



Intellectual Property Counsel



E-Commerce

---

**Manchester**

7 November 2002

**Bradford**

13 November 2002

**Mr. John Lambert**

**Dr. Alex Khan**

**Kingsgate Chambers**

Intellectual Property and Technology Group

Kingsgate House  
51-53 South King Street  
Manchester  
M2 6DE  
**DX** 710297 *Manchester 3*  
**Tel** +44 (0)161 831 7477  
**Fax** +44 (0)161 832 5645  
**Email** [clerks@KingsgateChambers.co.uk](mailto:clerks@KingsgateChambers.co.uk)  
**Web site** [www.nipclaw.com](http://www.nipclaw.com)

## Course Programme

Time	Speaker	Topic
2:00 - 2:30	John Lambert	<p><b>Introduction and welcome</b></p> <ul style="list-style-type: none"> <li>- What is electronic commerce and why does it require special treatment?</li> <li>- What are the legal issues?</li> <li>- How are these issues being tackled?</li> </ul> <p>UNCITRAL Models Laws on E-Commerce and Electronic Signatures</p> <p>EC Directives on distance selling, digital signatures and e-commerce</p> <p>Implementation in the UK</p> <p>Electronic Communications Act 2000 and Regulation of Investigatory Powers Act 2000</p>
2:30 - 3:00	Alex Khan	<p><b>The EC Legislative Framework</b></p> <p>Distance Selling</p> <p>Electronic Signatures</p> <p>Electronic Commerce</p> <p>Data Protection</p>
3:00 - 3:15	<b>Refreshments</b>	
3:15 - 4:00	John Lambert	<p><b>Electronic Commerce (EC) Regulations 2002</b></p> <p>What are "Information Society Services"</p> <p>What services are covered</p> <p>Information that information society service providers must give</p> <p>Enforcement of regulations</p> <p>ISP and telecommunications operators' liability</p> <p>Dispute resolution</p>
4:00 - 4:30	John Lambert	<p><b>Domain Name Disputes</b></p> <p>Domain name system</p> <p>ICANN and country code registrars</p> <p>Methods of resolving domain name disputes:</p> <ul style="list-style-type: none"> <li>- UDRP, Nominet and litigation</li> </ul> <p>Preparing a case for WIPO</p> <p>Preparing a case for Nominet</p>
4:30 - 4:45	<b>John Lambert and Alex Khan</b>	<b>Questions and Answers</b>

## Speakers Details



### **John Lambert**

Barrister, FCIArb and Accredited Mediator

Born in Manchester and educated at St Andrews University and UCLA. He read for the bar after a spell in the City and was called in 1977. After pupillage he practised in Lincoln's Inn for several years. In 1983 he became in-house legal advisor to VISA International for Europe where his work included computer and telecommunications law competition and trade marks. In 1985 he returned to Manchester to specialize in IP and technology law. In 1988 he became a tenant of a London patent set and was in several important early software protection and computer supply cases. He established NIPC in Lancaster Buildings in 1997 initially as an annexe of his London patent set. It later became the first IP set outside London. Since he has been in Manchester he has appeared in cases on threats, obviousness and circuit designs. He was also one of the first English counsel to use the ICANN UDRP. A fellow of the CIARB since 1992 and now an accredited mediator he will accept instructions to act as a mediator and neutral in technology cases. He was on the NCC legal panel and is a member of the IP and Chancery Bar Associations.



### **Alex Khan**

Barrister with expertise in Biotechnology

Dr Alex Khan was John Lambert's pupil. Another native Mancunian he was educated at Leicester Polytechnic, UMIST and Birmingham University where he did his doctorate in biotechnology. He read law at the University of Central England and was called to the bar by Lincoln's Inn. He has published numerous scientific and legal articles. While practising all aspects of IP, technology, media and competition law he intends to specialize in patents and plant varieties.

# 1. Introduction and Welcome

## 1.1. Definitions

1.1.1. The e-commerce team of the Information Society Directorate-General of the European Commission suggests the following definition:

"any transaction that involves an on-line commitment to purchase or to sell a good or service, and that results in the import or export of this good or service."

The WTO General Council's definition<sup>1</sup> is slightly broader:

"the term "electronic commerce" is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means."

1.1.2. It is an aspect of *electronic business* which covers all other electronic transactions such as customer relations management, fund transfers, logistics management, securities trading, stock purchasing and so forth.

1.1.3. E-business is itself an aspect of the *information society* which includes all sorts of non-commercial transactions such as delivery of central and local government services, education, entertainment and health care by electronic media.

## 1.2. Characteristics of Electronic Commerce

1.2.1. **Scale:** Despite the .com bust<sup>2</sup> over the last few years e-commerce remains a fast growing business activity. The Census Bureau of the US Department of Commerce<sup>3</sup> estimates that U.S. retail e-commerce sales for the second quarter of 2002 increased by 24.2%<sup>4</sup> from the second quarter of 2001. By contrast, the general retail sector grew by only 2.5 percent<sup>5</sup> over the same period.

