REPORT PREPARED FOR THE WELSH ASSEMBLY GOVERNMENT

ON

IP CRIME & E CRIME

Presented by IP Wales on 26th March 2009

CONTENTS

APPENDICES
(Supplied under separate cover)

IP CRIME
(a) UK Counter Offensive an IP Crime Strategy, UK Patent Office, Revised 2006.
(b) UK IP Crime Data, IP Crime Group, 2007.
(c) UK IP Crime Report, IP Crime Group, 2007.
(d) OECD 'The economic impact of counterfeiting and piracy', 2007.
(e) EU Framework Study: "Effects of counterfeiting on EU SMEs and a review of various public and private IPR enforcement initiatives and resources" Framework contract B3/ENTR/04/093-FC-Lot 6, Specific agreement n°SI2.448309.
(f) G8 Report on Discussions of the Intellectual Property Expert's Group Meeting in Tokyo on 19th February and 10th April 2008.
(g) UK Supply Chain Toolkit, Protecting your IP Rights, 2009.

E CRIME
(h/i) The future of net crime now; Part 1 – Threats & Challenges & Part 2 Responses, Home Office, 2004.
(j) Card Fraud – the facts, Association for Payment Clearing Systems (APACS), 2005.
(k) What your business really needs to know, National Hi-Tech Crime Unit (NHTCU), 2005.
(l) Fraud and Technology Crimes – Findings from the 2003/4 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources, Home Office, 2006.
(m) Information Security Breaches Survey, Department for Business Enterprise and Regulatory Reform, 2008.
(n) UK Threat Assessment of Serious Organised Crime, Serious Organised Crime Agency (SOCA), 2008-9.

INTRODUCTION

This Report builds upon the published findings in the Opportunity Wales *State of the Nation Report 2006/7*[1] and represents a development on themes explored in the World Intellectual Property Organization / Organization for Economic Co-operation & Development IP Forum held at Cardiff in September 2008.[2]

The aforementioned State of the Nation Report 2006/7 provides encouraging evidence of increased use of ICT by Welsh SME business. Over 70% of Welsh SMEs (with employees) have a web site and nearly 18% of Welsh SMEs (with employees) are now selling products/services on-line. But Welsh SMEs seeking to trade electronically within the global economy are just as susceptible to the risk of 'electronic attack' as their larger competitors. A survey of business organisations by the National Hi-Tech Crime Unit [3] revealed that 77% had suffered virus attacks which cost them £27.8m and 17% had suffered financial fraud costing them £121m.

Whereas on-line trade mark abuses (e.g. counterfeit goods) and copyright infringements (e.g. illegal downloads) are well documented our understanding of the relevance of the linkage between IP Crime and E Crime to the SME sector (e.g. the taking of confidential information) is still in its relative infancy.

The findings of Opportunity Wales would suggest that Welsh SMEs are not in a fit state of readiness to address the threat of electronic attack to their business. There is a demonstrable lack of E Business strategic awareness and management and a clear failure to integrate E Business thinking within overall business planning.

It is in the economic interest of the Wales Region that this commercial weakness is addressed by business support advisory services. Whilst SMEs within Wales account for over 75% of employment within the Region (15% above the UK average) and their number has grown (175,000 enterprises in 2005 as compared to 172,000 enterprises in 2003) this rate of growth is the weakest within the UK.[4]

Andrew Beale
Director IP Wales

---

[1] Paul Beynon-Davies, Donna March, Chloe Chadderton, Bethan Caines, *eBusiness in Welsh SMEs: the State of the Nation Report 2006/2007,* eCommerce Innovation Centre, Cardiff Business School (2007).

[2] WIPO/OECD IP Forum, Millennium Stadium, Cardiff, 10th - 11th September, 2008.

[3] Hi-Tech Crime – The Impact on UK Business (NHTCU), 2004.

[4] Small Business Service (SBS) *Small and Medium-sized Enterprise (SME) Statistics for the English Regions, Scotland, Wales and Northern Ireland 2005*.

EXECUTIVE SUMMARY

In the next Chapter of this Report we scope and review IP Law within the UK. Intellectual property law has developed considerably since the early copyright laws arising from The Berne Convention in 1886 and The Universal Copyright Convention in 1952. The main modern legislation has been the Registered Designs Act 1949; The Patents Act 1977, The Copyright Designs and Patents Act 1988 and The Trade Marks Act 1994. This legislation has been amended by various Regulations in order to incorporate a substantial number of EU Directives into UK law.

The EU legislative programme has sought to address the lacuna existing in national law throughout the EU, as a result of developing technology and scientific progress. The law has to keep pace with these developments; otherwise IP right holders will have no effective redress against infringement of their products, if the law does not recognise those rights and provide adequate protection for them. As the sophistication of those involved in IP infringement develops, along with easy access to a global market via the internet, the incentive to expend inordinate sums of money on creating new software and pharmaceuticals is reduced, if they can be re-produced at a fraction of the cost. If this situation occurs, the national economy will suffer; technology and creativity will be stultified.

This Report progresses to scoping and reviewing the law relating to IP Crime. The main legislation protecting copyright, designs, trade marks and patents is woefully inadequate, insofar as it relates to criminal sanctions. The criminal provisions are under used, and the penalties which can be awarded are derisory, in that most offences are 'either way' offences, triable in the Magistrates Court as well as the Crown Court. Penalties are therefore low. Interestingly the Trade marks Act 1994 provides greater protection for trade mark infringements than other IP legislation save for offences under the Video Recording Act 1984. Both of these Acts contain provision for a maximum 10 year sentence following conviction on Indictment.

This is followed by chapters scoping and reviewing the nature of E Commerce Law and E Crime (otherwise described as Net Crime, Hi-Tech Crime, Computer Crime, Cyber Crime or Internet Crime). Whilst the EU Directives have sought to increase the nature of the protection of IP rights and to facilitate e-commerce via greater consumer protection and recognition of electronic contracts and signatures, it is the general criminal law applied to new technology situations that contains powers, which could be used more effectively in the fight against IP infringement. In particular, the Serious Organised Crime and Police Act 2005 provides for the search and seizure of material, to include electronic data. The Serious Crime Act 2007 contains the power to issue a Serious Crime Prevention Order, which has the effect of restricting the activities of persons involved in IP infringement. In particular conditions can be attached to these orders which regulate a person's business and economic activities. The Proceeds of Crime Act 2002 could be an invaluable tool in recovering assets accrued by a person involved in infringing activities. The Fraud Act 2006 could be invoked to bring charges against a person falsely applying a trade mark to goods, as well as the Trade Descriptions Act 1968 or the Trade Mark Act 1994.

If the Anti-Counterfeiting Trade Agreement, discussed at the July 2008 G8 Summit is implemented in the EU and the UK, there may well be a range of fixed penalties available in situations where a person is found to have infringing material in their possession. It is questionable whether such penalties will have any effect upon organised, large scale infringement. These measures would affect the teenager with illegal downloads on his I-Pod. An encroachment on civil liberties? Maybe. However,

if enough teenagers illegally download music from a popular rock band, the revenue payable to that band will be greatly reduced. A fixed penalty and seizure of the I-Pod would be a great incentive to prevent such low level infringement, and to increase the public awareness of IP infringement generally.

What becomes apparent upon a study of the legislative provisions relating to the protection of IP assets is the lack of uniformity and consistency of protection for various IP rights, and the ineffectiveness of civil and criminal sanctions. The main legislative provisions provide mainly civil sanctions against infringement. Civil remedies are expensive to pursue with costs orders running into thousands of pounds, especially in cases involving patents. Civil remedies for copying or dealing commercially with protected material, consist of damages, account of profits, declarations, destruction of infringing material or injunctive relief. Whilst inhibitive, the remedies are usually only awarded, following protracted litigation. Injunctive relief is often difficult to obtain especially in relation to the search and seizure of infringing material.

The concluding chapters of this Report explore the relevance of the linkage between IP Crime and E Crime for Welsh SMEs. The available legislative provisions are, to a great extent, inadequate to protect IP rights, and in particular to prevent the infringement of 'know how' and confidential information within the UK. The Report recognises that confidential information (including trade secrets) is potentially an important Intellectual Asset of any business but there are no criminal sanctions specifically available for a breach of confidence, as confidential information is not classed as property for the purposes of criminal law. However E Crime provisions include The Computer Misuse Act 1990; The Data Protection Act 1998 and The Public Order Act 1986, which provide criminal sanctions where computers or the internet have been used to facilitate criminal activities, rather than being used for infringing activities. By way of illustration the Computer Misuse Act 1990 creates a series of offences that protect against unauthorised access to computer material, unauthorised acts that impact upon the operation of computers and the use of computers to commit other crimes. There is no definition of a 'computer' within the Act which may result in devices such as I-Phones coming within the scope of the Act. Moreover a person may commit an offence by simply having the intent to secure unauthorised access, without actually gaining access to the data itself. This Report would seek to draw attention to the application of this legislation which is not well known as a tool to combat IP infringement, and may not be used frequently enough to provide a disincentive to the taking of confidential information and know how in the UK.

This Report challenges the perception of IP Crime & E Crime as being no more than counterfeiting, piracy and fraud. At a time when the UK Government is seeking to accurately quantify the scale of the economic threat posed, Welsh SMEs seeking to trade on-line find themselves exposed to a real and present danger from organised crime they are ill-equipped to combat. Whilst this risk certainly includes the dangers of fake goods entering business supply chains, illegal digital downloads and an exposure to new forms of old crimes such as fraud, it also significantly embraces the taking of commercially sensitive data.

IP LAW

1. Intellectual property is a grandiloquent term for legal and enforceable rights, derived from international conventions; European Directives and Regulations; UK legislation; and common law. These rights are primarily rights, and therefore assets, arising out of creative works; scientific inventions; designs; brand identification and the protection of confidential information, such as trade secrets. Many IP rights are also protected by reciprocal arrangements between countries which are signatories to treaties or conventions.

2. IP rights protect the fruits of labour which have been put into the creation of designs; creations and inventions. IP rights represent a valuable economic asset, which must be protected in a way which balances the rights of the IP holder against the need to place into the public domain, life enhancing technology; important scientific discoveries and creative works. Further, IP rights allow the right holder to have a monopoly over his rights for a reasonable period of time, whilst placing his work into the public domain on a limited basis, such as under a licence agreement, or unconditionally, for example, when copyright has expired.

3. IP rights frequently arise out of extensive creative input or prohibitively expensive research and development, producing a product which can be relatively easy and inexpensive to reproduce. As technology and science develops at a rapid speed, trade competition also increases, as companies, or individuals seek to dominate the market with an innovative and desirable product, which potentially provides the creator with financial rewards and a substantial economic asset.

4. The advance of the internet as a device for selling and advertising products, coupled with the expansion of national borders and free movement of goods and services throughout the EU and the ease which businesses can operate on an international level, via communication technology and the use of third world labour, has resulted in a dramatic increase in IP crime, such as piracy and counterfeiting and the illegal use of trade marks. The management of IP rights, whether of a civil or criminal nature has serious ramifications. The IP right holder does not receive the appropriate remuneration for his efforts and there is an obvious danger from substandard copies of electrical goods or pharmaceutical products. The economy also suffers when creativity and innovation are stifled, as the incentive to expend time and money is reduced.

5. IP rights are primarily protected in the UK by way of civil remedies. Whilst the main IP legislation does create a number of criminal offences and sanctions for counterfeiting, piracy and trade mark infringement, the criminal law does not address the problem of IP crime to a sufficient level whereby it is an effective tool in the protection of IP rights in the UK.

6. The scope of IP rights law in the UK is contained in primary legislation, supplemented by various European Regulations. The main legislative provisions are:-

   (i) The Copyright Designs & Patents Act 1988

(ii) The Patents Act 1977

(iii) The Trade mark Act 1994

(iv) The Registered Designs Act 1949 as amended

(v) The Designs (Semi Conductor Topographies) Regulations 1989 (S.I. 1989/1100). These are specific to the industry and of little relevance for the purpose of this paper

In addition to the legislation, protection is offered via the common law, relation to confidential information and passing off. The European Union has issued various directives which have resulted in the amendment of substantive legislation, or the direct implementation of Regulations with the UK.

