There are prohibitions on using 'bank' as or as part of a domain name unless it is with the consent of the Monetary Authority pursuant to section 27 of the Banking Ordinance (Cap 155). Similarly there is a prohibition with respect to the words 'insurance' and 'assurance' under section 56(A) of the Insurance Companies Ordinance (Cap 41)

Whether a generic top level domain name ('gTLD') or a country code top level domain name ('ccTLD') is used, so far as the user is concerned, is of no consequence. A 'ccTLD' may, however, be preferred to indicate local connections.

It has already been noted that the laws applicable to the Internet have not been harmonised save through the application of general international convention requirements. One of the difficulties of harmonising 'Internet law' is that it covers so broad a range of personal, financial, commercial, criminal and other activities. Harmonisation, if it ever comes, will undoubtedly be piecemeal. In the United States there are already many reported cases. Only a few United States' judicial decisions have been referred to in this work; the difficulty with US judicial precedent is that the decisions turn on the application of constitutional provisions which simply do not apply here. In particular, the First Amendment to the US Constitution guarantees the right to free speech and this has been applied to allow 'deep-linking', where such a practice may well otherwise be regarded as an infringement of copyright, and the publication of material on the Internet which, in other places including Hong Kong, would likely be taken as being defamatory. There has, however, been significant international cooperation in the technical administration of the Internet.

Internet Corporation for Assigned Names and Numbers (ICANN)

In 1998 the United States Government set up a non-profit making organisation called 'The Internet Corporation for Assigned Names and Numbers' ('ICANN') as an independent body to manage the systems and protocols which will enable the Internet to develop. Hong Kong is represented on this body by the Director of Information Technology Services who sits on ICANN's Government Advisory Committee. The function of this committee is to advise ICANN generally about the concerns of government with particular regard to the interaction of ICANN's policies and local (ie Hong Kong) laws. The hierarchical nature of Internet governance recognises the pre-eminence of the United States in the history and the development of the Internet and the United States will not give up its position lightly. One writer has observed that

> It is impossible that the US will surrender its control … [b]ecause the Internet is the brainchild of the US [and] it is unlikely that the US will give up governance of [the Internet Assigned Numbers Authority] to simply see

> it fall into the domination of other countries who will also treat the registries as their own natural monopolies.[17]

Domain Name System for Hong Kong

The procedure for obtaining a .hk domain name in Hong Kong starts with an application by an individual, company or other organisation to their Internet Service Provider. The ISP then contacts the Hong Kong Domain Name Registration Company Ltd ('HKDNR') who will permit registration of the domain name on a 'first come, first-served' basis. A check is made to ensure there has been no previous registration of the same domain name, but that is all. There is no checking of the name against third party rights such as rights in registered trade marks. This is not considered to be feasible because trade marks may be registered in any one or more of 45 different classes,[18] the appropriate class being determined by the goods and services sold by the trade mark owner. A separate search would need to be carried out in each and every class. In the event of a dispute between, for example, a trade mark owner and an applicant for a domain name, the matter has to be referred to arbitration at the Hong Kong International Arbitration Centre. The question may be asked: 'Why does the HKDNR not simply cross-search a proposed domain name against a trade mark registration?'. This would not, however, necessarily produce a fair result; indeed such a procedure may well serve only to complicate matters. There are two reasons for this:

(a) A registered trade mark may have been left dormant on the register and although it is possible to cancel a trade mark registration on the basis that it has not been used for a period of three[19] or more years, the process is both time consuming and expensive.
(b) A clearance from the Trade Marks Registry obtained as a precondition to the registration of a corresponding domain name may well operate only to give approbation to so-called 'Reverse Domain Name Hijacking'. This is the converse to cybersquatting in that the owner of the trade mark registration is asserting rights beyond the legitimate boundary of the trade mark registration. A fictional trade mark such as SQUIFFO registered for books ought not necessarily be used to stop another's registration of the domain name squiffo.com

17 Rodriguez Aurora, 'Competing Telecommunications and Cyber Regulation – Is There a Need for a Transatlantic Regulatory Framework?', http://mars.coleurop.be/infosoc.
18 See 9th edition of NICE Classification by the World Intellectual Property Organisation applied in Hong Kong with effect from 1 January 2007; http://www.wipo.int/classifications/en.
19 Trade Marks Ordinance (Cap 559), s 52(2)(a).

The judge added:

> … if the local courts are responsible for enforcing and deciding questions of validity and infringement, the conclusions are likely to command the respect of the public.

Aldous J did, however, leave open the possibility that the courts of the UK (and presumably, therefore, Hong Kong) ought to be prepared to intervene in intellectual property rights granted in foreign places if that locality did not provide any or any adequate remedies:

> … it would not normally be right for the courts of this country to decide a dispute on infringement of a foreign patent in respect of acts done outside this country provided there is an adequate remedy in that country. The local court is able to look at the particular acts in which they are carried out. If it happened that there was not an adequate remedy in the other state, it might then be appropriate that action be taken in a state in which there was an appropriate remedy … [But on the facts of the case] I have come to the conclusion that this court has no jurisdiction to hear this claim and for that reason I believe that the allegations in respect of the German and French patents should be struck out …[3]

Double Actionability Principle

In the broader context of tort law, traditionally the courts in the UK applied a principle which was known as 'double actionability'. If a tort was to be actionable in the UK it also had to be a wrong in the country where the event took place. However, what may be a wrong in England may not be a wrong overseas and this deficiency was corrected as between parties to the Brussels and Lugano Conventions.[4] The strict double actionability rule requiring the matter complained of to be a wrong both domestically and in the place where the tort was committed appears to have been abandoned, at least in so far as concerns intellectual property law generally and copyright in particular. In the recent decision of *Pearce v Ove Arup*[5] the parties were able to litigate before the UK courts a matter of infringement of copyright in circumstances where the material in issue was not copyright protected in

3 *Plastus Creative AB v Minesota Mining and Manufacturing Co & Anor* [1995] RPC 438 at 447, per Aldous J; see also *Molnlycke AB & Anor v Proctor & Gamble* [1992] RPC 21 where Dillon LJ at 28 said: '…proceedings for infringement of a United Kingdom patent can only be brought in a United Kingdom court, in the present case the English court, and can only be founded on infringement in England. The German court could entertain the action for infringement of the comparable German patent, but could not entertain a claim for infringement of an English patent.'

4 Since Hong Kong is not a party to these Conventions, they will not be discussed further. The discussion consequently centres on common law principles deduced from UK cases which therefore have persuasive authority in Hong Kong.

5 [1999] FSR 525.

the UK but did have copyright protection in the Netherlands. 'Provided this decision holds up in future – further, it seems to have become permissible to bring an action in England in respect of the infringement abroad of foreign intellectual property rights, no matter whether the country concerned is or is not a Member State of the EU or of the European Free Trade Agreement (EFTA)'.[6] There is no reported case as yet in Hong Kong in which the *Pearce v Ove Arup* decision has been considered. It is submitted that the decision is good law, especially in view of e-developments, and ought to be adopted in Hong Kong. In *Red Sea Insurance Co v Bouygues SA*[7] the court had to consider whether the defendant could rely on Saudi Arabian Law to establish direct liability in tort when Hong Kong law does not recognise liability.[8] The brief facts of the case were that the plaintiffs bought an action in Hong Kong against the defendant, a Hong Kong insurance company with its head office in Saudi Arabia, claiming an indemnity for loss and expenses incurred in relation to a building project in Saudi Arabia. The Privy Council held that the case could be heard in the courts of Hong Kong subject to the court applying Saudi Arabian law. The court noted that the project was to be carried out in Saudi Arabia; the Saudi Arabian Government owned the property on which the work was to be carried out; the supply contract, the service contract and certain other contracts were made subject to Saudi Arabian law; the breaches and alleged damage occurred in Saudi Arabia and so on. On the facts of the case, the Privy Council was prepared to follow the revised rule asserted in Dicey and Morris:[9] '… a particular issue between the parties may be governed by the law of the country which, with respect to that issue, has the most significant relationship with the occurrence and the parties'. In other words, the strict effect of the 'double actionability' principle was ameliorated in the particular circumstances of the case. This is quite different from asserting that the 'double actionability' principle has been abrogated.