<sup>1</sup> [http://www.wto.org/english/tratop\\_e/ecom\\_e/wkprog\\_e.htm](http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm)

<sup>2</sup> There are signs that the bust has begun to level out. *Webmergers.com* charted the number of closures of e-commerce websites between June 2000 and June 2002 as follows:

	Jun	Jul	Aug	Sept	Oct	Nov	Dec	Jan	Feb	March	April	May
2000-2001	17	20	10	22	36	50	49	56	59	49	56	64
2001-2002	61	40	46	33	36	21	23	19	18	17	12	14

Source: *Webmergers.com* ([www.webmergers.com](http://www.webmergers.com))

<sup>3</sup> [www.census.gov](http://www.census.gov)

<sup>4</sup> The Bureau reports a margin of error of plus or minus 5.5%.

<sup>5</sup> Margin or error of plus or minus 0.4%

1.2.2. **Global:** Websites can be hosted anywhere, and accessed from almost anywhere. Although there are still cultural, regulatory and logistical barriers to trans-national marketing, suppliers are no longer limited to traditional markets. The other side of the coin is that the technology that opens up new markets also exposes suppliers to new competition within their home markets.

1.2.3. **Automated:** Most e-commerce sites are open for business 24 hours a day, 365 days a year. Many transactions take place without any direct human intervention giving rise to all sorts of challenges in marketing, logistics and security. The downside is that the prodigious capacity of modern computer systems to acquire, store, collate and disseminate data challenges privacy.

1.2.4. **Paperless:** Transactions may be completed without the need for paper records or the exchange of signatures. The problem for most legal systems is that some transactions have to be made or evidenced in writing.

### 1.3. Legal Issues

These are many and various and this selection should not be regarded as exhaustive.

1.3.1. **Jurisdiction:** Because a website may be accessed almost anywhere, an important question is whether it should be subject to the law of every place where it may be accessed. One view is that if a supplier aims his products or services to the world it is not unreasonable for him to comply with local consumer protection, intellectual property and other laws. The competing view is that it is impossible to take legal advice on the laws of every jurisdiction and to keep abreast with changes in the law.

1.3.2. **Enforcement:** A related issue is cross-border enforcement of obligations. Many consumer claims are for small amounts that do not justify the costs of cross-border litigation. That, however, can be a barrier to e-trade because consumers are unlikely to purchase goods or services unless they are sure they can obtain swift and cost-effective redress if things go wrong.

1.3.3. **Authentication:** The Internet is global and users are anonymous. How can a trader be sure that the person with whom he is dealing over the Internet is the person with whom he intends to deal?

1.3.4. **Security:** Governments have conflicting interests in protecting technical and business secrets and the privacy of individuals on the one hand and preventing and detecting crime and anti-social behaviour on the other. Occasional access to encrypted material is essential for law enforcement and regulation but the potential for abuse is obvious. A challenge to legislatures around the world is to strike a balance between those conflicting public interests.

1.3.5. **Intellectual Property:** Intellectual property rights are essentially territorial while the Internet is global. How can IPR be protected and enforced across national frontiers, particularly as some countries provide actions for groundless threats of infringement proceedings?

1.3.6. **Competition:** National and regional markets were regulated by national and regional anti-trust laws, but the Internet is global.

1.3.7. **Tax:** How far can tax authorities take into account revenues generated electronically by off-shore subsidiaries? Should value added tax be levied on cross-border sales and if so how is it to be collected? How should digitized goods such as music or software downloaded from a website be taxed?

#### 1.4. The International Context

1.4.1. Although every country has its own national interests to protect, inter-governmental collaboration is essential for harmonization of e-commerce law. Collaboration is taking place at the following levels:

1.4.2. **UNCITRAL**<sup>6</sup>: The United Nations Commission on International Trade Law ("**UNCITRAL**") was established by the UN General Assembly on 17 December 1966 with a mandate to further the progressive harmonization and unification of international trade law. UNCITRAL has 6 working groups one of which is Working Group IV on Electronic Commerce<sup>7</sup>. This working group has produced two model laws on electronic commerce for adoption by national legislatures:

- **UNCITRAL Model Law on Electronic Commerce**<sup>8</sup> adopted on 16 December 1996; and
- **UNCITRAL Model Law on Electronic Signatures**<sup>9</sup> 12 December 2001.