7. <u>The Copyright Designs and Patents Act 1988</u>

The Copyright Designs and Patents Act 1988 (CDPA 1988) sets out 8 categories of copyright protected work. The first 4 categories are works which are authorial or primary works

(i) literary works
(ii) dramatic works
(iii) musical works
(iv) artistic works

The second 4 categories are entrepreneurial, secondary or derivative works:

(v) sound recordings
(vi) films
(vii) broadcasts
(viii) the typographical arrangement of published editions; (the typography right)

The CDPA 1988 also sets out 3 categories of moral rights, which are the right to be identified as the author or director of a work; the right to object to the derogatory treatment of a work; and the right to privacy of certain photographs and films. The Act also provides protection for databases as well as a basic level of protection for satellite broadcast transmissions made in a country which fails to offer any such protection.

8. Copyright will not subsist in any work unless it was created by a qualifying person; it was published in or transmitted from a qualifying country and in the case of literary, dramatic and musical works, it is reduced into a tangible, or fixed form. The author is a qualifying person if, at the time of making or publishing the work, he or she was a national of an EU country or a country to which the CDPA 1988 has been extended or applied via the Copyright (Application to Other Countries) Order 1999, SI 1999/1751). The first publication in any of those same countries will qualify the work for copyright protection, even if the work is published in a non protected country. Works, which cannot be published, such as sculptures, qualify if

they are exhibited or copies of images of them are issued to the public. The work must also be original.

9. The duration of the protection offered by copyright, is generally 70 years from the end of the calendar year, in which the author does the work was made, or when it was first made available to the public. Sound recordings, performances and broadcasts, are protected for 50 years, and typographical arrangements for 25 years.

10. A copyright owner has the exclusive right to undertake certain restricted acts in relation to his work. Primary infringement occurs when any person directly or indirectly does any of these acts. The restricted acts are:-

(i) to copy the work (the reproduction right)
(ii) to issue copies of the work to the public (the distribution right)
(iii) to rent or lend the work to the public (the rental and lending right)
(iv) to perform, show or play the work to the public ('the public performance right')
(v) to communicate the work to the public (the communication right)
(vi) to make an adaptation of the work, or to do any of the restricted acts in relation to the adaptation of the work (the adaptation right)

11. Secondary infringement concerns the commercial use of a copyright work, without the consent of the copyright owner. Such infringement occurs when a person:

(i) imports an infringing copy
(ii) possesses an infringing copy
(iii) sells, exhibits or distributes an infringing copy
(iv) deals with that are used for the making of infringing copies of specific works and
(v) permits premises to be used for an infringing performance or provides apparatus for such performances

12. Primary infringement occurs when the whole or a substantial part of a copyright work is reproduced, whereas secondary infringement occurs when a person, without the licence of the copyright owner, and with actual or constructive knowledge that he or she is infringing undertakes any of the restricted acts which only a copyright owner may undertake.

13. The CPPA 1988 provides both civil and criminal sanctions in respect of copyright infringement. Criminal sanctions will be set out in a separate category. However, civil remedies can be categorised as pecuniary and non-pecuniary. Pecuniary remedies consist of damages or account of profits, whilst non-pecuniary remedies can take the following forms:-

(i) declaratory relief – a declaration of infringement or non-infringement
(ii) delivery up and destruction of infringing goods
(iii) a Court order under Part 31 of the Civil Procedure Rules 1998, whereby an order can be made, providing for disclosure of information such as the name and address of an importer or supplier of infringing goods
(iv) injunctive relief – an interim or final injunction can be ordered, preventing infringing activity – injunctions can also be ordered for

the purpose of searching premises for infringing material, or for freezing infringing activities.

CIRCUMVENTION OF TECHNOLOGICAL PROTECTION MEASURES

14. Modern technology, such as computer games, databases or even certain publications or performances which qualify for protection, can have a technical device such as encryption, digital water marking or digital fingerprinting installed onto it, in order to prevent infringement. An example of this is a code implanted into a play station, which prevents an infringing game being played upon it. These devices, known as technological protection measures, can, however, be circumvented. A technical device is defined in the CDPA 1988. Section 296(b) defines a technical device or any device intended to prevent or restrict copyright restricted acts which are not authorised by the owner of copyrights in the (computer) program. Section 296ZF defines a technological protection measure as any technology, device, or component which is designed in the normal course of its operation, to protect a copyright work, other than a computer program.

15. Under Section 296, certain persons have the right to bring proceedings against anyone who manufactures, supplies or advertises devices or information which enable or assist the circumvention of a technical device applied to a computer program. That right is given to the following persons:

(i) the copyright holder
(ii) an exclusive licensee of the copyright
(iii) a person who issues or communicates to the public, copies of the protected program, and
(iv) the owner or exclusive licensee of any intellectual property rights in the technical device itself

These persons have the right to apply for the delivery up or to have seized, any means for facilitating the unauthorised removal or circumvention of a technical copy protection device, provided that certain conditions are met. Those conditions are that the articles must be on display in a publicly accessible place; the police must be informed beforehand, of the intention to seize the goods, and a notice in the prescribed form must be left at the address from which the articles are seized.

16. Under Section 296ZF, any person other than a cryptology researcher, who does anything which circumvents a technological measure, knowing or having reasonable grounds to know that circumvention is the objective, will be at risk of copyright infringement. The right to bring proceedings is granted to the same person as set out under S.296.

ELECTRONIC RIGHTS MANAGEMENT

17. Electronic rights management, or copyright management, concerns systems for encryption, or for securing electronic material. It may also encompass systems relating to the identification, trading and monitoring of the use of electronic material content, and can be used to manage the distribution and exploitation of material, including copyright works; public

performances; database rights or computer programs. Section 296ZG provides that any person engaged in the unauthorised removal or alteration of rights management information that induces, enables, conceals or facilitates copyright infringement, will be liable, where there is constructive knowledge.

DATABASES

18. A database can be protected under the provisions of the CDPA 1988 as a literary work. A database is defined as a collection of independent works, data or other materials which are arranged in a systematic or methodical way and are individually accessible by electronic or other means. A database is deemed to be original if, by reason of the selection or arrangements of the contents of the database, it constitutes the author's own intellectual creation. The general provisions of the CDPA 1988 apply in relation to the duration of the copyright protection, the rights of the owner infringement.

19. The law provided an additional protection for databases in 1998, following the EU database directive which was implemented in the UK via the Copyright and Rights in Databases Regulations (SI 1997/3032), which amended the CDPA 1988 and prescribed a sui generic right of protection, which is a right granted to the maker of the database against extraction or re-utilisation of the contents of the database. This right applies whether or not the arrangement of the material or the material itself in the database justifies copyright. The database has to be the product of substantial qualitative or quantitative investment, of financial, human or technical resources, in obtaining, verifying or presenting the contents of the data.

20. The database right lasts for 15 years form the completion of the database, or 15 years from the date it becomes available to the public, during that 15 year period. However, any further and substantial investments in adding to, deleting or altering the database result in the 15 year protection period being renewed. The right can be infringed by a person extracting or re-utilising all or a substantial part of the contents of the database. However, repeated and systematic extraction or re-utilisation of insubstantial parts of the contents of the database, may also constitute infringement. The sui generic right, essentially focuses upon the contents of the database as opposed to the organisational structure in order to provide protection where the contents have been wholly re-organised, in circumstances where such re-organisation would not necessarily amount to an infringement of copyright in the original arrangement. The right therefore protects the investment made by the creator of the database.

DESIGN RIGHTS

21. Design rights may be protected via 5 different regimes:

(i) registered designs under UK law (Registered Designs Act 1949)
(ii) registered designs under EU law
(iii) unregistered community design rights arising automatically in respect of registerable designs
(iv) unregistered design rights under UK law
(v) under the CDPA 1988

REGISTERED DESIGNS UNDER UK LAW

22. The law relating to registered designs contained in the Registered Designs Act 1949 was amended by the Designs Directive (98/71/EC). A design under Section 1 of the RDA 1949 is defined as "the appearance of the whole or part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture or materials of the product or its ornamentation". Any aspect of the appearance of a product is potentially registerable. However, functional designs will also be protected, provided that they are not solely dictated by technical function. A product is defined as "any industrial or handicraft item other than a computer program. This definition includes the 'get up' and purchasing of a product, graphic symbols and typefaces. The inclusion of graphic symbols means that loops and character drawings may be registered as well as computer icons.

23. A design may be registered and protected if it is new and of individual character. The RDA 1949 defines novelty as being new, if no identical design or a design differing only in immaterial details, has been made available to the public before the date of the application to register the design. A design will have individual character if "the overall impression it produces on the informed user, differs from the overall impression produced on a user, by an earlier design. An informed user is familiar with the product in question such as a product buyer.

24. The exceptions to registration are: component parts of a complex product, that are not visible during normal use; purely functional designs; designs contrary to morality or public policy and 'must fit' designs which are "features of shape that are required for the product in which the design is incorporated or to which it is applied to be mechanically connected to or placed in, around or against another product, so that either product may perform its function. This exception does not extend to modular systems such as legs.

25. The registered design owner is the designer, or commissioner of the design and he or she has the exclusive right to make, offer, place on the market, import, export, or use as product incorporating the design, or stocking a product for those purposes.

26. The duration of the design right is 5 years from the date of registration, renewable in 5 year periods, for up to 25 years.

27. Infringement of the UK registered design right occurs if a person, without the authority of the registered proprietor does any act which is the exclusive right of the registered proprietor. There are a limited number of acts which do not constitute infringement and which include non-commercial use; experimental and teaching use.

28. The remedies which are available for infringement include damages; injunctions; amount of profits and groundless threats of infringement. However, no damages may be awarded against any innocent infringer.

REGISTERED DESIGNS UNDER EU LAW

29. The Registered Community Design (EC.6/2002 of 12 December 2001 on Community Designs) introduced the Registered (and Unregistered) Community design. The Registered Community design must satisfy the same criteria as for the UK registered design. The substantive requirements and duration mirror that of the UK Scheme. However, the criteria is subject to a one year grace period, which means that disclosures such as the marketing and selling of products made to the design which have been made by the applicant for registration during the 12 months prior to registration are not taken into account in determining whether the product is new and has individual character. The only real difference between the UK and EU registered design is the geographical scope of the protection; with the EU registration protecting the design throughout the European Community.

UNREGISTERED COMMUNITY DESIGNS

30. The Unregistered Community Design Right applies automatically to a design, for 3 years from the date of the first sale or marketing of the design in the EU. The substantive requirements for protection are the same as for the registered design right.

31. The test for infringement is the same as for the infringement of the Registered Community Design, save that there is the additional burden of proving that the infringer actually copied the original design.

32. The ownership of the Unregistered Community Design lies with the designer or his or her employer. Any action for infringement can be brought by the right holder, the exclusive licensee, if the right holder fails to take action against an infringer, or a non-exclusive licensee, with the right holder's permission. The remedies for infringement mirror those for the Registered Community Design. However, the Court will need to be satisfied as to the right holder's title to the design right and the subsistence of the right itself.

UNREGISTERED DESIGNS UNDER UK LAW

33. The Unregistered Design Right under UK law, is conferred by Part III of the CDPA 1988, which was introduced for original designs created on or after 1 August 1989. The design right protects industrial drawings, and is a right which is peculiar to UK law.

34. In order to qualify for protection the design must relate to any aspect of the shape or configuration, whether internal or external, of the whole of any substantial part of an article. Essentially this relates to the three dimensional character of objects or aspects of objects. There is a distinction made between aesthetic and functional design and an unregistered design can be protected even if it only relates to a part of an article which is not placed on the market separately, but which is incorporated into the main article. The design must be recorded in a design document in order to be protected. Alternatively an article must be made to the design, even if it is not in the public domain at that time.

35. To qualify for protection, an unregistered design must be original in the sense that it has not been copied from an existing design; albeit that 2 identical designs can be protected, provided that they are created independently. The design must not be "commonplace in the design field in question at the time of its creation". This criteria does impose novelty on the design, but it must have an aspect to it which 'excites attention'. The exceptions to the design right are methods or principles of construction, surface decoration or must fit, must match designs.

36. In order for the design to quality for protection, the design right holder must be a citizen of the UK, the EU, New Zealand or the Channel Islands or the design must have been initially marketed in one of those qualifying countries. The right holder is the first marketer who holds the design right. Thereafter, the order of priority goes to the commissioner of the design, the employer of the designer then the designer.

37. The term of protection is for 15 years from the end of the calendar year in which the design is recorded. Once articles made to the design are marketed, the right expires 10 years from the end of the calendar year when the articles were first marketed, unless the 15 years term expires first. However, a licence of the design right is available to any person as of right, during the final 5 years of the design right's term. Infringement of the design right occurs primarily by copying the design or dealing commercially with infringing articles.

