislation that has been described by counsel as a ‘thicket’ \textit{(Campbell v Mirror Group Newspapers)}. The chapter does serve its purpose, which is to put IT managers on alert for the need for compliance with the legislation and offer some procedures that will help them avoid falling foul of the Act. For the lawyer \textit{IT Policies} can offer you something of an insight into how system management can work, though in reality it is more likely that in a law firm it would find itself on the desk of the practice manager who wishes to get a better grip on her IT infrastructure, or the IT director of the firm.

These three works are unlikely to be at the top of the reading list for many readers of this journal, but they will all make good presents if you have IP/IT neophytes, practice managers or contract designers in your circle: for those of your friends that do not yet understand the issues arising
in information technology, intellectual property and law, *Digital Property* will get them started; for your IT support group or practice manager *IT Policies and Procedures* will help them adopt tried and trusted methodology for system infrastructure; and *Computer and Internet Contract and Law* will make a fine gift to someone in the computer contract area, or even for yourself if you desire to turn out the odd contract.

*The Internet – Business Strategies for Law Firms* by Andrew Terrett, Law Society Publishing, 2000, £32.95, 240 pages (ISBN 1 85328 582 X)

Review by IAN KING

Andrew Terrett is currently a consultant with Baker Robbins and Company technology consultants. Previously, he has been an Information Systems Advisor and non-practising solicitor at Masons, and co-ordinator of the Law Technology Centre at the University of Warwick. He therefore has wide experience of all aspects of legal IT at both the practical and academic levels. However, as its title suggests, this book is very much aimed at legal practitioners rather than academics, containing practical guidance for law firms wishing to implement an Internet business strategy.

The author does, though, provide some theoretical context for his practical advice. In Chapter 1 he makes no secret of the fact that he supports Susskind’s view that the Internet is changing the way in which legal services are delivered, that the old ‘paradigm’ of one-to-one, advisory legal service will eventually give way to a new one-to-many, packaged legal information service. He argues ‘it is no longer a question of whether information technology will alter the practice of law but a question of how and when’. However, Susskind’s arguments are dealt with very briefly and are largely accepted as proven fact, though there is a short analysis of contrary views in Chapter 12. Those interested in learning more about the theory should read Susskind’s *The Future of Law* and *Transforming the Law*, as this book is very much for practitioners who wish to know how the Internet may be exploited for the benefit of their own business.

As the book was published in 2000, some references to the technology are inevitably slightly out of date. However, this does not detract at all from the book’s usefulness. The main focus is on application rather than technology, the business strategies that law firms must adopt if they are to make successful use of the opportunities provided by the Internet. The structure of the book is clear and easy to follow. It is divided into discrete sections that can be read separately. At the end of each chapter there are useful ‘Action Points’ and suggestions for further reading. The book’s main strength is in outlining strategies for such things as on-line marketing (Chapter 3), law firm Intranets (Chapter 5), knowledge management

---

1 Solicitor & Senior Lecturer, Anglia Law School, APU, Chelmsford. E-mail: i.d.king@apu.ac.uk
BOOK REVIEWS

(Chapter 6) and legal e-commerce (Chapter 8). The author gives numerous examples of how the Internet can be used to enhance and expand legal practice.

Whilst some may still question the real impact of the Internet on the provision of legal services, this book clearly shows that the opportunities are there for firms that are willing to embrace change. As the author rightly points out, the main challenge is in accepting and encouraging the cultural change necessary to make a success out of the Internet. The technology itself is only a minor issue. A recent survey of FTSE-100 companies by Oyez Legal Technologies found that only 47% of law firms dealing with large, complex or multinational litigation provided electronic support services to their clients, in spite of the fact that they all had the technical capability to do so (Law Society Gazette, 19 September 2002, p.13). That even the largest law firms are failing to exploit their Internet technology to the full suggests that there is still much to be done by the legal profession as a whole in developing effective business strategies for the Internet.

So is this book worth buying? Yes, both for firms that as yet have no website, and also for the very many firms that do, but are not entirely certain what they are trying to achieve by having one. This book provides much useful information and assistance for firms in developing a strategy for effective use of the Internet. As the author makes clear, it is not a book to be read from cover to cover, but to be dipped into. Not all sections will be of equal interest to all readers, but this does not detract from the value of a book that offers excellent practical advice to legal practitioners.


Review by SUSAN SCHIAVETTA

The recent United Kingdom consultation paper Modernising the Civil Courts noted that ‘[o]ther countries are pointing the way to what can be achieved’ in the area of e-justice and the courts. Justice and Technology in Europe: How ICT is changing the Judicial Business aids the discussion in this domain by canvassing the ways in which information and communication technologies (ICTs) have been implemented in a variety of countries. Based on the European seminar on Court Technology held in Bologna in September 2000, this book is made up of contributions from different professionals in the field. It is divided into two parts; Part I focuses on developing e-justice from case management systems and Part II deals with developing ICT in centralised and fragmented judicial systems.