---

<sup>6</sup> <http://www.uncitral.org/>

<sup>7</sup> [http://www.uncitral.org/english/workinggroups/wg\\_ec/index.htm](http://www.uncitral.org/english/workinggroups/wg_ec/index.htm)

<sup>8</sup> <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>

<sup>9</sup> <http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf>

1.4.3. **European Community:**<sup>10</sup> European governments individually and collectively attach enormous importance to the development of the information society and, in particular, e-commerce. EC initiatives are co-ordinated by the Information Society Directorate-General. The Council has adopted directives to harmonize national law that address many of the above issues including, in particular:

- **The Distance Selling Directive:** Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts;<sup>11</sup>
- **The Electronic Signatures Directive:** Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures;<sup>12</sup> and
- **The Electronic Commerce Directive:** Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular e-commerce, in the Internal Market.<sup>13</sup>

1.4.4. Each of those important directives has now been implemented at least partially in the UK. These are by no means the only Community initiatives. There is important EC legislation in competition, consumers' rights, data protection, intellectual property, jurisdiction, monetary union, taxation and telecommunications regulation, all of which affect the development of e-commerce in Europe.

## 1.5 UK Legislation

Ever since the present government came into power, its avowed objective has been to make the UK one of the world's leading knowledge economies. Its strategy includes providing an environment for electronic trading by 2002 and identifying and removing all existing regulatory and legal barriers to electronic ways of working. So far, it has passed 2 important pieces of primary legislation:

### 1.5.1. **Electronic Communications Act 2000:**

regulates cryptographic services, provides for electronic signatures and allows for the amendment of other legislation by statutory instrument to accommodate paperless transactions; and

### 1.5.2. **Regulation of Investigatory Powers Act 2000:** provides a statutory basis for the monitoring and interception of electronic communications.

<sup>10</sup> [http://europa.eu.int/information\\_society/index\\_en.htm](http://europa.eu.int/information_society/index_en.htm)

<sup>11</sup> [http://europa.eu.int/ISPO/ecommerce/legal/documents/31997L0007/31997L0007\\_en.html](http://europa.eu.int/ISPO/ecommerce/legal/documents/31997L0007/31997L0007_en.html)

<sup>12</sup> [http://europa.eu.int/information\\_society/topics/ebusiness/ecommerce/](http://europa.eu.int/information_society/topics/ebusiness/ecommerce/)

<sup>8</sup> [policy\\_elaw/law\\_ecommerce/legal/documents/1999\\_93/1999\\_93\\_en.pdf](http://europa.eu.int/policy_elaw/law_ecommerce/legal/documents/1999_93/1999_93_en.pdf)

<sup>13</sup> [http://europa.eu.int/ISPO/ecommerce/legal/documents/2000\\_31ec/2000\\_31ec\\_en.pdf](http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf)

These statutes are complemented by the Competition Act 1998, Data Protection Act 1998 and the Human Rights Act 1998.

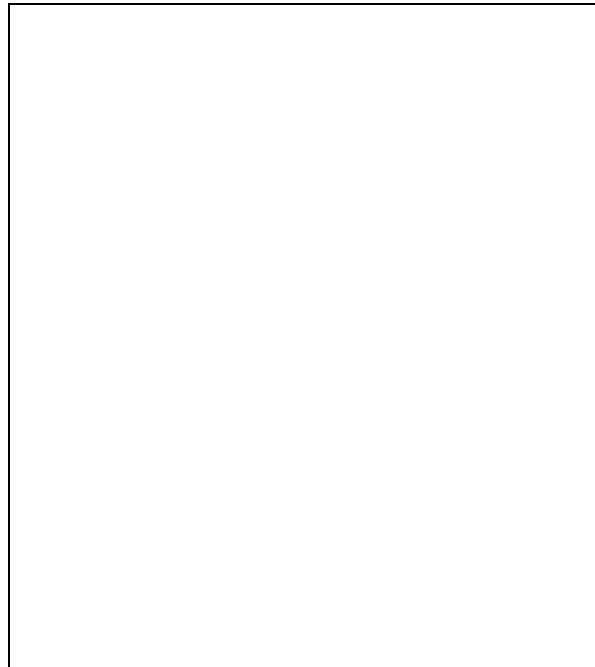


1.5. **Other International Drivers**

1.5.1. **World Trade Organization ("WTO")**:<sup>14</sup> In 1988 the WTO General Council established a comprehensive work programme to examine all trade-related issues relating to global electronic commerce covering trade in goods and services, intellectual property and trade and development.

1.5.2. **Organization for Economic Co-operation and Development ("OECD")**<sup>15</sup>: The OECD has carried out research and published material on tax, trade and development related to e-commerce.

1.5.3. **The World Intellectual Property Organization ("WIPO")**<sup>16</sup> is a UN agency charged with administering various intellectual property conventions and co-ordinating national intellectual property laws. It has various interests in e-commerce which are amplified in its publication *Primer on Electronic Commerce and Intellectual Property Issues*.<sup>17</sup> The WIPO Arbitration and Mediation Centre provides domain name dispute resolution services.



1.6 **Non-Governmental Initiatives**

It is important to note initiatives by the internet community in establishing procedures for the resolution of generic and country code top level domain name disputes. These are models for resolving other trans-national business to business and business to consumer disputes.