If, contra the decision in *Pearce v Ove Arup*, the 'double actionability' rule is continued in Hong Kong requiring a tort in both the foreign jurisdiction and in Hong Kong to be proved before action can be taken in the courts of Hong Kong, a possible problem peculiar to the Internet could arise. Some jurisdictions may weaken intellectual property rights in order to attract e-businesses, especially that of Internet Service Providers. Thus, acts that are commonly treated as breaches of laws

6 Cornish, *Intellectual Property*, (4th edn) at p 93, para 2–73.

7 [1995] 1 AC 190, Privy Council hearing an appeal against a decision of the Hong Kong Court of Appeal.

8 The law of insurance in Hong Kong and Saudi Arabia was such that if Hong Kong law was applied, there was no claim whereas if Saudi Arabian law was applied the plaintiff did have a claim.

9 Dicey and Morris, *The Rule of Displacement* (1993), (12th edn), r 203(2) – the rule has been further refined in the 13th edition of the work.

than one jurisdiction. However, it may well be futile to litigate over the same wrongdoing in more than one jurisdiction because courts generally will not enforce double recovery for losses sustained by the wrong.

If the Hong Kong court is satisfied that an unlawful event has occurred in Hong Kong, the court has a discretion whether or not to accept jurisdiction over a dispute concerning the content of a website. This potential for accepting jurisdiction exists despite the fact that the web site's proprietor and host computer are situated outside Hong Kong. Two tests are applied:

(a) Can the plaintiff show a 'good arguable case'? Clearly, a Hong Kong court ought not to permit the issuance and service of a writ overseas in respect of matters the court considers frivolous or without a decent chance of success.
(b) The application of Order 11 rule 1 of the Supreme Court Practice: this Order is lengthy but basically permits those who have:
    (i) made contracts in Hong Kong, or
    (ii) broken contracts in Hong Kong, or
    (iii) committed torts in Hong Kong, or
    (iv) have committed torts outside Hong Kong but as a result of which damage is suffered in Hong Kong
    to sue and be sued, as the case may be, notwithstanding that that party is not resident or incorporated in Hong Kong.

Forum non Conveniens

The doctrine of *forum non conveniens* is a principle by which courts are not obliged to exercise jurisdiction if, in their opinion, the courts of a foreign country are significantly more suited to hear the dispute. As a general principle, where the legal bases of action are the same, the courts of one country will not (or ought not) to hear a case which is already being litigated in the courts of a foreign country. The obvious reasons are, firstly, to prevent double recovery from the defendant for the same wrongdoing and, secondly, to avoid the potential for different courts reaching conflicting and perhaps irreconcilable decisions.

RSC Order 11, forum non conveniens and computer hacking

The Commercial Court in London has considered the issues relating to service out of the jurisdiction in *Ashton Investments Ltd v OJSC Russian Aluminium*[48] in which the claimants alleged that for commercial reasons connected with the need on the part of the Russians to obtain certain confidential information, the defendant had inserted spyware into the claimant's computer system. Under Hong Kong law, the material that was

48 [2006] EWHC 2545 (Comm) (18 October 2006).

alleged to have been obtained would have been in breach of the civil law of confidential information and a criminal offence under the provisions of section 161 of the Crimes Ordinance (Cap 200). The act of hacking was performed from Russia but the computer system was in London. Deputy Judge Hurst QC conducted a review of the authorities and the case is worth consideration in some detail since it involves a rare illustration of the principles that ought to be applied in service outside the jurisdiction in the cyberworld.

It was argued on behalf of the defendants that the case should be dealt with in Russia and in examining this issue, expert evidence as to the position under Russian Law was adduced by both parties. The experts gave evidence as to the law and procedure in Russia and the court pronounced its verdict as to the efficacy of applying Russian law in Russia in no uncertain terms: '… it is a cumbersome, complicated and often unrealistic regime'.[49] Later in the judgment[50] Deputy Judge Hurst added: 'I think it is clear that any Russian proceedings would be likely to be rather slow', concluding rather obtusely on this point (given those remarks): He said: 'That is not a criticism of the Russian legal system. However, it is a highly significant factor in this case.' As in Hong Kong, the law on confidential information and hacking is clear under English law, but the position in Russia was less certain. As far as criminal law was concerned, even the expert for the defendant agreed that the case would need the involvement of the relevant law enforcement body and this could not be guaranteed. As for civil law, the claimant's expert said that the legal status of 'information' was unclear. In a similar case in Hong Kong, therefore, the fact that there may be a remedy under the 'black-letter' law of another country does not finish the issue on that point. The question that also has to be determined is whether it is practicable, or efficacious, to force a party into being obliged to rely upon that law.

The other factors considered by the court included the submission that the unauthorised access took place in London. The analogy was made with a letter containing information being taken from the UK but which was not opened and read until it was in a foreign place. Where the information was read was irrelevant. The tort took place in England and the fact that a virtual, rather than physical, medium was used was not relevant to that fact. The judge averred:

> I regard the unauthorised access to the server as being by far and away the most significant element of the events which occurred. Events which occurred abroad were all directed at the server in London. The confidential information was also held in London and English law is probably the applicable law.[51]

49 Para 82 of the judgment.
50 Para 84(vi) of the judgment..
51 Paragraph 83(iii) of the judgment.

The problem of relying on the defence of innocent defamation from the point of view of the Internet Service Provider is the requirement contained in the proviso to section 25(5). This requires that the publisher must exercise 'all reasonable care'. In the same way that a library cannot vet all the books on its shelves, neither can an Internet Service Provider be expected to study all its sites and know whether any material is defamatory. The Defamation Ordinance must, at least on this issue, be regarded as deficient when looked at from the point of view of the Internet Service Provider.

In the UK case of *Godfrey v Demon Internet Ltd*, the defendant was an Internet Service Provider carrying on business under the laws of England and Wales. Demon hosted a forum in which users of the Internet could post messages, which were stored for access for about a fortnight. A message was posted on the website from an unnamed person based in the United States which was defamatory to the plaintiff who requested that Demon should remove the article forthwith. Demon failed to act and it was not disputed that they could have removed the offending message after receiving the plaintiff's request. Demon was held unable to rely on the defence of innocent dissemination set out by section 1 of the Defamation Act 1996.[15] Moreland J put the matter this way: 'the defence [of innocent dissemination] was not available to a defendant who knew that his act involved or contributed to publication defamatory of the plaintiff. It was available only if, having taken all reasonable care, the defendant had no reason to suspect that his act had that [defamatory] effect'. Applying the *Godfrey v Demon* case to the Hong Kong Defamation Ordinance, section 25(5) is satisfied only if the offending message is removed as quickly as possible after receipt of the notification that the site contains defamatory material. There would seem to be room to argue that the Defamation Ordinance goes further than the UK Defamation Act. The use of the words '*all* reasonable care' (emphasis added) in section 25(5) could be argued to mean that the Internet Service Provider ought to establish that the material was not defamatory before it is placed on the worldwide web rather than, as in the UK, allow the posting on the web subject to the requirement that the defamatory material is removed as soon as possible after receiving notification that the material is defamatory. If the freedom of information exchange via the Internet is not to be stifled, it is to be hoped that such an interpretation would be avoided.