PROTECTION OF DESIGNS BY COPYRIGHT UNDER THE CDPA 1988

38. Copyright protection remains available for purely decorative features applied to the surface of an article, including three-dimensional features added to an article, purely for decorative effect. Further, any three dimensional object or structure which is classified as an artistic work, such as buildings, sculptures or work of artistic craftsmanship made by a craftsman with interest to produce an artistic piece will attract copyright protection.

39. The copyright protection is limited by Sections S1 and S2 of the CDPA 1988. Section 51 provides that it is not an infringement of any copyright in a design document or model, recording or embodying a design for anything other than an artistic work or a typeface, to make an article to the design or to copy an article made to the design. Design documents are themselves treated as copyright works. S51 of the CDPA 1988 provides that if a copyright work is reproduced by or under licence from the copyright holder in the form of articles made by an industrial process and subsequently marketed, the copyright ceases to be enforceable after 25 years. An industrial process is defined as the production of 50 pieces, or 50 sets, if the design is embodied in a set of articles. The usual term of protection for a copyright protected design is the life of the author plus 70 years; as with other copyright works.

40. UK trade marks are used to act as an indicator of quality and reliability, protecting customers from confusion or deception in the market place and they can be enforced to protect the mark's proprietor against certain acts of unfair competition. The law is contained in the Trade marks Act 1994 (TMA 1994) which implements the Trade marks Directive (No. 89/104/EEC). An application for a national trade mark may be made by

the Trade Mark Registry in the UK Patent Office. It is also possible to apply for a Community Trade Mark (CTM) under the provisions of the Community Trade Mark Regulations (Council Regulations) (EC) No. 40/94). (TM's are registered at the Office of Harmonization for the Internal Market, in Alicante, Spain).

UNDER TMA 1994

41. The definition of a trade mark under the TMA 1994 (S1) is 'a sign capable of being represented graphically, capable of distinguishing goods or services of one undertaking from those of another undertaking'.

A SIGN

A sign includes conventional trade marks such as letters, words, pictures or drawings and 'non conventional trade marks such as slogans; shapes; colours; sensory signs such as sounds; action signs and holograms.

A GRAPHIC REPRESENTATION

A sign must be represented graphically in such a way that a third party can determine and understand what the sign is. The European Court of Justice has set out the criteria in that graphic representations use images, lines and characters which must be clear, precise, self-contained, easily accessible and intelligible, durable and objective. Examples of registerable graphic representations are musical notation for sounds; shades of a colour; rotating earth globes or photographs or line drawings of a shape from different perspectives.

CAPABLE OF DISTINGUISHING

For a sign to be capable of distinguishing the goods and services of one undertaking from that of another undertaking, it is necessary for the trade mark sign to identify the product in respect of which the registration is applied for, and therefore to distinguish the origin of that product.

GROUNDS FOR REFUSAL OF TRADE MARK REGISTRATION

42. A trade mark may be refused registration if it falls within the criteria for either

(i) absolute grounds for refusal or
(ii) relative grounds for refusal

ABSOLUTE GROUNDS FOR REFUSAL

The absolute grounds for refusal of registration are that:

(i) the sign does not satisfy the definitive requirements of SMA 1994
(ii) The mark is devoid of distinctive character
(iii) The sign is exclusively generic
(iv) The sign consists of an unregisterable shape
(v) The mark is likely to offend morals or deceive
(vi) The mark is prohibited by UK or EU law
(vii) The application is made in bad faith

(viii) The mark is a specially protected emblem

RELATIVE GROUNDS FOR REFUSAL

The applicant for trade mark registration must also overcome the relative grounds for refusal, which are:

(i) the mark conflicts with an earlier mark; either a UK CTM, or well known mark (as protected under Article 6 of the Paris Convention of Industrial Property 1883)
(ii) the mark conflicts with an earlier identical or similar mark for identical or similar goods or services, where is likelihood of confusion on the part of the public
(iii) the mark conflicts with a mark of repute and the later mark would take unfair advantage of or be detrimental to the earlier mark's distinctiveness or reputation
(iv) the mark conflicts with earlier rights, including those conferred by copyright, design rights or passing off

LOSING THE TRADE MARK

43. The registration of a trade mark may be lost by surrendering it; or it may be revoked as a result of non-use; or because it has become generic or deceptive. The mark will be invalid if it breaches any of the absolute grounds for refusal. Where no objection has been made by the proprietor of an earlier mark, to the use of a later mark for a continuous period of 5 years, the proprietor of the earlier mark cannot apply for a declaration that the mark is invalid, or oppose its use, unless it is in bad faith. Any person with a 'sufficient interest' can apply to rectify an error or omission in the trade mark register, as long as the rectification does not relate to the validity of the mark.

INFRINGEMENT

44. The registered proprietor of a trade mark and any exclusive licensee has certain rights in relation to the trade mark which are set out in Section 9 of the TMA 1994, and infringed by certain forms of unauthorised use as set out in Section 10. These rights come into existence at the date of filing the registration. All infringing acts require the mark to be used in the UK in the course of trade which is in the context of commercial activities with a view to gaining economic advantage. The infringing acts can be summarised as follows:

(i) using in the course of trade an identical sign for identical goods or services
(ii) using in the course of trade an identical or similar sign on identical or similar goods or services
(iii) using a mark which is similar to a mark of repute for dissimilar goods or services
(iv) contributory infringement, whereby a person who applies a trade mark to certain materials, has actual or constructive knowledge that the use of the mark is not authorised

REMEDIES

45. The remedies available for infringement include damages; account of profits; injunctions; delivery up and destruction of infringing goods, as well as the erasure of the infringing sign. In certain circumstances the threat to bring trade mark infringement proceedings can become actionable. It is also open to the proprietor of a trade mark registered outside the UK to bring injunctive proceedings to restrain the use of identical or similar marks where confusion would result.

COMMUNITY TRADE MARK PROTECTION

46. The provisions of the CTM Regulations closely follows that of the Trade Mark Directive, and subject to minor differences, the provisions for UK Marks and CTMs is broadly similar as regards registerability and infringement. The CTM is protected throughout the EU and therefore has direct applicability within the UK.

INTERNATIONAL TRADE MARK REGISTRATION

47. An international trade mark registration can be applied for, pursuant to the Madrid Agreement concerning the International Registration of Marks, adopted at Madrid on 27 June 1989. The Madrid Protocol allows a mark to be registered in any jurisdiction designated in the application provided that country is a signatory to the Madrid Protocol.

OLYMPIC MARKS

48. The Olympic Symbol etc (Protection) Act 1995 created a right to the British Olympic Society to control the use in the course of trade of certain signs and symbols associated with the Olympics. Similarly, the London Olympic Games and Paralympic Games Act 2006 created a London Olympic Association Right, which prevents any person attempting to claim an association with the 2012 London Olympics without using the specific words or symbols protected by the Olympic Association right. This right prevents any person from using any representation in a manner likely to create an association in the public mind between the London Olympics and his goods or services.

PASSING OFF

49. An IP right is often used to protect business goodwill and trade marks, in the tort of passing off. The traditional elements for passing off are:

(i) The existence of goodwill which is a property right, or "the attractive force that brings in custom". Whilst non profit making professional bodies have successfully established goodwill, such as the British Medical Association, it is usually associated with a legal property right in business. The source of goods or services is vital for establishing goodwill and it is necessary to demonstrate the presence of goodwill through elements such as a mark, logo, name or image created by a business, which makes that business distinctive in the public mind.

(ii) There must be a misrepresentation as to the goods or services offered by the Defendant to the action such as misrepresentation by the Defendant that the goods he sells are those of the Claimant; or that his business is the Claimant's business. There is also misrepresentation where the Defendant has pretended to be an agent for the sale of the Claimant's goods. The misrepresentation should occur at the point of sale

(iii) there must be damage or likely damage to the Claimant's goodwill by diverting trade from the Claimant to the Defendant, or by damaging the Claimant's trade reputation

REMEDIES

The usual remedies are available for passing off and include damages; account of profits; delivery up or destruction; a declaration of infringement or injunctive relief.

CONFIDENTIAL INFORMATION

50. Traditionally, there is no right to privacy under UK law. The Human Rights Act 1998 now recognises a right to privacy, under Article 8 of the European Convention on Human Rights. However, this right must be balanced against the freedom of expression enshrined in Article 10. The balance must be achieved when the Court is determining whether an actionable breach of confidence exists and whether interim injunctive relief should be granted. The Courts appear to be moving towards a situation where the right of freedom of expression is given preference to the right of privacy. A person seeking interim injunctive relief must demonstrate that any interference in the freedom of the press must be justified, for example, when that person is seeking to prevent the publication of alleged confidential information.

ELEMENTS FOR AN ACTION FOR BREACH OF CONFIDENCE

51. The information sought to be protected must have the necessary quality of confidence and must be communicated in circumstances importing an obligation of confidence. There must also be unauthorised use of the information.

THE NECESSARY QUALITY OF CONFIDENCE

The information alleged to be confidential may take any form; photographs; a verbal disclosure; written documentation or a drawing. There is no limitation on the type of information deemed to be protected by the law of confidence, but the most widely protected information consists of:

(i) Commercial or Trade Secrets
(ii) Government Secrets
(iii) Personal Secrets

The information must not be public property or within the public domain; it must be clearly identifiable and sufficiently well developed so as to be capable of realisation.

THE OBLIGATION OF CONFIDENCE

The circumstances which give rise to an obligation of confidence are:

(i) an express contractual term providing an obligation of confidentiality to a contracting party
(ii) a commercial relationship in which an obligation of confidence may be implied
(iii) an employment relationship where duties of confidence are significant, in order to protect trade secrets. In this situation there may be an express term of confidentiality in the employment contract or an implied duty of good faith or fidelity imposed on the employee. There is a duty to protect commercial secrets as well as a duty not to compete unfairly with the employer. An ex-employee is less restricted in that in the absence of an express contractual term, the implied duty of confidence only extends to trade secrets.
(iv) professional relationships, whereby a professional advisor owes a duty of confidence to clients
(v) relevant statutory provisions such as those contained in the Official Secrets Act 1989 and Section 85 of the CDPA 1988 which provides a right to privacy for photographs and films taken for private and domestic purposes

THE USE OF THE CONFIDENTIAL INFORMATION

In general terms, a person who receives information which he knows is confidential is subject to an obligation of confidence. There must be actual or threatened use of the confidential information in breach of the obligation of confidence.

REMEDIES

The remedies for breach of confidence are damages; account of profits; delivery up; modification or destruction and injunctive relief, to include the restraint of use of information from a limited period of time. The 'springboard doctrine' can be used to prevent a person using confidential information as a springboard to launch his own business or project, in competition with, for example, his ex-employer.

IP RIGHTS AND THE INTERNET DOMAIN NAMES

52. The organisation of the internet is governed by the Internet Corporation for Assigned Names and Numbers (ICANN). Internet users are assigned domain names, which serve as descriptors for their internet addresses. A domain name may be registered as a trade mark provided it meets the criteria under the TMA 1994. There is also a national register administered by Nominet for use by EU businesses and persons, whereby a domain name is allocated for a period of time, subject to a fee. Nominet provides a dispute resolution policy in order to deal with allegations of abusive domain name registration. The act of cyber squatting, when well known trade marks are registered by person seeking to make a profit by making false representation that the cyber squatter's domain name is a business connected with a well known enterprise, thereby amounting to passing off or trade mark infringement. The use of a domain name for the

purpose of extracting money from the owners of the goodwill in the well known enterprise, by making express or implied threats that the domain names will be exploited amounts to registering the domain names as instruments of fraud.

COPYRIGHT AND RELATED RIGHTS REGULATIONS 2003

53. The Copyright and Related Rights Regulations 2003 (SI 2003/2498) implemented in the UK, the new IP rights provided by the Copyright Directive (2001/29EC) and the E-Commerce Directive (2000/31/EC) which addressed the legal aspects arising out of electronic commerce in the EU. The 2003 Regulations introduced 2 new rights:

(a) a copyright of electronic communication to the public and
(b) a related right for performers to make available, their performances to the public through on-demand services. These rights were in addition to the new rights given to copyright owners and the manufacturing of technological protection mechanisms prohibiting the circumvention of such mechanisms; or the removal of electronic rights managements information.