---

<sup>14</sup> [http://www.wto.org/english/tratop\\_e/ecom\\_e/ecom\\_e.htm](http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm)

<sup>15</sup> <http://www.oecd.org/EN/about/0,,EN-about-29-nodirectorate-no-no-no-29,00.html>

<sup>16</sup> <http://ecommerce.wipo.int/index.html>

<sup>17</sup> <http://ecommerce.wipo.int/primer/index.html>

## 2. EC Legislation

Dr. Alex Khan

### 2.1. Introduction

This paper concentrates on the following areas of Community legislation in so far as they affect e-commerce:

2.1.1. distance selling

2.1.2. electronic signatures

2.1.3. electronic commerce, and

2.1.4. data protection.

These are not the only areas for which there is EC legislation affecting e-commerce. Other matters include, but are not limited to jurisdiction, trade marks, non-contractual obligations and IP.<sup>1</sup>

### 2.2. Distance Selling

2.2.1. **Definition:** The Commission offers the following definition<sup>2</sup>:

"the conclusion of a contract regarding goods or services whereby the contact between the consumer and the supplier takes place by means of technology for communication at a distance. The '*distance*' element means that the two parties do not meet face to face."

It catches catalogue shopping and other forms of mail order as well as e-commerce.

2.2.2. **Legislative Initiatives:** The Distance Selling Directive<sup>3</sup> was adopted in 1997 and has already been implemented in the UK. A further directive for distance marketing of financial services<sup>4</sup> has been proposed by the Commission and endorsed by the European Parliament.

2.2.3. **Distance Selling Directive:** This directive was adopted by the Council on 20 May 1997 and came into force on 4 June 1997. It is implemented in the UK by The Consumer Protection (Distance Selling) Regulations 2000.<sup>5</sup>

<sup>1</sup> A good gateway to this legislation is the Information Society D-G's e-commerce site at [http://europa.eu.int/information\\_society/topics/ebusiness/ecommerce/index\\_en.htm](http://europa.eu.int/information_society/topics/ebusiness/ecommerce/index_en.htm)

<sup>2</sup> Commission Press Release IP/97/495 of 5.6.97 Brussels, 5 June 1997

[http://europa.eu.int/comm/consumers/policy/developments/dist\\_sell/dist02\\_en.html](http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist02_en.html)

<sup>3</sup> Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in respect of Distance Contracts

<sup>4</sup> [http://europa.eu.int/comm/consumers/policy/developments/fina\\_serv/fina\\_serv07\\_en.pdf](http://europa.eu.int/comm/consumers/policy/developments/fina_serv/fina_serv07_en.pdf)

<sup>5</sup> SI 2000 No. 2334

2.2.4 **Main Provisions:** consumers must be provided with clear and comprehensible information concerning:

- identity and address of the supplier;
- characteristics and price of the goods or services;
- delivery costs;
- arrangements for payment, delivery or performance;
- the consumer's right of withdrawal;
- a cooling-off period for which an offer or price remains valid and the minimum duration of any contract, where applicable;
- the cost of using the means of distance communication,

before entering any distance selling contract.

Consumers must also receive written confirmation at the time of performance of the contract together with information about:

- how to exercise their right to withdraw;
- where to address complaints;
- after-sales service; and
- conditions for rescinding the contract.

Each consumer has the right to withdraw from most kinds of distance selling contracts. Suppliers have 30 days in which to perform their obligations under distance selling contracts. Should a supplier fail to do so, he must inform the consumer and offer to refund his money. Where unsolicited goods are supplied, failure to respond does not constitute consent to an agreement.

2.2.5. **Draft Directive on Distance Marketing of Financial Services:** The distance selling directive excludes from its scope contracts relating to financial services. The following draft directive is intended to fill that lacuna. Its main provisions are:

- banning inertia selling - that is to say, pressing consumers to pay for services they have not ordered;
- restricting unsolicited phone calls and e-mails;
- requiring service providers to supply consumers with comprehensive information before entering a contract; and
- a cooling-off period for consumers.

### 2.3. Electronic Signatures

An electronic signature is data that identifies a particular user of a telecommunications system. It may take the form of a password, pin number, scanned signature, digital representation of a retina or fingerprint or data generated by cryptographic means.

**2.3.1. Electronic Signatures Directive:**<sup>6</sup> This directive came into force on 19 January 2000. Art. 13 (1) required implementation by 19 July 2001. The directive was implemented in the UK partly by the Electronic Communications Act 2000 and partly by The Electronic Signatures Regulations 2002.<sup>7</sup>

**2.3.2. Validity of Electronic Signatures:** Member states are required by art. 3 (1) (a) to ensure that *advanced electronic signatures* - that is to say those that are uniquely linked to a signatory and capable of identifying him, are created by means that are under the signatory's sole control and are linked to data in such a way that any alteration of such data is detectable - satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data. Such signatures must also be admissible in evidence.