The UK High Court has considered the potential for liability of Internet Service Providers in cases where they host a site that is defamatory but have no knowledge of the content of the web site in *Bunt v Tilley & Ors*.[16] The 'high point' of the claimant's case was the fact that

15 See p 39.

16 UK High Court (QBD) [2006] EWHC 407; the full title of the case is *Bunt v Tilley, Hancox, Stevens, AOL UK Ltd, Tiscali UK Ltd and British Telecommunications plc.* This discussion concerns only the last three defendants, all being ISPs.

the ISPs acted as intermediaries that enabled electronic communications to pass from one computer to another resulting in a posting to the Usenet message board. Other organisations such as 'Google' hosted the Usenet service. They were not, however, made a party to the proceedings.[17] The proceedings involved a strike out application brought by the ISPs on the ground that the claimant had no cause of action against them.[18] Although the analogy was drawn with a postal delivery service, this was regarded as too simplistic a comparison upon which to assert that since the postal service would not be acting in a defamatory manner by reason only of the delivery of material, so an Internet Service Provider was a mere conduit. The point was made that:

> … to be liable for a defamatory publication it is not always necessary to be aware of the defamatory content, still less of its legal significance. Editors and publishers are often fixed with responsibility notwithstanding lack of such knowledge. On the other hand, for a person to held responsible there must be knowing involvement in the process of publication if the relevant words. It is not enough that a person merely plays a passive instrumental role in the process.[19]

The court distinguished the facts from those of *Godfrey v Demon* on the basis that the ISPs in this case had not been given any notice of the defamatory acts alleged and the pleadings were inadequate. It was only when particulars of claim were served upon the ISPs did they appreciate that there was a problem. Eady J concluded that the defendants had not 'in any meaningful sense, knowingly participated in the relevant publications' and that '…[M]ore generally, I am also prepared to hold as a matter of law that an ISP which performs no more than a passive role in facilitating postings on the Internet cannot be deemed a publisher at common law'.[20] Eady J went on to say that an ISP was not a publisher or distributor when it played a merely passive role. A distributor might need to prove lack of negligence in order to escape liability for defamation[21] whereas an innocent ISP needs no defence.

One issue that emerges clearly from the decision is that in order to make an ISP liable under the *Godfrey v Demon* principle, the ISP must be notified in terms that are unambiguous which statement(s) are

17 Para 8 of the judgment.

18 This is contrary to the assertion of the claimant at para. 6 of the judgment: 'This is not some tuppeny ha'penny storm in a tea cup, this is a truly vast case, the like of which English Defamation law has never before seen, because of both the scope and nature, as well as the medium. It positively screams out for a Trial, and one way or another it will have one.' The position of BT was pleaded as 'insane and beyond belief': para 34 of the judgment.

19 Para 22 of the judgment.

20 Para 36 of the judgment.

21 Para 37 of the judgment. Here the judge was relying on *Gatley on Libel and Slander* (10th edn) para 6–18

Electronic Messages Ordinance) to deal with spam is section 34 of the Personal Data (Privacy) Ordinance (Cap 486). This requires that if information is addressed to a named individual, it must contain a statement that if the recipient objects to further approaches being made using that particular medium, the advertiser will desist from sending such further materials. An individual's e-mail address is a piece of private information and to send an e-mail to the named individual gives rise to what may conveniently be called a 'first time requirement', that is, to inform the receiver that no further e-mails will be sent to him or her if they object to receiving such communications. The second time an e-mail is sent to that person by the same sender does not require a restatement of the obligation to desist from sending further e-mails, although the recipient can demand that no further use be made of such private information, ie the e-mail address. Section 34 of the Data Privacy Ordinance is not a panacea against spamming because it applies only to communications to named individuals rather than mass communications where the recipient is not named.

Many areas of commercial activity have their own industry specific rules, regulations and codes of practice. This text is not about advertising law per se. It is essential for any trader or advertising agency that is involved in advertising in any way to research and obtain copies of all relevant legal materials. Considerable assistance can be gleaned from contacting trade associations, the Consumer Council or taking specific legal advice if necessary. Particular consideration must be given as to whether it is sensible to advertise on the worldwide web products which cannot lawfully be sold to, for example, people under 18 years, etc. Some countries may specifically prohibit the advertising of certain goods or services on the Internet. It would therefore be advisable to include a term and condition that the company (web advertiser/supplier) may refuse to accept any order on the ground that to fulfil the order would be a breach of the customer's local law. Further, the terms and conditions should state that the supply dates may have to be delayed pending a check being made on local law relating to the sale of a product in a particular country. Where it is known that a particular country prohibits the sale or advertising for the sale of certain products, it may be as well to state in the website that the prohibited goods are not for sale in the country concerned and that no orders will be accepted from, and no deliveries will be made to, that country. It may be prudent to remember that there are no genuine profits to be made without some expense and the cost of obtaining local advice is a necessary corollary to worldwide profit being gained via Internet trading.

It is probable that the Internet will be used widely as a means of comparing the merits and demerits of products and services as a (supposedly) objectively detached survey, or by traders comparatively advertising their goods or services against their competitors and it is to this topic we now turn.

Comparative Advertising

Comparative advertising normally involves comparing one item with another to extol the virtues of the advertiser's product. The advertising is aimed to show that the advertised product is better value than another, performs better than another, lasts longer than another and so on. The law is governed basically by the Trade Marks Ordinance (Cap 559) which, in principle, allows trade marks to be used comparatively, and the Copyright Ordinance (Cap 528) which forbids the use of copyright material in a comparative advertisement. To put the position more accurately, there is no defence contained in the Copyright Ordinance that would make lawful a breach of copying by reason of the material being used comparatively. The distinction can be explained in this way. A trade mark that consists of a single word or small number of words may be registered under the Trade Marks Ordinance. The effect of section 21(1) is to positively permit the use of another's trade mark in a comparative advertisement. A trade mark that consists of, or contains, a logo, however, may also be protected as a form of artistic copyright. It follows that to use the logo in a comparative advertisement may be valid under the Trade Marks Ordinance but unlawful under the Copyright Ordinance as a breach of artistic copyright.

For the sake of convenience, the law of comparative advertising will be examined from the standpoints of (i) infringement of a registered trade mark (ii) passing off and (iii) copyright infringement under separate headings although the advertisement must be considered cumulatively against each of those possible causes of liability. It should be noted that there is also a fourth possible head of liability, that is, malicious falsehood but this will not be considered in detail here. The problem with malicious falsehood is that it requires proof of malice which is always a difficult task for a plaintiff. In *BA v Ryanair*[2] Jacob J questioned whether a claim to injurious falsehood added anything that was not available under a claim to a trade mark infringement. He said: 'It is difficult to imagine a case where, given a valid trade mark registration covering the goods or services concerned, could add anything. Including such a claim was, for instance, wasteful in one of the earlier telephone wars.'[3] The learned judge added that it appeared to him that the claim for injurious falsehood merely put the plaintiff to the added burden of proving malice and dealing with problems concerning the 'one meaning rule'[4] thereby

2 [2001] ETMR 235 paras 9-14.

3 The 'earlier telephone wars' referred to was *Vodaphone Group Plc v Orange Personal Communications Services Ltd* [1997] FSR 34.

4 In defamation proceedings, '[T]he judge's function is to delimit the range of meanings of which the words are capable and to rule out any meanings outside that range: the jury's role is to decide what meaning within that permissible range the words actually bear' – see para 30.4 of Gatley on Libel and Slander (9th ed).

(a) The nature of the employment.
(b) The nature of the information itself.
(c) Whether the employer impressed upon the employee the confidentiality of the information.
(d) Whether the relevant information can be easily isolated from other information which the employee is free to use or disclose.

These four considerations will be dealt with in turn.

Nature of the employment

Where the employee habitually handles 'confidential' information, the employee may be expected to appreciate its sensitive nature to a greater extent than if he were employed in a capacity where such material reaches him only occasionally or incidentally. The job of a person in a marketing department is to extol the virtues and products of a company. That person may be in much greater need for guidance as to what is and is not to be kept confidential than would, say, a person working in research and development who would generally appreciate the need to avoid leaks and the competitive edge that may be lost if confidential information is allowed to leak.