54. The 2003 Regulations implemented the protection for internet service providers (ISP's). An ISP is defined as "any person providing an Information Society Service… which is any service normally provided for remuneration, at a distance by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service". The protection offered to an ISP relates to the practice of hosting, and transmitting information, and caching, whereby the ISP sets up a cache, or holding place for copies of remote web sites and which would respond in place of the original web site when a local user attempted to access the remote web site, thereby increasing the speed of web site access. A cache is not a temporary copy and theoretically an ISP could be liable for damages for infringement of the copyright in the original web site. The E-Commerce Directive provided a 'notice and take down' arrangement exonerating the ISP holder from liability for damages provided that upon acquiring actual knowledge of infringing material, the ISP acts promptly to remove it. Similar provisions protect the ISP in relation to hosting or transmitting information. The 2003 Regulations provided the High Court with an express power to grant injunctive relief against an ISP with actual knowledge of a person using its services to infringe copyright or a performer's property right.

COMPUTER SOFTWARE

55. A computer program is now protected under the CDPA 1988 as a literary work; as long as it is recorded in writing or otherwise. The programs can be recorded in coded form and there is no specific definition of the medium in which, or the method by which it is recorded. It will suffice if the program is stored in a computer. The general copyright provisions apply, in that the program must constitute an original literary work. The Software Directive (91/250/EEC) was implemented in the UK by the Copyright (Computer Programs) Regulations 1992 (SI 1992/3233) to a great extent and hence by amending the CDPA 1988.

56. The copyright in a computer program will be infringed if there has been a substantial reproduction of the original, often described as the re-creation of the 'look and feel' of the original program. The Court will undertake an analysis of the actual program content through the source or object code in order to ascertain whether the sequence, structure and organisation of the infringing program amounts to infringement in the absence of direct line by line copying.

57. Certain acts are permitted under the provision of the Directive and the CDPA 1988. The making of necessary back-up copies is permitted as well as decompilation and other reverse analysis (or reverse engineering) for a permitted objective. Decompilation is converting a copy of a computer program expressed in a low level language into a higher level language, or incidentally copying the original program whilst doing so. The permitted objective of decompilation is obtaining the information necessary to create an independent program which can be operated with the decompiled program or with another program.

PATENTS

58. A patent can be described as a grant by a State to an inventor of an absolute monopoly over the exploitation of an innovative technical device or process, for a limited period, in return for a complete written disclosure of how to carry out the invention. This protection has the benefit of encouraging innovation and the commercial exploitation of the innovation in the patent granting State, leading to increased employment and trade. Patent law is contained within the Patents Act 1977 and the Patents Act 2004, which had made a number of amendments to the 1977 Act.

59. A patent is a negative right which prevents third parties from doing any activities within the scope of the patent. An application for a patent must be made to the UK Intellectual Property Office and the application should consider whether the patent protection should be extended within the EU or internationally. There are no legal limitations as to who can apply for a patent but it is usually the person who 'devises the heart of the invention' who can apply for a patent. An employee is generally deemed to be entitled to apply for a patent, unless the invention was made in the course of his normal duties as an employee and the invention might reasonably be expected to result from the carrying out of those duties or if the employee had a special obligation to further the employer's undertaking and the invention was made in the course of those duties, whether or not the invention might be expected to result from the undertaking of those duties. If an employee devises an invention of outstanding benefit to an employer, he may be able to apply for compensation under the 1977 legislation. A commissioner of an invention is not the inventor and subject to express contractual terms, he may only be entitled to an implied licence to use the invention.

60. A patent may be granted for any technological invention; invention being classed as products or processes. The Patent Office or (UKIPO) will undertake a detailed process of examining the patent application or 'specification' and the complete process takes about 2 to 4 years, with a statutory limit of 4½ years, after which the application must be granted or rejected.

61. A patent is usually granted for 4 years, being renewable annually up to a maximum of 20 years upon a renewal fee being paid. A Supplementary Protection Certificate is granted in a limited number of situations whereby veterinary, pharmaceutical and agrichemical industries may delay the marketing process on the basis of compliance with regulations in respect of quality and safety. A patent or patent application may be assigned or licensed. In certain cases a licence of right may be granted.

WHAT IS PATENTABLE

62. The PA 1977 (S.I) provides conditions for patentability, which are that

(i) the device or process is novel
(ii) it involves a non obvious inventive step
(iii) it is capable of industrial application and
(iv) the subject matter is not excluded from patentability

EXCLUSIONS

(i) pure scientific theories or discoveries or mathematical methods
(ii) methods for performing any mental act, playing games or doing business or
(iii) computer programs

INFRINGEMENT

63. Methods of infringement are set out under Section 60 of the PA 1977. Primary infringement occurs as follows:

(i) where a product patent is at issue; making, disposing of, offering to dispose of, using, importing or keeping the patented product (for disposal or otherwise)
(ii) where a process patent is at issue; use of the process with actual or constructive knowledge that non-consensual use constitutes infringement
(iii) using, offering to dispose of, importing or keeping (for disposal or otherwise) a product directly obtained from a patented process.

Contributory infringement is supplying or offering to supply, any of the means that relate to an essential element of the invention, for putting the invention into effect, may constitute infringement. This is the case where there is actual or constructive knowledge that these means are suitable for and are intended for putting the invention into effect.

There are certain exceptions to patent infringement which include private and non-commercial use, or experimental use.

64. A Defendant to a claim for infringement can bring a counterclaim for revocation of the patent, on the following grounds:

(i) the invention is not patentable
(ii) the person granted the patent is not entitled to it
(iii) there is insufficient information or detail in the patent specification
(iv) the protection afforded by the patent has been extended by an impermissible amendment

DETERMINING INFRINGEMENT

65. A great deal of patent litigation is based upon claim interpretation, the process of determining the scope of a patent. An infringing act must fall within the scope of the patent claims and this is difficult to determine where the alleged infringing product or process is a variant of the patented produce or process. The UK Courts take a purposive approach

(i) did the variant have a material affect upon the manner in which the invention works?
(ii) If not, would this have been obvious?
(iii) if yes, would the reader understand that strict compliance with the wording of the invention was required by the patentee?
(iv) if yes, the variant is outside the claim

REMEDIES FOR INFRINGEMENT

66. The civil remedies available for patent infringement are the usual IP remedies of damages; account of profits; delivery up or destruction and a declaration that the patent is valid and not infringed. A declaration, injunction and damages are also available for claims relating to a groundless threat of patent infringement.

Jane Foulser
Barrister, Temple Chambers

IP CRIME

1. Counterfeit goods and pirate copies of music and other performances are merely the tip of the iceberg which constitutes IP infringement. In the ever expanding world of commerce, which extends into all corners of the globe, as a result of the internet and easily accessible and affordable travel services, the economy of the UK, like that of other jurisdictions, is under an increasing threat from IP infringement. The problem is enhanced by the growing sophistication of infringers, who can reproduce computer software at a fraction of the cost of the original or who can have instant access to international designer fashion shows on the internet and reproduce the garments within weeks, using third world labour. The relatively unsophisticated teenager has on average, 800 illegal downloads on their I-Pod according to a recent British Music Rights Group research document.

2. A high level of IP infringement stultifies creativity, by reducing the incentive to create innovate products, which cannot be marketed for their true value if well reproduced copies can retail for a fraction of the price. This, in turn, has a knock on effect on the creation of jobs and national wealth.

3. In July 2008, the G8 Summit discussed proposals for a new Anti Counterfeiting Trade Agreement which would enhance both civil and criminal enforcement procedures, to include the imposition of a fixed fine if a person is found to be in possession of infringing goods and control measures which would provide Customs officials with the power to search for, examine and seize personal electrical equipment with a view to the discovery of infringing material. It remains to be seen whether ACTA will be implemented internationally.

4. The present scope of IP Crime law sanctions in the UK is far more limited and can hardly be described as draconian.

   <u>CRIMINAL PROVISIONS FOR COPYRIGHT INFRINGEMENT</u>

5. The main criminal provisions for copyright infringement are set out under Section 107 of the CDPA 1988. Section 107 provides that it is a criminal offence to do any of the following activities in respect of an article, which the dealer knows, or has reason to believe is an infringing copy:

   (i) make it, for the purposes of sale or hire
   (ii) import it, other than for private and domestic use
   (iii) possess it in the course of a business with a view to carrying out an infringing act
   (iv) sell, let, offer, exhibit, or distribute it, in the course of a business or
   (v) distribute it, even if not in the course of a business, if it is to the extent, that the IP owner's rights are prejudiced.

   The CDPA 1988 also makes it an offence to possess any article specifically designed or adapted to make infringing copies if the holder has actual or constructive knowledge that it will be used for that purpose (S108)

6. A copyright owner can apply to the Criminal Court for the following orders:

(i) an order for delivery up of infringing goods (S108)
(ii) a search warrant for the purpose of the discovery and seizure of infringing goods (S109)
(iii) an order that seized goods can be destroyed or forfeited to the copyright owner (Ss 99, 100, 108, 114)
(iv) an order prosecuting a Company Director for offences under S107 (S.108)
(v) an order under S198 in order to prevent bootleggers from making or dealing with illicit recordings.

7. Section 296 2B makes it an offence to make, or deal with any device, product or component which is designed, produced or adapted for the purpose of facilitating the circumvention of effective technological protection measures. Section 297 and 297 A deal with the offences of fraudulently receiving broadcasted programs and making or dealing with unauthorised decoders. Provision is also made in those sections for search warrants and forfeiture.

8. The penalties for criminal copyright infringement are surprisingly light; usually attracting a fine of up to £5000 and/or a sentence of up to 6 months in the Magistrates Court on Summary Indictment, or a higher fine and up to 2 years imprisonment in the Crown Court for an indictable offence. The exception is to be found under S198(S) of the CDPA 1988, which provides that the criminal penalty for making, dealing with, or using illicit recordings, is a term not exceeding 10 years, on Indictment. This would appear to be an indication that performance rights are afforded a higher priority than other copyright works.

9. Private prosecutions are also available under the CDPA 1988 which is a cheaper alternative than bringing a civil action, against infringers. The Federation Against Copyright Theft (FACT) and the Federation Against Software Theft (FAST) will bring private prosecutions on behalf of the members of those organisations.

CRIMINAL PROVISIONS FOR TRADE MARK INFRINGEMENTS

10. The Trade Marks Act 1994 provides for criminal sanctions in respect of unauthorised use of a trade mark in relation to goods. The main provisions are set out in Section 92, which makes it an offence if:

(i) a person with a view to making a gain for himself or a third party or with interest to cause loss to a third party applies to his goods or their packaging any sign which is identical or similar to a registered trade mark.. It is also an offence to make any commercial dealings with goods or packaging which bear such a sign, or to have such goods within his possession, custody or control. The offence is extended to the application of such a sign to any labelling or packaging of goods; business paper relating to those goods or for the purpose of advertising those goods.

(ii) It is an offence to make an article specifically designed or adapted for making copies of such a sign or to have possession, custody and control of such an article in the course of a business with actual or constructive knowledge that it is to be used to produce goods,

materials for packaging or labelling of goods or for the production of business paper or advertising.

11. In order to obtain a conviction under S92 the trade mark must be registered, with a reputation in the UK, such that the use of the infringing sign takes unfair advantage of, or is or would be detrimental to the distinctive character or the repute of the trade mark. It is a defence under Section 92(4) to show that there were reasonable grounds for belief that the use of the sign in the manner in which it was used was not an infringement of the registered trade mark.

12. The criminal sanctions available in respect of an offence under Section 92 are a fine not exceeding the statutory maximum or a term of imprisonment not exceeding 6 months, on a summary conviction, or a fine and a maximum term of imprisonment for 10 years on Indictment.

13. Other sanctions include the provision to treat any infringing goods, materials or articles as prohibited goods pursuant to Customs and Excise legislation and the provision of search warrants, and forfeiture of infringing goods or materials (Ss 92A and 97). Section 94 makes it an offence to make a false entry in the register of trade marks, with a penalty of a fine or imprisonment for up to 6 months on a summary conviction, or a fine and a maximum 2 year sentence for a conviction on Indictment. Section 95 makes it an offence to represent that a mark is a registered mark or to make false representations as to the goods and services for which the trade mark is registered. The penalty for a conviction under S95 which creates only a summary offence is a fine not exceeding level 3 on the Standard Scale.