**2.3.3. Certification Licensing:** Member states must ensure the establishment of an appropriate system for supervising agencies that certify advanced electronic signatures in accordance with guidelines annexed to the directive ("**certifying service providers**")<sup>8</sup>.

**2.3.4. Liability of Certifying Service Providers:** Anyone who suffers loss or damage through relying on a certificate that proves to be inaccurate may recover damages for such loss from the certifying service provider unless the service provider can prove that he did not act negligently.<sup>9</sup>

**2.3.5. Implementation in the UK:** Reg. 3 of The Electronic Signatures Regulations 2002 requires the Secretary of State to keep the activities of certification-service-providers established in the UK under review.

---

<sup>6</sup> Directive 1999/93/EC of the European Parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l\\_013/l\\_01320000119en00120020.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf)

<sup>7</sup> SI 2002 No. 318

<sup>8</sup> Art. 3 (3)

<sup>9</sup> Art. 6 (1)

## 2.4. Electronic Commerce

2.4.1. Directive 2000/31/EC ('**the electronic commerce directive**')<sup>10</sup> was adopted on 8 June 2000 and came into force on 17 July 2000. Member states were required to implement it by 17 January 2002. The Electronic Commerce (EC Directive) Regulations 2002<sup>11</sup> carry most of its provisions into effect in the UK. The directive seeks to contribute to the proper functioning of the internal market by ensuring free movement of information society services between member states.

2.4.2. The directive prohibits member states from imposing special authorization schemes for information society service providers. In particular, they may not restrict service providers' freedom to provide information society services from another member state unless such restrictions are necessary to protect a vital national interest in which case they may obtain a temporary derogation. They are required only to make available to customers and authorities in easily accessible and permanent form basic information concerning their activities such as name, postal and e-mail address, trade registration particulars and VAT number. Information service providers that act as a "mere conduit" of information from third parties enjoy conditional exemption from liability for damage caused by material passing through their networks.

2.4.3. Member states must neither prohibit nor restrict the use of electronic contracts. They must however require certain information to be given to parties who enter electronic contracts.

2.4.4. Commercial communications, such as advertising and direct marketing, must be clearly identifiable. Professional persons shall be allowed to offer their services on-line provided they comply with general professional standards.

2.4.5. Codes of conduct for delivering information society services are to be developed. Member states are to co-operate in setting up effective, cross-border on-line, dispute resolution procedures.

---

<sup>10</sup> OJ L 178 , 17/07/2000 P. 0001 - 0016  
[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32000L0031&model=g uichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32000L0031&model=g uichett)

<sup>11</sup> <http://www.legislation.hmsso.gov.uk/si/si2002/20022013.htm>

**2.5 Data Protection:** Concern over the speed by which electronic profiles on individuals can be assembled and disseminated around the world has been the subject of debate and development in the UK, Europe and throughout the world for over 20 years. Effective privacy protection clearly requires international co-operation. The OECD proposed voluntary guidelines for trans-border data flows as long ago as 25 September 1980<sup>12</sup>. These were initially encouraged by the US government and endorsed by many leading American based multinationals. Several countries in Europe, notably Sweden, Germany and Austria, imposed stringent national data protection laws which impeded trans-border data flows. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data<sup>13</sup> prompted legislation throughout Europe including the Data Protection Act 1984 in the UK.

**2.5.1. Current Community Legislation:** The Council has adopted two new data protection directives both of which are now implemented in the UK:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("**the data protection directive**");<sup>14</sup> and
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector ("**the telecommunications data protection directive**").<sup>15</sup>

The data protection directive has been implemented into English law by the Data Protection Act 1998.

**2.5.2. Directive 2002/58 on Privacy and Electronic Communications**<sup>16</sup> supersedes the telecommunications data protection directive from 31 October 1993. It extends the data protection principles across the whole telecommunications sector including telephony, e-mails, and text messaging. Consent will be required for unsolicited calls or e-mails.

---

<sup>12</sup> Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data [http://europa.eu.int/comm/internal\\_market/en/dataprot/inter/priv.htm](http://europa.eu.int/comm/internal_market/en/dataprot/inter/priv.htm)

<sup>13</sup> [http://europa.eu.int/comm/internal\\_market/en/dataprot/inter/con10881.htm](http://europa.eu.int/comm/internal_market/en/dataprot/inter/con10881.htm)

<sup>14</sup> [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett)

<sup>15</sup> [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett)

<sup>16</sup> OJ 31.7.2002 L 211/37 <http://www.dataprivacy.ie/images/Directive%202002-58.pdf>

### 3. Electronic Commerce (EC) Regulations 2002

John Lambert

3.1. **Overview:** The Electronic Commerce (EC Directive) Regulations 2002<sup>1</sup> ("**the regulations**") implement arts. 3, 5, 6, 7(1), 10 to 14, 18(2) and 20 of the Electronic Commerce Directive<sup>2</sup> ("**the directive**") in the UK. It is one of several implementing statutory instruments.<sup>3</sup> It provides for the establishment and regulation of "*information society service providers*", their civil liability and the formation of electronic contracts. All but one of its provisions came into force on 21 August 2002. The provision for stop orders<sup>4</sup> came into effect on 23 October 2002.