Covering fourteen European Economic Area countries and Latin America, an in-depth overview emerges of the state of the art of ICT

1 Universities of Strathclyde and Oslo.
implementation in judicial systems. Unfortunately, the papers on Portugal, Luxembourg and the European Court of Justice (ECJ) have been omitted from the book for reasons that are unspecified. The loss of the ECJ analysis is particularly disappointing, in that it would have been interesting to establish the ICT diffusion occurring in judicial processes at a supranational level, especially considering the continued desire to harmonise the judicial systems of the European Union. Despite this, the extensive range of analyses produced offer a good insight into the current role of ICT.

Editors Marco Fabri and Francesco Contini have done a particularly good job of standardising the diverse contributions. Each chapter takes a similar approach, starting with a profile on the workings of the judicial system present in the respective country. Building on these foundations, the use of technology for managing judicial processes is discussed in greater depth. Conceptually, this works very well, as the reader can come to terms with the underlying theories and reasons behind each country's approach. Various solutions have been adopted by the different countries, which provide an informative overview of the judicial applications of ICT. Indeed, the diverse historical, political and legal differences present in each country have resulted in very contrasting approaches to, not only the operations of judicial systems, but also ICT diffusion. For example, the Spanish State is composed of seventeen Autonomous Communities, which has resulted in the inconsistent implementation of ICT.

Some common trends are identified in the opening chapter, focusing on the specificities and differences. Marco Fabri prepares the reader for the rest of the book, demonstrating that no delusions are held about the brilliance of ICT in the judicial business. The authors are similarly realistic and balanced throughout. For example, whilst the underlying desire to achieve access to justice is brought to the fore, the possible threats to judicial independence are also discussed. The chapter on Latin America pulls together the ideas presented in previous chapters, discussing strategic issues to be addressed during the implementation phase, with one of the main themes being to review past experiences. In the final chapter, Francesco Contini identifies three different phases in the evolution of ICT and its implementation in judicial institutions. Phase I consisted of the exploration of the original ICT legacy systems during the Eighties. During phase II, governance structures began to emerge, which exploited the experiences gained in phase I. Acknowledging the genesis of phase III, Contini is optimistic about the progress being made in respect of e-justice, that is to say the integration of judicial procedures and the Internet.

While emphasising the possibilities that ICT may have for reforming judicial systems, the main aim of the book is to encourage more research on the relationship between technology and the administration of judicial processes. Moreover, by exchanging information the contributors endeavour to accelerate the process of technology diffusion in European judicial
Justice and Technology in Europe is, however, an invaluable addition to the contemporary literature.


Review by MARTINA GILLEN

The editors of Virtual Gender have undertaken the task of bringing together a number of essays, which seek to challenge and explore the assumptions of work on gender and ICTs and which also inform theoretical examination of the gendered nature of our relations with technology with quantitative research data. This is a happy blending of materials.

The work is divided into four loosely themed parts. Part I concerns the gendered nature of access to ICTs, and the complex way in which individual’s experience of such technologies is mediated by the social process of gender. Chapters in this section include some which employ historical reflexivity and biographical narrative to show us the authors’ self-location in the social process of communication, while others draw on quantitative data to explore the ways in which we approach and observe technology. Despite the fascinating (and controversial) article by Michaelson and Pohl, which asserts that email tends to disrupt and neutralise the operation of gender stereotypes that one normally finds in face-to-face problem solving, based on their observations of an email problem exercise among a group of technology students, the highlight of this section is Gillian Young’s article. Young’s article explores the nature of virtual communication and its link to the reconceptualisation of international politics. This article raises the question of the potential for virtual communication to open up the arena of international relations to the marginalised.

Part II addresses the theme of technologies and their use for leisure, pleasure and consumption. This section is an intriguing mix of articles, which treat both with the height of sophisticated technologies (VR) and mundane domestic ones such as the telephone. Many of the chapters in this section explore feminist theories of the ‘gaze’ and conversely how MOO users construct their own identities and view themselves as subjects.
This theme of subjecthood and identity is continued in the final chapter of this section, which analyses the incorporation of specific technologies into our conceptions of gendered roles.

Part III explores aspects of citizenship and ethics in online gender relations. This section is invaluable since the ethical arguments advanced therein are consistently supported with empirical evidence and detailed reference to case studies. Alison Adam’s exploration of how the discipline of computer ethics can be informed by feminist theory is an excellent example of the accessible multidisciplinary nature of this text.

Finally, Part IV moves to the concept of the self and how this is manifested in different ways in e-life. This section not only explores the process of gender swapping (and explores many of the preconceptions surrounding it) but also introduces other approaches to the gendered body as mediated via the digital camera. The final chapter in this book is a stark warning against the rejection of the traditional gendered stereotypes associated with unreconstructed ‘nature’. This warning may sound strange to post-modern ears but drawing on the work of Luce Irigaray, Graham argues that some models of female as natural divinity are more radical and potent configurations of female empowerment than Haraway’s ‘cyborg’. Furthermore, she asserts that these configurations can profitably be used to enrich to cyber-feminist theory.

In summary, many of the ideas and concepts discussed here will not be entirely new to those experienced in this field. However, there is a nucleus of new thinking surrounded by solid empirical data (so rarely available at an accessible level in such a cross disciplinary field) that make this an ideal primer on this subject. Furthermore, the wealth of references make this text an indispensable one-stop reference for those in need of a substantive grounding for their theoretical work.