14. Section 99 of the TMA 1994 provides a miscellaneous offence of the unauthorised use of the Royal Arms in such a manner as to be calculated to lead to the belief that there is authorisation for such use. The penalty for this offence is a fine not exceeding level 2 of the Standard Scale, upon summary conviction. Section 101 provides for the conviction of Partners and Directors and Officers of Partnerships and Companies under the TMA 1994, where the proceedings for an offence have been brought against those Partnerships or Companies.

15. Similar criminal sanctions apply to infringement of trade marks brought under the Olympic Symbol etc. (Protection) Act 1995, as under the TMA 1994, which also has directly applicability to Community Trade Marks via the Community Trade Mark Regulations 2006.

PATENTS

16. The offences under the Patents Act 1977 are set out in Sections 110 and 111 which provide criminal sanctions in respect of an unauthorised claim that a person has patent rights or an unauthorised claim that a patent has been applied for. These sections prevent a person from disposing for value any product on the false basis that it is subject to a patent or that a patent has been applied for, in relation to it. In relation to both sections, there is a defence that the person has used due diligence to prevent the commission of the offence. Upon summary conviction, the penalty is a fine, nor exceeding level 3 on the Standard Scale.

DESIGN

17. The criminal sanctions for infringement of design rights pursuant to the CDPA 1988, are the same as for other copyright works, and the substantive offences are set out in Sections 107 to 114B.

REGISTERED DESIGNS

18. The Registered Design Act 1949 contains provision under Section 33 (or Section 35A for a corporate body) for the imposition of a fine following summary conviction for falsely representing a design as being registered. Such a fine will not exceed level 3 on a Standard Scale. There is also a provision under that Section for the imposition of a fine not exceeding level 1 for the false implication that a design is registered, if that design has been subject to registration which has since expired.

DATABASES

19. The general criminal provisions in the CDPA 1988 apply in respect of databases.

DOMAIN NAMES

20. There is authority that a domain name can be used as an instrument of fraud for the purpose of extracting money from the proprietor of a registered trade mark *BT Plc and Others –v- One-in-a-Million Ltd [1998] FSR 265. [1999] 1 WLR 903.* However, there are no specific criminal sanctions arising from abusive domain name registrations.

PASSING OFF

21. The tort of passing off attracts an award of damages or other relief under general common (civil) law and there are no criminal sanctions available.

BREACH OF CONFIDENTIAL INFORMATION

22. There are no criminal sanctions specifically available for a breach of confidence as confidential information is not classed as property for the purposes of criminal law. The Data Protection Act 1998 Section 55 sets out a series of criminal offences in respect of data theft. There are 5 key offences within Section 55, which are

    (i) obtaining personal data or the information stored in personal data
    (ii) disclosing personal data, or the information contained in personal data
    (iii) procuring the disclosure of information contained in personal data
    (iv) selling personal data and
    (v) offering to sell personal data

    There must be actual knowledge or recklessness as to the absence of the data controller's consent.

    The Criminal Justice and Immigration Act 2008, Section 77, provides the criminal penalty for an offence under Section 55 of the DPA 1998; that penalty being, upon summary conviction, the maximum fine or term of imprisonment (level 5 fine or 12 months imprisonment; and upon Indictment, a period of 2

years imprisonment or a fine. Personal data consists of data, or information which relates to a living individual who can be identified. The DPA 1998 does not provide specific criminal sanctions for breach of confidential information in an IP context.

THE VIDEO RCORDINGS ACT 1984

23. The Video Recordings Act 1984 sets out 5 offences under Sections 9-11 and 13 and 14. This legislation was introduced to ensure that all video works were labelled and classified. The Video Recordings (Labelling) Regulations 1985, made pursuant to Section 8 of the VRA 1984, provide for the positioning and clarity of labels and markings for videos, CD's and DVD's. The offences under the VRA 1984 were:

    (i) supplying a video recording of unclassified work which attracts a custodial sentence of up to 6 months and/or a fine of up to £20,000 upon summary conviction, or a sentence of 10 years and for a fine upon Indictment
    (ii) possessing a video recording of unclassified work, for the purposes of supply, which attracts a summary only penalty of 6 months imprisonment or a fine of up to £20,000
    (iii) supplying a video recording of unclassified work, for the purposes of supply, surprisingly only attracts a summary penalty of 6 months imprisonment or a fine of up to £5000
    (iv) supplying a video recording not complying with requirements as to labels, attracts a summary fine of up to £5000 and summary
    (v) supplying a video recording containing a false indication as to classification attracts a summary sentence of up to 6 months or a fine of up to £5000.

THE FRAUD ACT 2006

24. The Fraud Act 2006 provides an offence of fraud, committed in 3 different ways, which are:

    (i) fraud by false representation
    (ii) fraud by failing to disclose information
    (iii) fraud by abuse of position

    The penalty for a conviction is imprisonment for a term of up to 12 months or a fine not exceeding the statutory maximum £5000) or both, following a summary conviction, or imprisonment for a term not exceeding 10 years or a fine, or both, following conviction on Indictment. The Act creates further offences of making or possessing articles for use in or in connection with fraud and making or supplying articles for use in fraud.

25. The Fraud Act 2006 can be used to control IP infringement by using its provisions to bring charges against any person selling counterfeit goods or by the, manufacture, provision, use or sale of chipping or copying equipment. A charge of fraud by false representation can be brought against a person falsely applying a trade mark to goods.

PROCEEDS OF CRIME ACT 2002

26. The Proceeds of Crime Act 2002 makes provision for the recovery and confiscation of assets acquired by a person as a result of pursuing a criminal lifestyle. The amount of assets recoverable is an amount equal to that person's benefit from the criminal conduct concerned. Schedule 2(7) to the Act provides that offences under the CDPA 1988 or the TMA 1994 are criminal lifestyle offences, and conviction under these Acts may result in an order for the recovery of assets pursuant to the POCA 2002, which, if used extensively in practice, could act as a disincentive to IP infringement.

TRADING STANDARDS

27. The Trade Descriptions Act 1968 prohibits the application of false trade descriptions to goods and prohibits false or misleading statements as to services, accommodation or facilities provided in the course of trade. It also confers power to require information or instructions to be marked on goods or included in advertisements. This law is primarily concerned with the application of trade marks; trade descriptions; the use of particular emblems; badges; uniforms; assaying and hallmarking and approval marks under the Road Traffic Act 1988. The general penalty under the Trade Descriptions Act 1968, is a fine not exceeding the statutory maximum, following summary conviction, or a fine or a term of imprisonment not exceeding 2 years, following conviction on Indictment.

THE SERIOUS ORGANISED CRIME AND POLICE ACT 2005

28. The Serious Organised Crime and Police Act 2005 (SOCPA 20050 confers investigatory powers on the Direction of Public Prosecutions; the Director of Revenue and Customs Prosecutions and the Lord Advocate in relation to giving disclosure notices in connection with certain listed offences, including 'lifestyle offences' under the Proceeds of Crime Act 2002. These offences include offences under the CDPA 1988 and the TMA 1994. Their powers can be delegated to 'appropriate' persons, including Police Officers; members of the Serious Organised Crime Agency and HM Revenue and Customs Officials.

29. Under Section 62 of the Act the investigating authorities can serve disclosure notices on any person, where they have reasonable grounds for believing that a relevant offence has been committed, that the person has documentary or other information relating to a matter that is relevant to the investigation, and that information will be of substantial value to the investigation. The disclosure notice can require the named person to answer questions; provide specified information and produce documents. Section 66 of the Act gives Magistrates to power to issue search warrants which allow the investigating authority to enter and search premises, using reasonable force if necessary. The warrant also authorises the seizure of computer disks and other forms of electronic storage and to take steps to preserve electronic data. The Act provides a useful tool in combating IP crime in that it will allow information to be obtained by the authorities in relation to the existence and whereabouts of infringing goods and materials and to illicit information about persons involved in infringing activities. The power to allow for the seizure of digital data, is a useful tool in combating computer crime.

SERIOUS CRIME ACT 2007

30. The Serious Crime Act 2007, which includes IP Crime, pursuant to the CDPA 1988 and the TMA 1994 under Schedule 1 Part 1 Paragraph 12, provides that the Court can make a Serious Crime Prevention Order under Section 1, where it is satisfied that a person has been involved in serious crime in England, Wales, Northern Ireland or elsewhere and there are reasonable grounds to believe that the order would protect the public, by preventing, restricting or disrupting involvement by that person in serious crime, within the jurisdiction.

31. The standard of proof applicable to the making of these orders is the Civil Standard, that being, the balance of probabilities. The duration of the orders is for a maximum of 5 years. Section 5 of the Act contains a list of the type of prohibitions, restrictions or requirements which can be imposed by the order albeit the list is not exhaustive. The conditions include, conditions relating to:

    (i) a person's financial, property or business dealings or holdings
    (ii) a person's working arrangements
    (iii) a person's means of communication
    (iv) premises to which a person has access
    (v) a person's travel arrangements
    (vi) restrictions on a person's ability to enter into agreements
    (vii) the provisions of goods and services to a person or
    (viii) the employment of staff by such a person

    Conditions may also be imposed requiring a person to answer questions, or provide specified information.

    The Act also contains provisions providing for asset recovery; and an extension of the investigatory powers of HM Revenue and Customs.

32. The recent, Serious Crime legislation will assist in the prevention of IP Crime, in that the Courts have the power to inhibit the criminal lifestyle of IP infringers, as well as putting effective measures in place to recover assets accrued as a result of infringing activity.

Jane Foulser
Barrister, Temple Chambers

E COMMERCE LAW

1. The modern world has become a dotcom society and E Commerce is thriving and will continue to thrive with the advancement of technology. There are many businesses which operate purely as internet operations as well as businesses which operate a web site for purchasers to have the benefit of their products without the need to travel to the flagship store. An example of a pure E Commerce business is the designer emporium known as net-a-porter.com; where designer clothing is purchased online only.

2. The legislative provisions which have been introduced to deal with the new era of E Commerce cover the protection of intellectual property rights; the removal of monopolies and anti-competitive restrictions and the legal recognition and protection of electronic contracting.

DISTANCE SELLING

3. The Distance Selling Directive 1997 (97/7/EC) protects consumers in relation to distance contracts. The Directive does not cover financial services, which are protected by the Financial Services Distance Selling Directive (2002/65/EC); sale via vending machines; automated commercial premises or contracts in relation to real property. The exceptions are fully set out in Article 3(1).

4. Distance selling is defined in Article 2(1) as "a 'distance contract' means any contract for goods or services concluded between a supplier and a consumer under an organised distance sales or services provision scheme run by the supplier, who, for the purposes of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded". Distance communication is defined in Annex 1 of the Directive, but effectively covers sales which take place without the buyer and seller being in physical proximity to each other. Obvious examples are contracts made via e-mail or via online web sites.

5. The Directive provides the following benefits for consumer protection:

   (i) Transparency in Service Provision (Articles 4 and 5)

   The Directive stipulates that certain information must be provided by the seller to the buyer, prior to the conclusion of the contract. The information includes the name and address of the seller; the characteristics of the goods and services; the price, including taxes; delivery costs; delivery arrangements; details of the right to withdraw from the contract; the cost of using distance communication; the period for which the price remains valid; the minimum duration of the contract in respect of products or services. The information must be presented in a clear and concise way and must conform with the principles of good faith. This information can be provided orally or in writing. Once the contract has been concluded, the seller must provide, in writing or other durable medium, information about cancellation rights and procedures; the address for any complaints; after sales and guarantee information and the cancellation procedure for contracts of unspecified duration or for contracts lasting in excess of 1 year.

   (ii) Withdrawal, Cooling Off or Cancellation

The Directive gives the buyer a minimum of 7 working days in which to withdraw or cancel the contract; running from the date of receipt of goods to conclusion of a service contract. If the post contract information has not been provided in accordance with Article 5, the cooling off period is 3 months or 7 days from the date it is provided. Certain contracts are exempt from the cancellation rights and include the supply of personalised goods; contracts for newspapers, magazines or periodicals; gaming and lottery services; the supply of CD's or software which have been stripped of their protective seal by the buyer; or service contracts where performances began within the cooling off period; or where the contract relates to the supply of goods and services depending on fluctuating prices.

(iii) Performance

Article 7 provides for a maximum period of 30 days for the performance of the contract, unless a different period is specified in the contract. Any refund made for a failure to perform the contract must be made as soon as possible or within 30 days.

(iv) Prevention of Payment Card Fraud

Article 8 requires Member States to comply with the directive in relation to card fraud, by implementing measures to ensure that buyers can cancel any payment that has been fraudulently made, and to have their cards re-credited.