Nature of the information itself

The information will only be protected if it can properly be classified as a trade secret or material which, while not properly described as a trade secret, is in all the circumstances of such a highly confidential nature as to require the same protection as a trade secret. 'A restrictive covenant will not be enforced unless the protection sought is reasonably necessary to protect a trade secret or to prevent some personal influence over customers being abused in order to entice them away.'[20]

Whether employer impressed on employee the confidentiality of information

The key word here is 'impressed'. It is not sufficient that the employee is told that the information is confidential. It is the 'attitude' of the employer towards the information which is evidence as to whether information can properly be regarded as a trade secret. If confidentiality could be asserted merely by stating 'this is confidential' (or words of the same effect), the employer could make all his firm's information fall within the confidentiality-protected bracket irrespective of the true worth

20 Per Neill LJ in *Faccenda Chicken v Fowler* [1986] 1 All ER 617 at 626.

and intentions towards that information. Megarry J in *Coco v Clark* remarked that the law of confidential information will not extend to 'trivial tittle-tattle'[21] even if it is marked with a 'confidential chop'. Similarly, passing information around the office by internal e-mail would seem to be the antithesis of a confidential information paradigm. Often the material can read by others and forwarded far more easily than would be the case with physical files.

Whether relevant information can be easily isolated from other information which employee is free to use or disclose

It would appear from the judgment of Neill LJ that the 'separability' of the information regarded as being confidential is an evidential pointer as to whether the information really falls within the legal epithet 'confidential information'. Neill LJ asserted: '…we would not regard the separability of the information in question as being conclusive, but the fact that the alleged "confidential" information is part of a package and that the remainder of the package is not confidential is likely to throw light on whether the information in question really is a trade secret'.[22] The rationale here appears to be that the employee or other person to whom the confidential information has been communicated ought not to be required to assess whether he/she is dealing with confidential information: there should be no 'grey' areas. The material which is confidential ought to be kept in separate physical folders or different computer files and in the latter case, password controlled. It may, of course, be the case that the material which is confidential is so obviously apparent that to separate out the confidential information would be unnecessary, but where there is potential for doubt 'separate' must be the key.

Destroying confidentiality

The *making available* of confidential information destroys the confidentiality of that information. Thus, uploading confidential information onto the world wide web would be antithetical to confidentiality even if nobody actually accessed the particular web site. The placing of confidential information on the Internet means that the information becomes a part of the public domain over which there is no control. Publication on the Internet is in fact and in law publication to the whole world. A person who unlawfully puts confidential information

21 [1969] RPC 41 at 48.
22 *Faccenda Chicken Ltd v Fowler* [1986] 1 All ER 617 at 627.

imposes criminal liability upon 'any person who engages in bookmaking, whether on one occasion or more than one occasion, by receiving, negotiating or settling outside Hong Kong a bet – (a) which is placed from Hong Kong; or (b) placed by a person who is in Hong Kong when the bet is placed …'.

'Archbold Hong Kong 2007' raises the question that the new section 7(1A) may be beyond the competence of the legislature since there is no express power conferred by the basic law to make law with extra-territorial effect.[2]

Section 7(1A) is supported in its extra-territorial effect by section 8 which makes betting with a bookmaker an offence 'whether the bet is received inside or outside Hong Kong'.

Possible Liability for Internet Cafes

One issue that is open for the courts to consider is whether the operator of an Internet café or Internet shop could be made liable for unlawful gambling activities that take place on or from their premises. As a matter both of general law[3] and an application of specific provisions of the Gambling Ordinance, it would seem to indicate that the operators and managers of such establishments must be careful as to what activities are undertaken from their premises. Section 2 requires a 'place' to be physical but is widely drafted to include 'any ship, aircraft or vehicle and any spot on land or water'. Sections 13 and 15 may have the effect of imposing criminal liability in the following circumstances. Section 13 under the heading 'Gambling in any place not being a gambling establishment …' goes on to state:

> (1) Any person who operates or manages or otherwise controls unlawful gambling in any place whatsoever (not being a gambling establishment) whether or not the public have or are permitted to have access thereto … commits an offence ….

Section 15 extends the responsibility to 'owners, tenants, etc' in the following terms:

> (1) No person shall –
>
> (a) being the owner, tenant, occupier or person in charge of any premises or place, knowingly permit or suffer such premises or place or any part thereof to be opened, kept or used as a gambling establishment;

2 See para 38-61 (but the Basic Law does not expressly allow the Government of the Hong Kong SAR to refer matters to the People's Congress in Beijing for re-interpretation, but that does not stop such an act being undertaken).

3 See, for example, the copyright case of EASYINTERNETCAFÉ discussed at pp 174–175.

> (b) let or agree to let, whether as principal or agent, any premises or place knowing that such premises or place or any part thereof are or is to be opened, kept or used as a gambling establishment.

It will be noted that the burden on 'owners, tenants, etc' of section 15 is ameliorated by the requirement of proof of knowledge whereas the person who 'operates or manages' an establishment has no such defence.[4]

Part IIIA[5] applies in connection with –

> OPERATING PREMISES OR PLACES FOR PROMOTING OR FACILITATING BOOKMAKING, ETC, PROMOTING OR FACILITATING BOOKMAKING, ETC, AND RESTRICTION ON BROADCASTING OF TIPS, ETC.

Sections 13 and 15 deal with a person having control or managing the place where gambling takes place which, in the cyberlaw context, would be the owner, operator, tenant or franchisee of an Internet café or Internet shop. The insertions made by the Gambling (Amendment) Ordinance, namely, sections 16A–16D deal with operating and managing, etc premises for promoting and facilitating bookmaking and are germane to the current discussion. It should be noted that section 16E requires the consent of the Secretary for Justice before any proceedings under Part IIIA are commenced which may operate as a safeguard against the over-zealous prosecution of a *bona fides* Internet café or Internet shop. (Not directly relevant are the anti-fortune telling provisions of section 16E being a 'restriction on broadcasts of forecasts, hints, odds or tips as to results of horse, pony or dog races').

The broad definition given by the words 'any place whatsoever' in section 13 may well give the operator of an Internet café or Internet shop difficulties. The section 15 requirement of 'knowledge' does not, as has been noted, apply in favour of a person who 'operates or manages' a place used for unlawful gambling. The owner or manager of an Internet café or Internet shop must not, therefore, turn a blind eye to the obvious. For example, observing a user refer to credit cards may give rise to suspicion although the card usage may have nothing to do with gambling activities: the matter should be checked. A group of persons overheard talking about dog or horse racing may give rise to suspicion that an Internet site is being used for the purpose of gambling and it would appear sensible to check the sites being accessed and warn the customer not to use the facility for gambling purposes. It would, it is submitted, be going to far to install spyware on each computer so as to enable the owner or manager of the premises to have knowledge of the sites currently being viewed from the premises. Such an action would breach

4 The mens rea aspects of 'knowledge' are discussed in chap 6, see especially p 111.

5 Inserted by the Gambling (Amendment) Ordinance.

In common with other intellectual property rights, patents can be sold and licensed. The owner of the patent (called 'the patentee') can sell the patented product or a licence to perform the patented process. In principle, a patent can protect products, software, including software that is used to enhance the technical capabilities of a website, and processes facilitating the manner of transacting online. The right granted by a patent is that it can be used to stop any other party from making, disposing or offering to dispose of, use, import or keep the patented product, or using or offering for use the patented process. It might be noted that in order for there to be copyright infringement, the plaintiff has to prove that his work has been copied and not created by an independent method. In most cases, considerable similarity between the two works will lead the court to infer a rebuttable presumption[79] that there has been copying by the defendant. For patents and trade marks, however, liability may be regarded as a type of strict liability in the sense that intention to copy the trade mark or patent is irrelevant as is proof of copying. If a third party adopts a trade mark independently of knowledge about an earlier right there is an infringement; the same principle applies to a registered patent.