3.2. **Information Society Services:** "*Information society services*" are defined awkwardly. Reg. 2 (1) of the Electronic Commerce Regulations refers to the definition in recital 17 of the directive:

"covering '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'."

Art. 2 (a) of the directive provides that "*information society services*" has the same meaning as in art. 1 (2) of Directive 98/34/EC as amended by art. 1 (2) (a) of Directive 98/48/EC.<sup>5</sup> The definition of information society services provided by that paragraph is slightly different:

---

<sup>1</sup> SI 2002 No. 2013

<sup>2</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), O.J. L178, 17.7.2000, p.1  
[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett)

<sup>3</sup> The others are The Electronic Commerce Directive (Financial Services and Markets) Regulations 2002 (S.I. 2002/1775), the Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) (No. 2) Order 2002 (S.I. 2002/1776), The Electronic Commerce Directive (Financial Services and Markets) (Amendment) Regulations 2002 (S.I. 2002/2015) and the Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) (Electronic Commerce Directive) Order 2002

<sup>4</sup> Reg. 16

<sup>5</sup> Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations OJ L 217 , 05/08/1998 P. 0018 - 0026  
[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31998L0048&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31998L0048&model=guichett)

"any service normally provided for remuneration, *at a distance, by electronic means* and *at the individual request of a recipient of services.*"

The words "*at a distance*" mean simply that the service is provided without the parties being simultaneously present.<sup>6</sup> Services provided "*at a distance*" do not include

"services provided in the physical presence of the provider and the recipient, even if they involve the use of electronic devices

- (a) medical examinations or treatment at a doctor's surgery using electronic equipment where the patient is physically present;
- (b) consultation of an electronic catalogue in a shop with the customer on site;
- (c) plane ticket reservation at a travel agency in the physical presence of the customer by means of a network of computers;
- (d) electronic games made available in a video-arcade where the customer is physically present."

The phrase "*by electronic means*" requires the service to be

"sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means."

Those words do not extend to

"Services not provided 'by electronic means'

Services having material content even though provided via electronic devices:

- ) automatic cash or ticket dispensing machines (banknotes, rail tickets);
- ) access to road networks, car parks, etc., charging for use, even if there are electronic devices at the entrance/exit controlling access and/or ensuring correct payment is made,  
Off-line services: distribution of CD ROMs or software on diskettes,  
Services which are not provided via electronic processing/inventory systems:
  - (a) voice telephony services;
  - (b) telefax/telex services;
- ) services provided via voice telephony or fax;
  - (d) telephone/telefax consultation of a doctor;
  - (e) telephone/telefax consultation of a lawyer;
  - (f) telephone/telefax direct marketing."

---

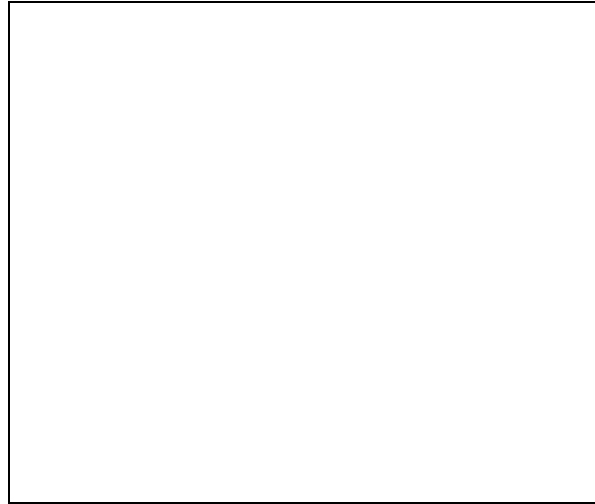
<sup>6</sup> Art. 1 (2) (a) of the directive

The expression "*at the individual request of a recipient of services*" means that the service is provided through the transmission of data on individual request. Excluded from that definition are

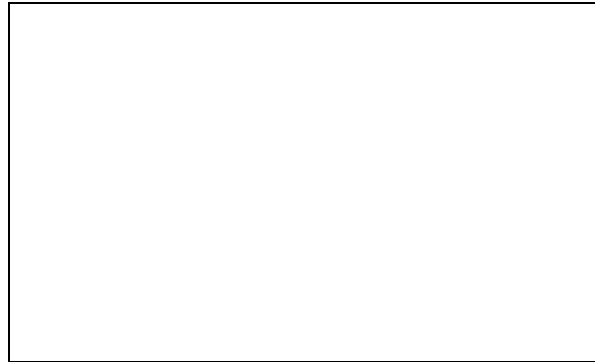
"Services provided by transmitting data without individual demand for simultaneous reception by an unlimited number of individual receivers (point to multipoint transmission):

- (a) television broadcasting services (including near-video on-demand services), covered by point (a) of Article 1 of Directive 89/552/EEC;
- (b) radio broadcasting services;
- (c) (televised) teletext."