(v) Unsolicited Communications-Restrictions on the Use of Automated Calling Systems

Article 10 prevents sellers from using automated calling systems and faxes without the prior consent of the buyer.

THE AVAILABILITY OF JUDICIAL REDRESS

(vi) Article 11 requires Member States to implement measures to ensure that the interests of buyers are protected by the availability of judicial and administrative redress, through public bodies, consumer groups or professional organisations. The burden of proof may be shifted to the seller, to show that he has complied with the directives.

THE FINANCIAL SERVICES DISTANCE SELLING DIRECTIVE 2002

6. The Financial Services Directive 2002 (2002/65/EC) relates to "distance selling in respect of financial services, defined as any service of a banking, credit, insurance, personal pension, investment or payment nature". Articles 3 and 5 correspond with the provisions of Articles 4 and 5 of the Distance Selling Directive, save that the provisions are more detailed. The provisions of Articles 6 to 11 can be summarised as follows:

(i) Withdrawal

Article 6 contains the right to withdraw from the contract within 14 days save for a period of 30 days which is the cooling off period relating to life insurance and personal pensions. The relevant period commences from the conclusion of the contract, or from the date when the buyer is informed that the contract for life insurance has been concluded. If the seller has

not supplied the information required by the Directive, the cooling off period begins when it is provided. Certain contracts are exempt from the right of withdrawal and these relate to the supply of financial services, where the financial markets dictate the price; travel and baggage insurance or short-term insurance (up to 1 month); or contracts which have been performed at the buyer's request, prior to the exercise of the right of withdrawal. Additional exemptions may be made in respect of any credit extended in relation of land or building renovation; the provision of a mortgage or declaration by a buyer via the services of an official person.

(ii) Articles 7, 8 and 9 provide for sellers to charge for services provided prior to withdrawal as long as they are proportionate in relation to the contract price as a whole, and do not constitute the imposition of a penalty (Article 7). Article 8 provides for payment and fraud protection similar to that contained within the Distance Selling Directive and Article 9 prohibits unsolicited financial services. Articles 10 and 11 also provide similar provisions relating to the Distance Selling Directive, insofar as they relate to unsolicited communications and judicial and administrative redress. The latter provision requires Member States to implement sanctions which are "effective, proportional and dissuasive" in respect of the non-compliance of contractual terms by the seller.

HOW ARE THE DIRECTIVES ENFORCED IN THE UK

7. The UK has implemented the following Regulations:

(i) Consumer Protection (Distance Selling) Regulations 2000 (S.I. 2000/2334) (amended by S.I. 2005, SI 2005/689) and
(ii) Financial Services (Distance Marketing) Regulations 2004, (S.I. 2004/2095) (amended by S.I. 2000/2334)

8. These Regulations adopt the provisions of the Directive save for some minor, or additional amendments. The Distance Selling Regulations require the seller to provide the buyer with a notice, proposing any substitution of goods (Reg. 7) and Regulation 10 sets out the cancellation provisions which include the right to cancel in writing or in another durable medium such as fax or e-mail. Regulations 15 to 19 deal with the automatic cancellation of related credit agreements, the payment of interest on cancelled contracts; the restoration of goods provided in part exchange and the performance period, which is 30 days from the day following the date on which the order is placed. The Financial Services (Distance Marketing) Regulations 2004 provides that the information and cancellation provisions do not apply to an 'authorised person', being a person authorised by the Financial Services Authority, pursuant to the Financial Services and Markets Act 2000.

THE E-SIGNATURES DIRECTIVE 1999

9. The E-Signatures Directive 1999 (1999/93/EC) was introduced to deal with the issue of data authenticity in order to allow the free movement of goods and services within the EU via new technology without compromising the necessary security required for commercial translations. The Directive effectively facilitates the use of electronic signatures and provides for their legal recognition.

10. The Directive makes provisions for 3 types of electronic signatures

    (i) electronic signature (Article 2(1)) defined as 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'
    (ii) Advanced electronic signature (Article 2(2)) which is defined as being an electronic signature meeting certain requirements. Those requirements are that the signature is uniquely linked to the signatory, and is capable of identifying the signatory. It must be created using a means which the signatory can maintain under his sole control and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. An advanced electronic signature is the product of signature creation data such as codes or private cryptographic keys used by the signatory to create his unique mark. The requirements for a secure signature creation device are set out in Annex III of the Directive.
    (iii) A qualified Certificate (Article 2(10)) is a Certificate provided by a Certification-Service-Provider (a natural person or legal person) who issues Certificates or other services relating to electronic signatures. The requirements for such a Certificate are set out in Annex I of the Directive and they must contain 10 provisions:

        (a) an indication that the Certificate has been issued as a qualified Certificate
        (b) the identification of the Certification-Service-Provider and the State in which it is established
        (c) the name of the signatory or a pseudonym
        (d) provision for a specific attribute of the signatory if relevant
        (e) signature verification data
        (f) the validity period of the Certificate must be identified
        (g) the identity code of the Certificate
        (h) the advanced electronic signature of the Certificate-Service-Provider, issuing it
        (i) any limitation on the scope of the Certificate
        (j) any limitation on the value of transactions for which it is used

11. The legal effects of electronic signatures are set out in Article 5 and Member States must ensure that

    (i) advanced electronic signatures based on a qualified Certificate created by a secure-signature creation device, satisfy the legal requirements of a signature in relation to data in electronic form, in the same way as a handwritten signature would
    (ii) such signatures are admissible as evidence in legal proceedings
    (iii) electronic signatures must not be denied legal effectiveness and admissibility in evidence solely on the ground that it is in electronic form; not based upon a qualified Certificate; not based upon a qualified Certificate issued by an accredited – Certification-Service-Provider or not created by a secure signature-creation device.

12. An electronic signature has the same legal effect as a standard handwritten signature and the Directive has implemented measures to ensure that Certification-Service-Providers comply with the appropriate data protection legislation and are liable to persons suffering damage as a result of relying upon an inaccurate Certificate.

UK LEGISLATION IMPLEMENTING THE E-SIGNATURE DIRECTIVE

13. The E-Signature Directive was implemented in the UK via the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002 (S.I. 2002/318). The ECA 2000 provides for the legal effect of electronic signatures and the ESR 2002 deal with the implementation of the definitions and annexes of the Directive, especially in relation to free trade; liability and data protection. The ECA 2000, Section 7 provides that electronic signatures shall be admissible in legal proceedings in the same way as a normal signature.

THE E-COMMERCE DIRECTIVE 2000

14. The E-Commerce Directive (2000)31/EC) was implemented to encourage the use of Information Society Services and electronic commerce throughout the EC. Services such as e-mail and e-commerce are promoted by the protection of consumers and the imposition of legal validity of electronic signatures in e-commerce agreements. The Directive recitals note that many economic transactions now occur on line and include the sale of goods; information disseminated over the network and e-mail communication. In summary, the Directive covers "any service normally provided for remuneration at a distance, by means of electronic equipment and at the individual request of a recipient of a service".

15. The Directive protects the interests of internet service providers and this is already dealt with in paragraph 5 S3 and S4 of Paper 1. In summary where an ISP is acting as a storer of information or a 'mere conduct' of such information they are excluded from civil and criminal liability provided that the ISP acts to remove illegal or infringing material from the network once it has actual or constructive knowledge of the presence of such material.

16. The Directive sets out provisions for transparency in the provision of services provided by ISP's and these provisions apply to both consumer and non-consumer services. The information required under Article 5 includes the name, address, VAT number, professional details and information about their inclusion in a trade or public register. Articles 6, 7 and 8 concern the information which must be provided to ensure that any commercial communications contain clearly identifiable information and details and Articles 10 and 11 deal with electronic contracts and the necessity for contracting parties, especially the buyer, to be provided with clear information in relation to the concluding of contracts. Article 9 entitled 'Treatment of Contracts' provides that Member States legislate to allow contracts to be concluded by electronic means and to have such contracts recognised as being legally valid and effective.

UK IMPLEMENTATION OF THE E-COMMERCE DIRECTIVE

17. The E-Commerce Directive has been implemented in the UK, by the Electronic Commerce (EC Directive) Regulations 2002 (S.I. 2002/2013 as amended by S.I. 2003/115; S.I. 2003/2500 and S.I. 2004/1178). These Regulations mirror the provisions of the Directive, save for some minor additional amendments which include a provision that it is a breach of statutory duty for a service provider to breach the provisions of the Regulations in relation to transparencies; the rules governing commercial

communications; unsolicited commercial communications; information regarding the technical steps for concluding a contract and acknowledgement of orders. There is provision for the Court to award damages for such breaches and to ensure compliance with the rules. The Court has the power to prevent issue orders against service providers to prevent IP infringement and the buyer has the right to rescind an agreement where certain rules have been breached.

18. The effect of the Distance Selling Directive and the E-Commerce Directive is to ensure that both consumer and non-consumer issues are protected in relation to electronic interaction. There is effectively no distinction between the operation of a traditional enterprise and an electronic based enterprise for the purposes of legal recognition, validity and enforcement. It remains to be seen whether these legislative provisions will have the effect of undermining the traditional business, whilst promoting internet based operations.

GENERAL CONSUMER LAW

SALE OF GOODS ACT 1979

19. The main legislation applicable to the Sale of Goods in the UK is the Sale of Goods Act 1979 (SOGA 1979) which has been amended by the Enterprise Act 2002. The corresponding legislation in relation to the Supply of Goods and Services, is contained within the Supply of Goods and Services Act 1982 (SOGASA 1982). The basis for this legislation is contract, with the necessity for offer and acceptance, a clear definition of the goods being sold, monetary consideration, capacity to contract, and clear and unambiguous contractual terms and conditions. There is an obligation upon the seller to deliver the goods which have been contracted for, to the buyer in accordance with the terms of the contract. Property, possession and risk in relation to the goods, passes from the seller to the buyer in accordance with the rules set out in Section 18 of SOGA 1979.

IMPLIED TERMS

20. The SOGA 1979 implies certain statutory terms into a contract for the sale of goods and these are:

(i) implied terms as to title (S12)
(ii) implied terms where there has been a sale by description (S13)
(iii) implied terms as to quality or fitness for purpose (S14)
(iv) implied terms where there has been a sale by sample (S15)

In essence, these implied terms provide that the seller has the right to sell the goods at the time when the title in the goods is to pass to the buyer; goods must correspond to any description given of them by the seller and the sale of goods to a buyer will correspond to any sample of those goods shown to a buyer, in that they will be of a similar quality to the sample and free from any defect which would not be apparent on a reasonable examination of the sample. The goods sold must be of satisfactory quality and fit for their purpose. This implied term means that the goods must be fit for the purpose for which goods of the kind are commonly supplied; they must be satisfactory in appearance and finish; be free from minor defects and be safe and durable.

21. In consumer contracts made after the implementation of the Enterprise Act 2002, there are provisions which protect the buyer, where the seller is in breach of the main contractual provisions. The main provisions are as follows: (S48-54)

    (i) If the goods do not conform to the contract at any time within 6 months of delivery they are taken not to have conformed at the date of delivery unless it is established that they did conform and the burden is on the seller. There is an exception for perishable goods. If the goods do not conform, there is a breach of and express term of the contract or of the statutory implied terms. The seller is required to repair or replace the goods within a reasonable time, without inconvenience to the buyer and at the cost of the seller. There is also provision for a reduction in the purchase price to be offered to the buyer. Additionally the Court has the express power to make an order for specific performance; reimbursement damages and otherwise as it thinks fit

    (ii) Where there is non delivery of the goods, the buyer is entitled to damages; special damages; interest or specific performance. A wrongful refusal by the seller to perform his obligation under the contract, will amount to a repudiatory breach allowing for the payment of damages, specific performance or a claim in restitution. Similarly, a wrongful re-sale by the seller or a loss of goods attract similar sanctions.

22. There are obligations placed upon the buyer under the SOGA 1979, and it is the buyer's duty to accept the goods and pay for them in accordance with the terms of the contract. A late payment will attract simple interest and a failure to accept the goods places the buyer at risk of a claim for damages for non-acceptance.

23. Where a seller attempts to sell goods to a buyer, in circumstances where he does not have the title to pass in those goods, he cannot pass a good title in the goods to the buyer, save when the situation falls within certain exceptions, set out under SOGA 1979 Section 21, 23, 24, 25, 62. The Hire Purchase Act 1964 (Part III) and Torts (Interference with Goods) Act 1977, Section 5. Generally the law protects an innocent purchaser acting in good faith buying goods for valuable consideration without notice of the seller's lack of title.