An example of patent infringement using the Internet would be where a computer network user situated in France logs onto the network, accesses a machine that is physically located in Hong Kong and runs software that would infringe a Hong Kong patent registration.[80] In Hong Kong the law relating to patents is contained in the Patents Ordinance (Cap 514) and the Patents Rules. It is true to say that software 'as such' is not patentable but software which produces a technical effect can be the subject of a patent registration. In *Fujitsu's application*,[81] software to build molecular models on a screen which had previously been built by hand was not patentable because the software merely automated the process that had formerly been done by hand. Mere automation is not patentable because the software here falls into the 'as such' category. Contrast, however, where there is a technical problem to be solved and

79 In law, a presumption can be one of two types. The most common type is a 'rebuttable presumption'. For this type of presumption, the law will assume a fact is true or that an event occurred unless the party against whom the presumption is made can adduce sufficient evidence to rebut the presumption, that is, to show it is based on a false premise in the circumstances of the case. An 'irrebuttable presumption' is one that the law will treat as if cast in a tablet of stone and cannot be rebutted by evidence. As an illustration, in Hong Kong criminal law, a child under the age of ten years is irrebuttably presumed to be incapable of possessing the intent necessary to commit a criminal act and between the ages of ten and fourteen years a child is rebuttably presumed not to be capable of possessing the intent necessary to commit a criminal act.

80 This is an adaptation of an example given by Fawcett and Torremans, *Intellectual Property and Private International Law*, at p 158.

81 [1996] RPC 511.

the solution to the problem is to be derived from running software, the software, providing the technical result, should be patentable assuming it is new, involves an inventive step and is not obvious. An example of a computer program producing a technical result is shown in *Vicom Systems Inc's Application*[82] where a computer program was used to improve the quality of pictures and speed up their processing. Since the software produced a technical effect on the pictures, it was held to be patentable.

The rationale for patents is to encourage inventiveness – who will spend money on research and development if, as soon as the invention is made, it falls into the public domain? The problem with the worldwide web is that the technologies are developing and the need to 'interface' technologies between hardware is of the essence if the web is to continue its development. 'Interface' in this context refers to the requirement that hardware be interconnectable and/or interoperable. The continued development of the seamless infrastructure of cyberspace will doubtless be hindered if the patent system works in an anti-competitive fashion, honing the key developments in the hands of an elite few.

Registered Design Rights

The law relating to the registration of designs is to be found in the Registered Designs Ordinance (Cap 522) and the Registered Designs Rules. Prior to the return of Hong Kong to China, the procedure for protecting a design in Hong Kong was to obtain a design registration at the UK Designs Registry. The design was then deemed to be registered in Hong Kong although there was a common practice of advertising the design in a widely circulating newspaper in Hong Kong so as to draw the attention of the trade and the public to the fact that the design has effect in Hong Kong. Another method commonly employed was to advertise the design in the Hong Kong Government Gazette. Designs registered through the UK Designs Registry before 1 July 1997 are deemed to be registered in Hong Kong.[83]

A registered design protects the outward appearance of new three-dimensional objects which have aesthetic appeal. The 'shape, configuration, pattern or ornament applied to an article by any industrial process' may be registered if the finished article has 'appeal to and is judged by the eye' rather than being simply 'a method or principle of construction' or an article or object whose design is determined by the function it has to perform, or the design is determined by other object(s) to which the design must fit in order operate. Registered designs do not,

82 [1987] 2 EPOR 74.

83 Registered Designs Ordinance (Cap 522), s 91.

investigators were obtained by the consent of the copyright owners and therefore such transmission to the investigators could not be said to be unauthorised. 'The owner might not have consented to a copy being placed in the sharing folder, but that is not transmission.'[31]

Having obtained the Norwich Pharmacal order, what happens next? What criminal and/or civil penalties are available against users?

Criminal sanctions

Insofar as concerns the ultimate user, the question to be considered is whether that person is merely in possession of the copyright material or has that person copied the material so as to obtain possession? The converse to that question is this: does the party that makes the file sharing scheme available do the copying? Alternatively, do both the ultimate user and the party that makes the file sharing scheme available do the copying? These are, of course, interrelated questions but the answers are determinative as to whether the end user is criminally liable for copyright infringement.

Assistance in answering these questions may be gleaned from *Playboy Enterprises v Frena.*[32] Playboy's copyright protected images were exchanged over the Internet via a bulletin board 'sysop'. Sysop is the shortened form of sys(tem) op(erator) and refers to an individual who manages a bulletin board system or special interest group. Users of the system were held to be liable by storing[33] (and a fortiori) transmitting images. It is submitted that the same decision would be reached under Hong Kong law:

Copyright Ordinance sections 24(2) governs uploading onto the Internet and section 26(2) governs the making available of unauthorised copies through, *inter alia,* '… the service commonly known as the INTERNET'.

Application of criminal law

Mr Colin Mackintosh, sitting at the Tuen Mun Magistracy, has examined the criminal law concerning P2P file sharing in *HKSAR v Chan Nai Ming.*[34] A so-called 'Seeder' computer was used to uplift copyright protected DVDs onto the Internet which would then be distributed using BitTorrent software. The defendant advertised the existence of the files through newsgroups on the Internet and he enabled others to download

31 At para 12.
32 839 F Supp 1552 (MD Fla 1993).
33 Reed, *Internet Law,* (2nd edn) (Butterworths) comments that '… although the intermediary is, as a matter of technical fact, copying or reproducing the work, it is somewhat metaphysical to say it is *making* the copies or reproduction'.
34 [2005] 4 HKLRD 142.

them. A customs officer traced the source of the uploading to the defendant via information contained in the advertisements. The computer was confiscated and subsequent examination showed that the defendant was the Internet account holder and that he operated under the (unfortunately prejudicial) pseudonym 'Big Crook'. The defendant was charged primarily under section 118(1)(f) of the Copyright Ordinance in that he had attempted to distribute infringing copies of a copyright protected work, other than in the course of or in connection with any trade or business, to such an extent as to affect prejudicially the rights of the copyright owner. He faced an alternative charge of obtaining access to a computer with dishonest intent contrary to section 161(1)(c) of the Crimes Ordinance (Cap 200).

The primary defence to section 118(1)(f) was that 'distribution' is an active, not merely passive, ingredient of the offence and that all the defendant was doing was making available the works to others who wanted to download the material. The defence was shallow. The defendant had had to take the following steps:

(a) Leave his seeder computer connected to the Internet.
(b) Images from the films were contained on 'inlay' cards and superimposed onto a '.torrent' file.
(c) Advertised his activities through the 'Big Crook' name.

The defence was untenable and conviction followed. The learned Magistrate went on to say that, in any event, there would also have been liability under section 161(1)(c) of the Crimes Ordinance but such *obiter* hardly seemed necessary in this case where liability under the Copyright Ordinance is so manifest. On the unlawful accessing point, the Magistrate said this:

> However, it is appropriate, in all the circumstances, for me to record that I am in no doubt that the defendant's act in publishing the '.torrent' file on the newsgroup computer, which thereby made it possible for the seeder computer to upload infringing copies to others, did amount to obtaining access to a computer with a view to a dishonest gain for another. The gain in question was the obtaining of a complete infringing copy of the film. The gain was dishonest in that it was obtained by avoiding the inevitable payment for genuine copy of the film.[35]

The writer cannot envisage any circumstance under which a defendant could, in the case of P2P file sharing, be found not guilty under the Copyright Ordinance and yet be liable under the Crimes Ordinance. Indeed the conviction under the Crimes Ordinance is, arguably, misconceived. It would seem to be legitimate to argue that the physical act of 'dishonest accessing' requires accessing without the consent of the owner of the computer. If there is consent, as impliedly there must be,

35 [2005] 4 HKLRD 142 at 152.