For good measure, art. 1 (2) of Directive 98/34/EC adds that that directive does not apply to radio or television broadcasting services.



**3.3. Services Covered:** Despite this ponderous definition, the expression "information society services" includes just about every public on-line service including electronic commerce, search engines, on-line databases, internet service provision, web hosting and the provision of public services on line. Radio and TV broadcasts are not *information society services* as such unless they are interactive because they are not supplied in response to an individual request. Neither are emails or text messages unless they are commercial communications.



**3.4. Information to be given by Information Society Service Providers:** An information society service provider must make the following information available to recipients of his service and the enforcement authorities in an easily, directly and permanently accessible form and manner<sup>7</sup>:



---

<sup>7</sup> Reg. 6 (1)

- 3.4.1. his name;
- 3.4.2. the geographical address at which he is established;
- 3.4.3. his electronic mail address and other details to enable him to be contacted rapidly, directly and effectively;
- 3.4.4. details of his registration in a trade or other register that is available for public inspection including his registration number or other means of looking him up;
- 3.4.5. particulars of any relevant supervisory authority if the service supplied is subject to authorization;
- 3.4.6. details of any professional body or similar institution with which the service provider is registered, together with his professional title and the member state in which it was granted together with a reference to any professional rules that may apply and the means of accessing them;
- 3.4.7. the service provider's VAT number (where tax is charged); and
- 3.4.8. clear and unambiguous reference to any prices to be charged and whether they include tax and delivery costs.<sup>8</sup>

**3.5. Commercial Communications:** a communication designed to promote directly or indirectly goods, services or marketing image<sup>9</sup> must be clearly identifiable as such.<sup>10</sup> It must clearly identify the person on whose behalf the communication is made.<sup>11</sup> Any promotional offer, such as a discount, premium or gift, must be identified clearly. Any conditions must be easily accessible and presented clearly and unambiguously.<sup>12</sup> So too must any promotion, competition or game together with conditions for entry.<sup>13</sup>

**3.6. Spam:** Unsolicited commercial communications sent by email must be clearly and unambiguously identifiable as such as soon as they arrive.<sup>14</sup>

**3.7. Contracts concluded by electronic means:**

The following provisions apply to transactions with consumers,<sup>15</sup> whether they purport to opt out of them or not, and to contracts between non-consumers unless they agree otherwise.<sup>16</sup> They do not apply to contracts concluded exclusively by exchange of electronic mail or equivalent communications.<sup>17</sup>

---

<sup>8</sup> Reg. 6 (2)

<sup>9</sup> The definition of "regulated profession" in reg. 2 (1) of the regulations is identical to art. 2 (g) of the directive.

<sup>10</sup> Reg. 7 (a)

<sup>11</sup> Reg. 7 (b)

<sup>12</sup> Reg. 7 (c)

<sup>13</sup> Reg. 7 (d)

<sup>14</sup> Reg. 8

<sup>15</sup> A "consumer" is defined by art. 2 (1) as "any natural person who is acting for purposes other than those of his trade, business or profession",

<sup>16</sup> Regs. 9 (1) and (2) and 11 (1) .

<sup>17</sup> Regs. 9 (4) and 11 (3)

Where a contract for services covered by the regulations is concluded by electronic means, the service provider must provide the following information to prospective recipients in a clear, comprehensible and unambiguous manner before any order (whether it takes the form of an offer or some non-binding expression of interest<sup>18</sup>) may be placed:

- 3.7.1. the different technical steps to follow to conclude the contract;
- 3.7.2 whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
- 3.7.3. the technical means for identifying and correcting input errors prior to placing any offer to take the services; and
- 3.7.4. the languages offered for the conclusion of the contract.<sup>19</sup>

The information society service provider must also indicate any relevant codes of conduct to which he subscribes and give information on how those codes can be consulted electronically.<sup>20</sup> Should any special terms or conditions apply to the contract, the service provider must make them available for storage and reproduction.<sup>21</sup> If he fails to do so an application may be made to the court having jurisdiction over the matter for an order to comply.<sup>22</sup>

**3.8. Acknowledging Orders:** A service provider must acknowledge receipt of any order or expression of interest without undue delay by electronic means. He must provide appropriate, effective and accessible technical means of identifying and correcting input errors before any offer is placed.<sup>23</sup> If the service provider fails to provide such means a recipient may rescind any contract that he may have made unless a court having jurisdiction over the matter on the application of the service provider orders otherwise.<sup>24</sup> Receipt of an offer to take a service may be acknowledged by providing the service.<sup>25</sup>

**3.9. Enforcement:** The regulations apply to all information society service providers in the UK, whether their services are intended for the UK or not.<sup>26</sup> Information service providers established elsewhere in the EC are generally exempted from local requirements by reg. 4 (3) though UK authorities can take steps in an emergency to protect vital national interests.