UNFAIR CONTRACT TERMS ACT 1977

24. The Unfair Contract Terms Act (UCTA 1977) prevents contractual terms or notices which exclude or restrict liability for personal injury or death being effective at all (S2(1). Other loss or damage can only be excluded or restricted insofar as the Clause satisfies the test of reasonableness (S2(2). Knowledge of or agreement to any such term is not of itself to be taken as indicating any acceptance of risk (S2(3)). Once a contractual term has been accepted as a valid term of the contract there can be no exclusion or restriction of liability by one party, where the other party deals as a consumer, or on the other party's written standard terms of business, unless the term satisfies the test of reasonableness (S3(2)(a)). Schedule 2 of UCTA 1977 sets out the guidelines in respect of the matters to be considered in determining reasonableness. These matters include the strength of bargaining positions of each party; any inducement offered to the buyer; where the buyer ought reasonably to have known about the term; whether the

Clause comes into play if a condition is complied with, or whether the goods were manufactured processed or adapted to the special order of the customer. In general, the test of reasonableness is that the term must have been a fair and reasonable one to have been included in the contract, having regard to the circumstances which were, or which ought reasonably to have been known to, or in the contemplation of the parties. The burden of proof is on the person claiming that the Clause is reasonable.

25. Certain contracts are excluded from the provisions of the UCTA 1977 (Sch 1) and these include contracts relating to intellectual property.

CONSUMER CREDIT

26. Consumer Credit Agreements are covered by the Consumer Credit Acts of 1974 and 2006. The classes of Consumer Credit Agreements covered, include loans; overdrafts; credit cards; charge cards; hiring; hire purchase; conditional sales agreements; credit sales and chattel mortgages. The legislation provides for credit agreements not exceeding £25,000 and in summary it sets out obligations upon creditors and debtors in relation to the conclusion of the agreement; the information to be provided to the debtor; liability for breaches of the agreement by the creditor; liability of the other debtor to make payments; interest payable; early settlement; termination and termination statements. The County Court has exclusive jurisdiction to deal with all proceedings under the 1974 legislation. The important provisions relate to the regulation of extortionate credit and the power of the Court to re-open extortionate credit bargains (S137 to 140) and 'unfair relationships' between creditors and debtors (S140A to 140D). The Court has the power to determine that the relationship between the contracting parties is unfair to the debtor. Guidance is given under Section 140A(1), however the Court is to have regard to all matters it considers relevant and this new Court power which is extremely wide, can be invoked by the debtor on application or during enforcement proceedings by the creditor.

27. The Consumer Credit legislation is very detailed and the Distance Selling Regulations 2000 have direct applicability to e-commerce. It is not, therefore, necessary to explore this legislation in any great detail.

Jane Foulser
Barrister, Temple Chambers

E CRIME

1. The scope of E Crime law within the UK, encompasses legislative provisions which have already been dealt with in, such as the Serious Organised Crime and Police Act 2005, which provides for the recovery of computer disks and the preservation of electronic data. The Serious Crime Act 2007 provides for orders restricting the lifestyle of offenders involved in serious crime, as well as providing a regime for asset recovery, to supplement the provisions of the Proceeds of Crime Act 2002.

2. The substantive legislation for E Crime is contained in the following legislative provision:-

   (i) The Data Protection Act 1998
   (ii) The Regulation of Investigatory Powers Act 2000
   (iii) The Computer Misuse Act 1990
   (iv) The Malicious Communication Act 1988
   (v) The Communication Act 2003
   (vi) The Public Order Act 1986
   (vii) The Protection from Harassment Act 1997

   <u>THE DATA PROTECTION ACT 1998</u>

3. The DPA 1998 only provides for a limited category of criminal offences, the most prominent offence being 'data theft' under Section 55 of the Act. The 5 key offences are:

   obtaining, disclosing or procuring the disclosure of personal data or the information contained in personal data; or selling or offering to sell personal data. The person stealing the data must have actual knowledge or be reckless as to the absence of the data controller's consent. A data controller is the national or legal person who determines the purpose for which and the manner in which personal data are to be processed.

4. Section 1(1) of the DPA 1998 defines 5 categories of data which are:

   (i) information that is being processed by means of equipment operating automatically in response to instructions given for that purpose; which effectively means data held on computers or computer controlled equipment

   (ii) information that is recorded with the intention that it should be processed by means of equipment that operates automatically, which describes information that will be held on a computer or on computer controlled equipment at some time in the future. This encompasses information that has been transferred from a computer to a DVD or CD, or a handwritten note awaiting typed entry onto a computer

   (iii) information that is recorded as part of a relevant filing system, such as in a database or manual information awaiting storage in such a system

(iv) information which forms part of an accessible record such as health or education records

(v) recorded information held by a public authority

These categories cover electronic transference of information, such as e-mails and information put into a computer and transmitted over the internet for the purposes of trading via web sites such as e-bay or private on-line retailers. The personal data concerned is data relating to an individual who can be identified and includes information such as an identification number, bank account details, or details specific to a person's physical, mental, cultural or economic identity. Such information can be used to obtain credit; goods or services fraudulently and can be obtained with relative ease; to the detriment of the individual from whom and about whom it has been taken.

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

5. The Regulation of Investigatory Powers Act 2000 (RIPA 2000) Section 1, provides an offence of unlawful interception of a communication during the course of its transmission over a public telecommunications system. This includes transmission by means of a public postal service. Interception is defined as 'making the contents of a communication available to a person other than the sender or intended recipient whilst in the course of transmission. A telecommunications system means any system including the apparatus comprised in it which exists, wholly or partly in the United Kingdom or elsewhere, for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. This definition encompasses computers and telephones used in private or business premises.

6. The interceptions must be intentional and without lawful authority provided as a result of an interception warrant or the consent of the sender and the intended recipient. The penalty is a term of imprisonment not exceeding 2 years or a fine, following conviction on Indictment, or a fine not exceeding the statutory maximum (£5000) following summary conviction.

7. The RIPA 2000 provides for the education of criminal liability in certain narrow circumstances under Section 1(b) where the interception of a communication, in the course of transmission, is made by means of a private telecommunications system, if the interceptor is the person with the right to control the operation or the use of the system or he has the express or implied consent of such a person, to make the interception. The RIPA 2000 provides protection for information which is transmitted via e-mail or during a telephone conversation or via computer transactions.

THE COMPUTER MISUSE ACT 1990

8. The Computer Misuse Act 1990 (CMA 1990) creates a series of offences that protect against the unauthorised access to computer material, unauthorised acts that impact upon the operation of computers and the use of computers to commit other crimes. There is no definition of a 'computer' within the Act which may result in devices such as I-phones, coming within the scope of the Act, as well as lap top or desk computing equipment.

9. Section 1 of the CMA 1990 sets out the offence of unauthorised access to computer material. A person is guilty of such an offence if:

   (i) he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secure
   (ii) the access he intends to secure or to enable to be secured is unauthorised, and
   (iii) he knows at the time when he causes the computer to perform the function that this is the case

   There is no requirement for the person committing such an offence to direct his interest at any particular program or data; or a program or data of any particular kind; or a program or data held in any particular computer.

10. A person secure access to any program or data held in a computer, if by causing a computer to perform any functions he

   (i) alters or erases the program or data
   (ii) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held
   (iii) uses it, or
   (iv) has it output from the computer in which it is held (whether by having it displayed or in any other manner

   A person uses a program if the functions he causes the computer to perform, causes the program to be executed or is itself a function of the program

   A program is output if the instructions of which it consists are output and the form in which any instruction or other data is output is immaterial.

   The access to the program or data held in a computer is unauthorised if the person gaining the access is not entitled to control that kind of access to the program or data and he does not have the consent of the person with the control of the access to do so. The accessory person must have actual knowledge that the access is unauthorised. The penalty for an offence under Section 1 of the CMA 1990 is a term of imprisonment not exceeding 6 months fine and/or not exceeding level 5 following summary conviction.

11. Section 2 of the CMA 1990 provides for an offence of unauthorised access to a computer with intent to commit or facilitate the commission of further crimes, which are described as an offence for which a sentence is fixed by law or the offence is one for which a person aged 21 years or over may be sentenced to imprisonment for a term of 5 years, or might be so sentenced (subject to the provision of Section 33 of the Magistrates Act 1980). An offence may be committed under Section 2, even if the commission of the further offence is impossible. Following conviction on Indictment the penalty is a term of imprisonment not exceeding 5 years and/or a fine, or up to 6 months or a find not exceeding the statutory maximum, following summary conviction.

12. Section 3 of the CMA 1990 covers the offence of unauthorised modification of computer material. The offence is committed if a person does any

unauthorised act in relation to a computer, knowing or being reckless as to its authorisation. The unauthorised acts are:

(i) impairing the operation of any computer
(ii) preventing or hindering access to any program or data held in any computer
(iii) impairing the operation of any such program or the reliability of any data; or
(iv) enabling any of the aforementioned acts to be done

As with Section 1, the Act does not have to relate to any particular computer, program or data, or a program or data of any kind.

The penalty following summary conviction is a term of imprisonment for a term not exceeding 12 months and/or a fine not exceeding the statutory maximum. Upon conviction on Indictment, the maximum sentence is 10 years and/or a fine.

13. The CMA also provides for an offence of making supplying or obtaining articles for use in an offence under Sections 1 and 3. The same summary penalties apply as for an offence under Section 3, but following conviction on Indictment the maximum sentence is 2 years, and/or a fine. There is also provision in the Act for search warrants.

14. The CMA 1990 provides for the possibility of a person being convicted for turning on a computer, an act which causes a program to be 'executed' within the meaning of the Act, and which may result in a person committing an offence by having the intent to secure unauthorised access, without actually gaining access to data. This Act has been used to secure a conviction against a person who gained access to a computer to obtain a large discount on goods that he was purchasing. The CMA 1990 is a useful tool in the prevention of E Crime in that it prevents the fraudulent manipulation, deletion or alteration of data for the purpose of fundamental gain especially in the context of on-line retail or marketing. Section 3 of the Act has been used in the situation where an ex-employee tampered with 3 Company web sites operated by an ex-employer.

<u>THE MALICIOUS COMMUNICATIONS ACT 1988</u>

15. The Malicious Communications Act 1988 (MCA 1988) provides a criminal offence arising out of the sending of hate mail, to include e-mail. Section 1 of the Act provides that any person who sends to another person a letter, electronic communication or article of any description which conveys

(i) a message which is indecent or grossly offensive
(ii) a threat, or
(iii) information which is false and known or believed to be false by the sender, or any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature, is guilty of an offence, if his purpose, or one of his purposes, in sending it, is that it should (so far as it falls within the provisions, under Section 1) cause distress or anxiety to the recipient or any other person to whom he intends that it or its contents or nature, should be communicated.

16. There is a defence to the offence if the person shows that the threat was used to reinforce a demand made by him, on reasonable grounds and that he believed and had reasonable grounds for believing that the use of the threat was a proper means of reinforcing the demand. The penalty for this summary only offence is a term of imprisonment for up to 6 months and/or a fine not exceeding level 5.

THE COMMUNICATIONS ACT 2003

17. The Communications Act 2003 (CA 2003) also contains offences intended to deal with hate mail. Section 127 provides that the offences include sending, or causing to be sent, grossly offensive, indecent, obscene or menacing communications over the public network, which encompasses e-mails. It is also an offence to send false messages for the purpose of causing annoyance, inconvenience or needless anxiety and it is an offence to persistently use the network for these purposes. The penalty on summary only conviction is 6 months imprisonment or a fine up to level 5 or both. This legislation has been described as a method of prohibiting the use of public communications system for the transmission of communications that contravene the basic standards of society. Such communications would impart upon, in particular the use of e-mail correspondence.

THE PROTECTION FROM HARASSMENT ACT 1997

18. The Protection From Harassment Act 1997 (PHA 1997) provides under Section 1 that a person must not pursue a course of conduct which amounts to harassment of another, and which he knows or ought to know, amounts to harassment of the other. Section 1A prohibits a person from pursuing a course of conduct involving 2 or more persons with the requisite intention of persuading any person not to do something that he is entitled or required to do, or to do something that he is not under any obligation to do. The Court must be satisfied that a reasonable person would think that the course of conduct amounted to harassment. The defences are that the conduct was pursued for the purpose of detecting or preventing crime, or that it was pursued under a rule of law, or in compliance with a condition or requirement or that the conduct was reasonable in the circumstances. The criminal penalty under Section 2 of the Act is a term of imprisonment for up to 6 months, and/or a fine not exceeding level 5, as the offence is summary only.