(b) 'a sign may constitute a trade mark even though it is to be used in relation to a service ancillary to the trade or business of a undertaking and whether or not the service is for money or money's worth'.[5]

These provisions are, however, subject to the overriding need to be distinctive and thereby be '… capable of distinguishing the goods or services of one undertaking from those of other undertakings and which is capable of being represented graphically'.[6] It will be noted that *any sign* means that sounds and smells will be registrable as trade marks so long as they are distinctive. The requirement of this type of trade mark being 'represented graphically' is satisfied in the case of sounds by stating that the trade mark consists of 'the roar of a lion' or the 'bark of a dog'. A smell can be 'represented graphically' by setting out the chemical formula or by describing the smell. In respect of smells, the Trade Marks Register might not be the epitome of clarity when it comes to describing a trade mark.[7]

Whilst many web sites use distinctive corporate jingles in the introduction during the time when the site is being downloaded, the transmission of smells over the world wide web might be nearer than might be imagined.[8] It may become an increasingly important marketing tool to register the smell of an article for sale in addition to the more traditional word or logo associated with the item.

Trade mark registration requirements

There is no need for a trade mark to have been used in Hong Kong (or anywhere else) in order to obtain a trade mark registration but non-use for a period of three years from the date the mark is actually entered on the Trade Marks Register will make the trade mark registration vulnerable to a revocation action.[9] The registration of a trade mark is the grant of statutory monopoly rights in that mark and an infringement action can be brought successfully even if the mark has no acquired

5 Section 3(3); this provision overcomes the former position that the name of a retail outlet could not be registered as a trade mark.

6 Section 3(1).

7 The Chanel No 5 perfume has been registered in the UK as: 'The scent of aldehydic-floral fragrance product with an aldehydic top note from aldehydes, bergamot, lemon and neroli; an elegant floral middle note, from jasmine, rose, lily of the valley, orris, and ylang-ylang; and a sensual feminine base note from sandal, cedar, vanilla, amber, civet and musk. The scent is also being known by the written brand name No 5.'
(In other words, if you want to know what this trade mark smells like, buy a bottle of No 5!).

8 Devices that will enable scents to be digitised and transmitted down the Internet to be replicated by attachments to a PC, are being developed. See, eg http://www.digiscents.com and http://www.howstuffworkds.com/internet-odor1.htm.

9 Cap.559, s 52(2)(a).

reputation. In order for such a potentially powerful right to be granted, the corollary is the essential prerequisite that a trade mark must be distinctive in law and in fact before it can be granted the monopoly rights that attach to a trade mark registration. Another trader must not need to use the word(s) or logo that comprise the trade mark as a description or in bona fide advertising. Subject to certain comments appearing below concerning marks that are 'void of distinctive character', to take an extreme example, the words 'Very Good' cannot be registered as a trade mark because another trader's goods and services may also be 'Very Good'.

A short summary of the main objections to the valid registration of a trade mark is contained in the list below. It is, however, always open for an applicant of a trade mark registration to show that by virtue of long and extensive use, the trade mark has acquired a distinctive character sufficient to warrant the grant of exclusive rights even if the mark is 'devoid of distinctive character'.[10] Consequently, unused marks (and marks with insufficient use to establish distinctiveness acquired through use) must not:

- be descriptive for the goods or service or a characteristic of the goods or services;
- be a geographical name;
- be deceptive;
- be the same as or confusingly similar to an existing trade mark used/registered for the same goods/services or similar goods/services. Whether one trade mark is 'similar' to another or is used in relation to 'similar' goods or services can be a fertile source of argument;
- be offensive – in the UK, the trade mark HALLELUJAH[11] has been refused registration, and in Hong Kong the trade mark OPIUM is not acceptable for registration for any goods. It ought to follow that an Internet Service Provider should likewise refuse registration of 'hallelujah.com' or 'opium.com' as domain names, but doubtless commercial rather than moral considerations will take precedence. The problem here, of course, is that the answer to the question 'What is offensive?' is highly subjective. This has led to the anomaly in the UK that the trade mark LITTLE PENIS has been refused registration for clothing on the ground of being offensive but accepted for registration as an European Union Trade Mark (that applies to all EU member countries including the UK).

The 'best' trade marks (in the sense of most easily defended from the infringement perspective) from a legal point of view are invented words such as KODAK and PERSIL, to use two well known names, because

10 Sections 11(1)(b) and 11(2): the use proving distinctiveness must be use prior to the application date.

11 [1976] RPC 605.

One in a Million	Global Projects Management
The defendants had a previous history of registering domain names.	The claimant (defendant in the counterclaim) had no previous history of registering domain names.
The defendants sought to profit from registration of the domain names by seeking to sell them back to the owners.	Global Projects Management did not, and had no intention of, seeking to sell the domain name citigroup.co.uk to Citigroup or to any other party.
The various plaintiffs were well established companies with household name reputations.	At the point of issuing the announcement to merge, there had been no previous use of the name Citigroup and, indeed, it would be six months before the name was used commercially by the newly merged company.

Summary judgment was granted to Citigroup Inc on their counterclaim and consequently there was justification for bringing a threat of proceedings. In applying the *One in a Million* decision, the whole tenor of the decision of Park J was to avoid qualifying or limiting the effects of that judgment in any way:[29]

> A key strand in Aldous's LJ reasoning[30] was that the main names which One in a Million succeeded in having registered to it were 'instruments of fraud'. I do not think that he meant fraud in the criminal and most pejorative sense of the term. The directors of One in a Million no doubt thought that they were entitled to do what they had done and that they were not in breach of any legal rules. Nevertheless 'instruments of fraud' was the expression which Aldous LJ used. Mr Sumption at first instance had used the slightly toned down expression 'instruments of deception'.[31]

It would seem to the writer that the use of the terminology 'instrument of fraud' vis-à-vis passing off is unhelpful since there is no criminal basis to a passing off cause of action. 'Instrument of deception' would seem to be far more apposite for use in the civil context, reserving 'fraud' for the strictly circumscribed proceedings of fraudulent misstatement if that was ever to be the cause of action in the circumstances of cybersquatting and, *a fortiori*, phishing.

29 At one point in the judgment, Park J noted that counsel for Global Projects Management may have put forward arguments not considered in the *One in a Million* case, but since *One in a Million* had determined the question of trade mark infringement, those arguments were not going to be dealt with: see paras 59 and 60 of the judgment.

30 In the Court of Appeal hearing of *Marks & Spencer plc & Ors v One in a Million.*

31 Paragraph 39 of the judgment.

Passing off and similar fact evidence

With regard to the first point made by Aldous J in the *One In A Million* case concerning the previous history of the defendants, one wonders in relation to the registration of domain names what is the relevance of the history of the defendants? Unless the law relating to passing off vis-à-vis cybersquatting is uniquely to include a civil equivalent of the principle of *similar fact evidence*[32] found in criminal law, surely the history of the defendants is irrelevant to the question: has there been, as a fact, passing off in this case? If a type of similar fact evidence is to be applied in cybersquatting cases, it can only legitimately be applied in circumstances where it is unknown who is responsible for committing the passing off and not as to the issue of whether or not passing off has in fact taken place. In the *One in a Million* case, the identity of the culprits was never at issue: what was at issue was whether in law the defendants' activities constituted passing off. Secondly, the names concerned 'were well known "household names" denoting in ordinary usage the respective respondents'.[33] The registrations were held to be instruments of fraud and, as in the *Glaxowellcome* case, a mandatory injunction was ordered to transfer the domain names to the respective plaintiff.