19. Section 4 of the PHA 1997 provides an offence of putting in fear of violence as a result of a course of conduct on at least 2 occasions. The requisite intent and defence are the same as under Section 2. The criminal sanctions provide that following a conviction on Indictment, the maximum term of imprisonment is 5 years and/or a fine with summary conviction attracting the same penalty as an offence under Section 2 of the Act. The PHA 1997 may be used to prevent harassment of a person via e-mail or using other internet facilities such as Facebook.

OTHER SIMILAR OFFENCES

20. It is possible for the internet or e-mail to be used to intimidate persons or to stir up racial hatred or religious harassment. The relevant provisions are contained in the following legislation

THE PUBLIC ORDER ACT 1986

21. Section 21 of the POA 1986 provides that it is an offence to distribute, show, or play a recording of visual images or sounds which are threatening, abusive or insulting, with the intention of stirring up racial hatred, or if having regard to all the circumstances racial hatred is likely to be stirred up thereby. Section 23 of the Act provides an offence of possessing written material, or a recording of visual images or sounds which are threatening, abusive or insulting, with the same effect of stirring up racial hatred.

22. The POA 1986 provides for powers of search and entry and forfeiture of such material and the penalty is a term of imprisonment for up to 7 years and/or a fine, following conviction on Indictment, or a term of imprisonment for up to 6 months and/or a fine, not exceeding the statutory maximum upon summary conviction.

23. The aforementioned legislative provisions in Section 3 of this paper comprise the main areas which are applicable to E Crime in the context of the use of computers and computer related activities such as the transmission of e-mails.

DISHONESTY OFFENCES

24. The basic definition of theft is set out in Section 1 of The Theft Act 1968 and in the "dishonest appropriation of property belonging to another with the intention of permanently depriving that other of it". The Theft Act 1968 has been repealed to an extent, by the Fraud Act 2006, which has been dealt with, in paragraph 24 of Part 2 of this paper, insofar as it relates to the basic definition of fraud.

25. Section 11 of the Fraud Act 2006 (FA 2006) provides an offence of obtaining services dishonestly, on the basis that payment has been, is being, or will be made for those services. The penalty following a summary conviction is a term of imprisonment not exceeding 12 months and/or a fine not exceeding the statutory maximum and upon conviction on Indictment, the penalty is a fine and/or a maximum sentence of 5 years. Sections 9 and 10 of the Act provides offences of participating in a fraudulent business by a sole trader, or a Company, the penalty being the same as for an offence under Section 11, save that following conviction on Indictment the maximum sentence is 10 years. This offence applies to persons who are outside the ambit of the Companies Act 2006 (S.993) for the purposes of charging them with the offence of fraudulent trading, and it covers the situation where a person knowingly carries on a business, with intent to defraud creditors or any person for any other fraudulent purpose.

26. The Fraud Act 2006 will cover situations relating to dishonest activity in e-commerce such as offering stolen goods for sale via the internet or being involved in a business whereby rock concert tickets are offered for sale by a person or Company dishonestly, on the basis that the tickets are not available for sale, or the seller does not have a legal title to them and cannot therefore sell them.

27. The Theft Act 1968 is still in force in relation to offences of blackmail (Section 21), handling stolen goods (S22), or advertising rewards for the return of goods stolen or lost (S23). The penalty for blackmail and handling is a term of imprisonment not exceeding 14 years, following conviction on Indictment, and an offence of advertising rewards for lost or stolen goods is a fine not exceeding level 3 upon summary conviction.

Jane Foulser
Barrister, Temple Chambers

RELEVANCE FOR WELSH SMEs

E CRIME AND THE SME – THE THREATS

1 IDENTITY THEFT

A particularly prevalent criminal activity is that of identity theft. Identity theft refers to the illicit gain and use of another individual's personal and financial information in order to commit a variety of frauds such as the raising of illegitimate finance or committing a crime in the name of an unrelated individual / business. Identity theft includes mail theft, stealing from residences and the theft of information from business / organisational premises held on electronic storage devices.

One of the many problems associated with identity theft is that given the increasing trend of storing sensitive information on computer hardware, victims may not be aware of the fraud until weeks, months or even years later, by which time the information has been exploited by the criminal(s) and it is difficult to resolve the financial fall-out.

2 ONLINE TRADING

With the growth of on-line trading and the increasing use of electronic data storage devices, it is becoming increasingly common for businesses to fall victim to E Crime.

When a business trades on-line, it generally uses a web site to accept orders and credit card details from the customers. The order is processed without the need of the customer to enter the store or use the telephone and the customer does not need to show or swipe the credit card. Because of this, on-line trading can be referred to as "card not present transaction" and different businesses have different options as to how they conduct their on-line trading, for example some businesses may operate solely on the internet or combine internet activities with an existing store.

On-line credit /debit card fraud occurs when:

a. A customer fraudulently submits credit /debit card details over the internet as payment for goods ordered. The action is fraudulent in that:
    i. The use of the card is unauthorised
    ii. The card details have been obtained fraudulently
    iii. The card is legitimate, but the cardholder claims to have not ordered the goods (received) so as to claim a refund (and keep the goods) or obtain replacement goods.

b. Financial information input into the businesses data-handling system is intercepted (at any point) and used for criminal purposes. The threat may come from in-house (employees) or from criminals who "hack" the system to obtain the information

SMEs trading on-line can suffer serious financial hardship if they are the victim of on-line fraud, for when a retailer does not see the credit card or signature and does not swipe the card through any EFTPOS Terminal, as in

internet trading, financial institutions are unwilling to accept the heightened risks associated with on-line trading. This means that the SME will usually bear the costs of on-line credit card fraud.

3. PAYMENT CARD FRAUD

Payment card fraud is a major component of identity theft and is a significant threat to businesses, financial institutions and consumers, with the most prevalent form being counterfeit credit card fraud. In many cases, organised crime uses portable card skimmers that read and capture the data contained on the card's magnetic strip. The stolen card's information is then re-encoded onto a blank magnetic card which is either used directly by the criminal to drain the victims account, or sold on the black market.

Businesses must be aware that not only may they fall victim to such a scheme directly in terms of their own business credit card account, but that they also have an obligation to ensure the safety of their customers' information whilst it is in their custody. It is therefore vital that businesses put in place measures to protect against both external and internal (employee) threats to the businesses own information and that of its customers.

4 PHISHING

An increasingly popular form of internet related fraud is "phishing". This involves deceptive emails that impersonate legitimate institutions and lure recipients into divulging their personal financial information, such as credit card numbers or internet banking passwords.

It may also entail password detecting / decrypting software to illicitly capture encryptive passwords transferred over networks. Some spyware is designed to steal information, for example through key stroke – logging software. It is well known that criminals are increasingly targeting smaller financial institutions or commercial enterprises that perhaps do not have the sophisticated protection mechanisms in place to combat the crime.

<u>THE CONSEQUENCES OF E CRIME FOR THE SME</u>

As stated above, the consequences for all parties affected by E Crime are considerable:

- Victims of E Crime can suffer financial loss and / or be left with damaged credit ratings and disrupted personal and financial records; and

- Businesses either negligently or sometimes innocently providing the information to such criminals, will lose the trust of their clients and the business sector in which they work, as well as having the administrative burden of "clearing up" the security breach; and significantly

- In terms of on-line credit card fraud, losses from fraudulent on-line purchases are borne primarily by the small business itself, rather than credit card companies or financial institutions.

It is vitally important therefore that as part of any business development strategy, SMEs must expend time and resources a) identifying the risk to their

business from the taking of confidential information/know how and b) developing prevention and detection mechanisms.

THE EXTENT OF THE PROBLEM

Unfortunately for the SME, E Crime is a moving feast in that the tactics used by the criminals are constantly updated to keep ahead of protection offered by software vendors.

Efforts to combat the problem are hampered further by the fact that there is no central registry which records specific details pertaining to E Crime. This means that the charting of trends nationally and internationally so as to develop policies and practices that can fluidly adapt to the issue is difficult.

Exacerbating this problem is a finding that SMEs do not take precautions against E Crime until they become a victim. Yet one incident of fraud pre-exposes one business to another, so the effect of a single fraud can be felt by many more businesses than the primary victim of the crime.

PREVENTATIVE STRATEGIES

There are practical steps which can be taken to reduce the likelihood of a business becoming a victim of E Crime:

A. Secure the Business Computer Network:

The business computers and network must be secured. This can be achieved by:

1. installing password authentication software to protect business information, which is regularly updated;

2. installing and regularly updating antivirus software;

3. use encrypting software to convert transaction information into unreadable code.

4. Installing a firewall – software which identifies and rejects external threats to the system

B. Prevent business information from being stolen

Businesses need to be aware that there are two sources of threat: external threats; and internal threats.

External threats can be minimised by adopting the strategies mentioned herein. Internal threats are threats from dishonest employees and these can be minimised by careful vetting of staff; restricting staff access to information; ensuring staff sign employment contracts containing confidentiality clauses and where appropriate, non-competition clauses.

C. Set minimum identification requirements for credit card orders over the internet & screening of internet orders generally

As part of the protection exercise, SME's should be encouraged to put in place good working practices to help identify the potential for E Crime. For example, members of staff should be asked to conduct manual screening measures on all internet transactions when confirming orders, this not only raises awareness of the issue amongst staff, but also assists in identifying fraud at an early stage which can help minimise loss.

D. Be wary of unsolicited emails;

E. Wipe the hard drive of the computer before disposing of the computer; and

F. Obtain and maintain insurance against the risk posed by E Crime.

ENFORCEMENT ISSUES

If an SME should fall victim to E Crime, recovering / mitigating the loss will be dependent upon acting quickly and obtaining legal advice.

Recovering loss can be achieved via the criminal courts or the civil courts. In either instance, the court will require evidence of loss to be produced and produced in the correct format. It is therefore vital that property records are properly maintained – software should be installed to both maintain the information and quickly identify / produce reports when E Crime is suspected.

The practical steps a business can take include:

1. Ensure that its procedures and business computer system can establish the time and author of the record and provide details of any alterations made to the record;

2. Establish procedures for obtaining records; and

3. Ensure that employees who design, produce, correct, analyse and present IT evidence, have the appropriate training, experience and qualifications.

Stephen Clarke
Dr Kerry Beynon
Clarke and Hartland Solicitors

CONCLUSION

EXPOSURE TO RISK

Whilst the Information Security Breaches Survey 2008 identified real improvements undertaken by businesses to protect themselves against virus attack and hacking, it proffered the warning that confidential information remains a big exposure increasingly at risk. This warning has particular resonance with large businesses which had detected: 13% unauthorised outsiders within their network, 9% had fake (phishing) emails asking their customers for data, 9% had customers impersonated (e.g. identity theft), 6% have suffered a confidentiality breach, 10% of web sites that accept payment details do not encrypt them, 21% spend less than 1% of their IT budget on information security, 35% have no controls over staff use of instant messaging, 48% of disaster recovery plans have not been tested in the last year, 52% do not carry out any formal security risk assessment, 67% do nothing to prevent confidential data leaving on USB sticks etc., 78% of companies that had computers stolen did not encrypt hard discs, 79% are not aware of the contents of BS 7799/ISO 27001, 84% of companies do not scan outgoing email for confidential data.

AWARENESS RAISING

There may be web sites presently available offering advice and guidance to SMEs on what to do when faced with E Crime and how to manage the threat posed by the same (getsafeonline and evictims.org being two such examples). However, there is a stark absence of a co-ordinated approach which can only serve to alienate SMEs and prevent the community from adequately recognising, prioritising and dealing with the issue. Moreover, as already stated above, SMEs do not generally address the issue of E Crime until they have become a victim of it. Thus, these web sites, whilst containing a wealth of information, largely serve those who have already suffered from E Crime, as opposed to proactively raising awareness amongst the general SME business community.

EASY ACCESS TO GOOD ADVICE

Awareness is but a first step and the need for protection at an affordable cost is paramount in supporting the growth of Welsh SMEs trading on-line. The Welsh SME business community requires immediate and direct access to expert and professional advice at an early stage, both in terms of implementing mechanisms to reduce the threats posed by E Crime and in terms of reporting incidences of E Crime to a body that can adequately advise on the next steps in dealing with the same.

APPENDICES