Park J threw light on the previous history of the defendants in relation to proof of cybersquatting in *Global Projects Management Ltd v Citigroup Inc*[34] by reference to one of the plaintiffs in *One in a Million*, namely, Sainsbury plc. Park J explained that Sainsbury is a common surname in England and it is highly likely to be the case that there are many businesses apart from the famous chain of supermarkets that use Sainsbury as a corporate title. The evidence to show cybersquatting in that particular instance (as distinct from merely adopting a common English name and registering it as a domain name) was the previous conduct of the One in a Million company. In the case of *Global Projects Management*, the evidence of cybersquatting was the date that the

32 Similar fact evidence is a concept in criminal law which enables the prosecution to establish evidence of the accused's bad character, provided that the probative value of such evidence is such as to outweigh its prejudicial effect. In other words, the evidence must tend to show that X committed the crime and not simply that X is a bad person. Similar fact evidence is a type of circumstantial evidence which, in order to be admissible, must go directly to the issue of guilt. A stark illustration of the principle is *R v Straffen* [1952] 2 QB 911, where the defendant had killed two young girls and was committed to a 'secure' (sic) mental institution. He escaped and during the four hours of his freedom, another young girl was murdered. In each of the three cases, the girls had been strangled, they had not been sexually interfered with, they had apparently not struggled and their bodies had been left out in the open. The circumstances of the deaths of the first two girls was held to be admissible as evidence as proof of the guilt of the accused in the killing of the third girl.

33 *Marks & Spencer plc & Ors v One in a Million Ltd & Ors* [1999] FSR 1 at 23.

34 [2006] FSR 39.

arbitration panel's decision to order cancellation, the complaint should file its own application for the domain name.

A summary of the Hong Kong dispute resolution procedure is as follows:

Hong Kong Domain Name HKIAC Arbitration Procedure

Complainant submits Form A and fee

↓

HKIAC reviews document as a formalities check

↓

If there are any defects, they must be corrected within 5 days

↓

Complaint is sent to respondent

↓

Respondent must file a Form B to defend the proceedings within 28 days
(The failure of the respondent to file a Form B does not end the matter; the panellist must decide the issue on the evidence filed by the complainant)

↓

Within 5 days following receipt of Form B, HKIAC appoints arbitrator(s)[1]

↓

Within 7 days of the appointment of the arbitrator(s) the parties may object to that person(s)

↓

Arbitration panel rules within 21 days from receipt of Form B

↓

Decision is notified to the parties within 3 days of receipt by HKIAC

Governing Rules

The governing body for the administration of domain names and resolution of disputes is ICANN[2] which adopted a 'Uniform Domain Name Dispute Resolution Policy' on 24 October 1999. The notes state that the policy has been adopted by all accredited domain name registrars for domain names ending in .com, .net and .org. The policy has also been adopted by certain managers of country code top level domains. This includes Hong Kong: .hk

The substantive rules applicable to the resolution of domain name disputes are to be found in paragraphs 4 and 5 of the Policy. Paragraph 4

1 This depends upon whether the complainant chooses a one-person or a three-person panel. If a panel of three persons is chosen, the fee is higher. There are no dissenting opinions.

2 http://www.icann.org.

requires disputes to be submitted to 'Mandatory Administrative Proceedings' where an allegation is made that a domain name registered by a party is in breach of paragraph 4(a)(i), (ii) and (iii) of the Policy. The provisions concern allegations that:

(a) your domain name is identical or confusingly similar to a trade mark or service mark in which the complainant has rights; and
(b) you have no rights or legitimate interests in respect of the domain name; and
(c) your domain name has been registered and is being used in bad faith.

It should be noted that these requirements are cumulative so that an allegation based simply on an assertion of confusing similarity with trade mark would not be sufficient to cause the cancellation or transfer of a domain name. Evidence of Registration and Use in Bad Faith is dealt with expressly by paragraph 4(b) of the Policy which lists the circumstances which 'in particular but without limitation … shall be evidence of the registration and use in bad faith'. The circumstances are:

(a) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting or otherwise transferring the domain name registration to the complainant who is the owner of the trade mark or service mark or to a competitor of that complainant, for valuable consideration in excess of your out-of-pocket costs directly related to the domain name; or
(b) you have registered the domain name in order to prevent the owner of the trade mark or service mark from reflecting the mark in a corresponding domain name, provided you have engaged in a pattern of such conduct; or
(c) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or
(d) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

This guidance as to what may be considered to be bad faith is self-explanatory covering cybersquatting and unfair business practices subject to the proviso that there has been a previous course of such conduct. (It is unclear as to why the proviso was expressly inserted into the rules and it could perhaps have been better left to the tribunal to consider how much weight should be attached to previous conduct or the lack of it rather than making proof of previous conduct a prerequisite for bad faith under that head.). The circumstances of (c) would seem to be a sub-specie of (b) and

Schedule 1
Data Protection Principles[73]

1. **Principle 1 – purpose and manner of collection of personal data**
   (1) Personal data shall not be collected unless –
      (a) the data are collected for lawful purposes directly related to a function or activity of the data user who is to use the data;
      (b) subject to paragraph (c), the collection of data is necessary for or directly related to that purpose; and
      (c) the data are adequate but not excessive in relation to that purpose.
   (2) Personal data shall be collected by means which are –
      (a) lawful; and
      (b) fair in the circumstances of the case.
   (3) Where the person from whom the personal data are or are to be collected is the data subject all practical steps shall be taken to ensure that –
      (a) he is explicitly or implicitly informed, on or before collecting the data; of –
         (i) whether it is obligatory or voluntary for him to supply the data; and
         (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
      (b) he is explicitly informed –
         (i) on or before collecting the data, of –
            (A) the purpose (in general or specific terms) for which the data are to be used; and
            (B) the classes of persons to whom the data may be transferred; and
         (ii) on or before first use of the data for the purpose for which they were collected, of
            (A) his rights to access to and to request the correction of the data; and
            (B) the name and address of the individual to whom any such request may be made,

   unless to comply with the provisions of this subsection would be likely to prejudice the purpose for the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to

73 The Principles are recognised as being vague by necessity. To fill the gaps, the Data Privacy Commissioner is given powers to, *inter alia*, encourage data users to prepare Codes of Practice (see s 8, especially 8(b), and s 12). Breach of a Code of Practice is not in itself a breach of the Ordinance, but may be used as evidence to prove that a breach has occurred: see s 13.

which personal data are exempt form the provisions of data protection principle 6.

2. **Principle 2 – accuracy and duration of retention of personal data**
   (1) All practical steps shall be taken to ensure that –
      (a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;
      (b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used –
         (i) the data are not to be used for that purpose unless those grounds cease to be applicable to the data, whether by rectification of the data or otherwise; or
         (ii) the data are erased;
      (c) where it is practical in all the circumstances of the case to know that –
         (i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and
         (ii) the data were inaccurate at the time of such disclosure, and the third party –
            (A) is informed that the data are inaccurate; and
            (B) is informed of such particulars as will enable the third party to rectify the data having regard to that purpose.
   (2) Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. **Principle 3[74] – use of personal data**
   Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than –
   (a) the purpose for which the data were to be used at the time of collection of the data; or
   (b) a purpose directly related to the purpose referred to in paragraph (a).

74 See s 32 of the Ordinance: Statistics and research.
Personal data are exempt from the provisions of data protection principle 3 where –
(a) the data are to be used for preparing statistics or carrying out research;
(b) the data are not to be used for any other purpose; and
(c) the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them.

Cybersquatting

It may be hardly surprising to note that China already has experienced the cybersquatting phenomena but it appears that the courts are prepared to deal with the matter robustly even where the complaining company is a foreign one. Article 8[32] of the Dispute Resolution Policy prohibits the use of another's trade mark as a domain name and no account is apparently taken of the fame or repute of the registered trade mark, nor is account apparently taken of the fact that the registered trade mark and the domain name may be directed at totally different commercial activities or sectors of the economy. It should be noted that it is futile complaining to the CNNIC about cybersquatting because that organisation is not given the authority by the Implementing Rules to cancel domain names registered in contravention of the Rules. However, although CNNIC is prohibited from acting even as a mediator, it is empowered to give accreditation to Dispute Resolution Bodies which are intended to comprise experts in matters relating to the protection of intellectual property rights generally and Internet related issues in particular. None of the Rules, however, set out any procedure or objective standards by which the accreditation is to take place, although the draft measures provide that the procedure shall be organised by the Dispute Resolution Bodies themselves with the approval of CNNIC.

Operation of Dispute Resolution Bodies and Issues of Bad Faith

In *Inter IKEA Systems v International Network of Information Co*,[33] it was reported that the foreign owner of a Chinese trade mark succeeded in restraining the use by the defendant of the domain name *www.ikea.com.cn*. The 'defence' – a sham if ever there was one – was that 'I' stands for 'Internet' and 'KEA' is derived from the name of a parrot native to New Zealand. It might have not gone unnoticed by the court that the defendant had also registered about 2,000 other names, including well known household names, as domain names. The court's finding for the plaintiff was based on two grounds. Firstly, Article 5 of the Unfair Competition Law prohibits the faking of registered trade marks and from using false indicators to mislead people with regard to the quality of products. Secondly, that the defendant misled people into believing that the defendant owned the trade mark IKEA or that it had some partnership with the true Ikea company when no such partnership

32 See http://www.cnnic.net/dir/2003/12/12/1997.htm.
33 *China On Line*, 22 June 2000.

existed ('passing off' by any other name). From a purely legalistic point of view, the only criticism of the decision could be in the use the second limb of Article 5, that is, misleading people with regard to the quality of the product. The defendant had not sold nor had it offered for sale any products and, therefore, there can be no misleading as to the quality of anything. There might also be academic debate as to whether using another's trade mark as a domain name can amount to 'faking' a trade mark, but the writer can see no wrong being caused by such an interpretation.

Since October 1999, China has sought to impose compulsory arbitration for all new (and renewed) domain names. The aim is to seek to provide a level playing field to users of the Internet in resolving disputes by avoiding more expensive court action. The claimant files its complaint with an authorised dispute resolution provider specifying the trade marks or service marks on which the complaint is based. The claimant must also show how the public is or will be confused by the domain name registration and evidence of 'bad faith'. Such evidence could consist of an attempt by the alleged cybersquatter to sell the domain name to the claimant or some third party at an inflated price. The respondent must submit a written reply to the authorised dispute resolution provider within 20 days. A panel of three persons is then convened to hear and settle the dispute within 14 days thereafter. The decision of the panel can be challenged in court proceedings, but unless the court is prepared to apply a high threshold for intervening, that is, to be prepared to overturn the panel's decision in exceptional circumstances, the recourse to the court would logically appear to be to the advantage of the better financed.[34]

Electronic Signatures in China

The Electronic Signatures Law of the PRC came into effect on 1 April 2005. Article 1 states the objective of the law in these terms: 'The law is enacted to regulate acts concerning electronic signatures, and safeguard the lawful rights and interests of relevant parties.' In Hong Kong, the Electronic Transactions Ordinance

34 In Hong Kong, for example, most arbitrations will not be subject to court intervention unless it can be shown that no reasonable tribunal, properly directing itself, could reasonably have come to the decision, not merely that the court itself may have arrived at a different decision. See the test in *Associated Provincial Picture Houses Ltd v Wednesbury* [1948] 1 KB 223 where Lord Greene MR said, at 230: '… if a decision [of a tribunal] on a competent matter is so unreasonable that no reasonable authority could have come to it, then the courts can interfere … but to prove a case of that kind would require something overwhelming …[such that] the court considers it to be a decision that no reasonable body could have come to'.

Other Causes of Action

The limitation of the *Goetz v Pacific Supernet* case was that it was based on contractual arguments whereas most spamming activities involve no connection between the sender and the recipient of the spam. It has been argued in the United States that the sending of spam constitutes the tort of trespass to goods but there is no supporting case law to this effect in the UK or in Hong Kong. One would have thought that if, for example, a protest group bombards a web site with so much spam as to cause it to crash, the owner of the site could seek compensation in trespass although a more likely cause of action would be under the criminal law for criminal damage. In view of the potentially criminal nature of such an activity and the implementation of the Unsolicited Electronic Messages Ordinance (Cap 593), it seems unlikely that a trespass action would ever be resorted to in Hong Kong. Trespass thus remains a fanciful cause of action and for Hong Kong purposes, a topic for purist academic debate. One possible scenario where such an action may be considered is where the person sending the spam leading to a web site crash is based overseas and because of the difficulty in bringing criminal proceedings, no action is brought since the Unsolicited Electronic Messages Ordinance does not bite because of the foreign element.[7] As a last resort, an exasperated party may seek leave to serve out of the jurisdiction, basing the claim on trespass, but such a course of action seems to be a difficult road to follow especially with enforcement.

The main difficulty with formulating a strategy to deal with spam is that fact, according to a government statistic,[8] 99% of spam is thought to originate outside the jurisdiction of Hong Kong. This highlights the need for international co-operation to deal with the problem with countries being prepared to enforce judgements of other countries. Enforcing the criminal law of another country is always a 'touchy subject' and the idea that a UK court would enforce a financial penalty imposed by a Hong Kong court against a UK resident is, unfortunately, a long way off. With that limitation in mind, the Unsolicited Electronic Messages Ordinance confines its scope to activities where it is possible to deal with the problem without recourse to the need to seek enforcement outside of Hong Kong. Criminal law aside, it will be seen that seeking leave to issue out of the jurisdiction for the purpose of seeking a civil remedy against a foreign spammer is not an option.

7 See, further, p 415.
8 Paragraph 6 of Legislative Council Brief on the Unsolicited Electronic Messages Bill (CTB(CR) 7/5/18(06)).

Unsolicited Electronic Messages Ordinance (Cap 593)[9]

The Unsolicited Electronic Messages Ordinance contains 63 sections and two schedules, thereby highlighting the difficulties inherent in formulating a credible legislative framework to tackle spam. The Explanatory Memorandum to the Bill stated: 'The object … is to set up a scheme for regulating the sending of unsolicited electronic messages that have a commercial purpose, including e-mail messages and other forms of electronic messaging.' The first point to note is the emphasis on 'commercial' so that to send spam to advertise a purely amateur football event would not come within the ambit of the Ordinance. The necessarily jurisdictional nature of the Ordinance is highlighted by section 3 which circumscribes a 'Hong Kong link' in a manner that is consistent with enforcement. The fact that the spam originates outside of Hong Kong is irrelevant so long as the individual who sent it is physically present in Hong Kong when the message is sent[10] or is an organisation that is carrying on business in Hong Kong.[11] Of course, if the message originates in Hong Kong[12] or the sender is a Hong Kong company,[13] the Ordinance will have effect. It is to be noted that the recipient must either be physically present in Hong Kong when the message is accepted[14] or the organisation is carrying on business or activities in Hong Kong when the message is accessed.[15] A company based overseas but using virtual offices would therefore appear to benefit from the protection to be afforded by the Ordinance.

Spam, that is to say, the transmission of 'multiple commercial electronic messages' is defined by the Ordinance at sections 14(2) and 21(2) as the sending of 100 messages in a period of 24 hours or 1,000 messages during any period of 30 days. The features of the Ordinance can be listed as follows:

- to ensure that the correct source of the message can be traced
- to give an 'unsubscribe facility', ie no more e-mails to this address please

9 Parts of the Ordinance came into operation on 1 June 2007 and it is understood that the intention is to have the Ordinance fully effective by the end of 2007. This chapter is written on the assumption that the Ordinance has been brought fully into operation but readers are cautioned to check the starting date of any relevant provision. The Office of the Telecommunications Authority and the police are responsible for ensuring compliance.
10 Section 3(1)(b)(i).
11 Section 3(1)(b)(ii).
12 Section 3(1)(a).
13 Section 3(1)(b)(iii).
14 Section 3(1)(d)(i).
15 Section 3(1)(d)(ii).