---

<sup>18</sup> Reg. 12

<sup>19</sup> Reg. 9 (1)

<sup>20</sup> Reg. 9 (2)

<sup>21</sup> Reg. 9 (3)

<sup>22</sup> Reg. 14

<sup>23</sup> Reg. 11 (1)

<sup>24</sup> Reg. 15

<sup>25</sup> Reg. 11 (2) (b)

<sup>26</sup> Reg. 4 (1)

3.10. **ISP Liability:** An area particularly in need of harmonization is the liability of an ISP for material transmitted through its networks. In the USA, ISPs are exempted from liability by federal statute<sup>27</sup> however harmful the material.<sup>28</sup> In Germany, by contrast, ISPs and their managers may be prosecuted for permitting dissemination of racist or pornographic material.<sup>29</sup> The UK has taken a middle course between those extremes. For instance, an ISP may be liable as a publisher for storing and permitting access to defamatory material.<sup>30</sup>

2.10.1. The directive<sup>31</sup> recites that such disparities cause real difficulties:

"Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition."

Accepting that "service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities"<sup>32</sup> the directive largely leaves it to the industry to develop reliable procedures for removing and disabling access to illegal information.

3.10.2. **Mere Conduit:** Reg. 17 (1) exempts information society service providers from liability for damages or other pecuniary remedy and from criminal sanctions in respect of a service that consists of the *transmission* in a communication network of information provided by a recipient of the service or the *provision of access* to a communication network, provided that the service provider

- did not initiate the transmission;
- did not select the receiver of the transmission; and
- did not select or modify the information contained in the transmission."

---

<sup>27</sup> §.230 (c) (1) of the Communications Decency Act

<sup>28</sup> *Zeran v America Online Inc.* (1997) 129 F 3d 327 <http://www.law.emory.edu/4circuit/nov97/971523.p.html>

<sup>29</sup> *Somm* Amtsgericht Munich File No.: 8340 Ds 465 Js 173158/95

<sup>30</sup> *Godfrey v Demon Internet Ltd* [2001] QB 201 [http://www.cyber-rights.org/documents/godfrey\\_decision.htm](http://www.cyber-rights.org/documents/godfrey_decision.htm)

<sup>31</sup> Recital (40)

<sup>32</sup> *Ibid*

"Transmission" and "provision of access" include automatic, intermediate and transient storage of information for the sole purpose of carrying out the transmission provided that the information is not stored any longer than reasonably necessary for the transmission.<sup>33</sup> Reg. 17 (1) appears to exempt an ISP from criminal but not necessarily civil liability. Paragraph (1) excuses the ISP only from liability for damages or some other pecuniary remedy. Reg. 20 (1) (b) provides that nothing shall prevent a court or administrative authority from requiring a service provider to terminate or prevent an infringement.<sup>34</sup>

3.10.3. **Caching:** "Caching" for this purpose means "automatic, intermediate and temporary storage" of information for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request. Reg 18 exempts information society service providers from liability for damages or other pecuniary remedy any from any criminal sanction for any information that is so stored provided that the service provider:

- does not modify the information,
- complies with any conditions on access to the information,
- complies with any rules regarding the updating of the information, specified in a manner widely recognized and used by industry,
- does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information, and
- acts expeditiously to remove or to disable access to the information he has stored upon obtaining *actual knowledge* of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

3.10.4. **Hosting:** Reg. 19 exempts information society service providers from liability for damages or other pecuniary remedy or from any criminal sanction for storing web pages or other material provided by a recipient of its services in either of the following circumstances.

The first of these circumstances is where the information society service provider did not have actual knowledge of the unlawful activity or information. In civil but not criminal proceedings, knowledge may be imputed from facts or circumstances from which it should have been apparent to the service provider that the activity or information was unlawful.

---

<sup>33</sup> Reg. 17 (2) of the Electronic Commerce Regulations

<sup>34</sup> Art. 12 (3)

The second circumstance is where the information society service provider acts expeditiously to remove or to disable access to the unlawful information upon learning about it. The exemption does not apply if the person providing the offending material was acting under the authority or the control of the service provider.

3.10.5. **Contracting out:** An information society service provider can contract out of any of the above exemptions though it is not clear why he should wish to do so.<sup>35</sup>

3.10.6. **Actual Knowledge:** In determining whether a service provider has actual knowledge for the purpose of the caching and hosting exemptions, a court has to take into account all relevant matters including

- (a) whether a service provider received notice through any of the means of contacting him; and
- (b) the extent to which such notice includes:
  - (i) the full name and address of the sender of the notice;
  - (ii) details of the location of the information in question; and
  - (iii) details of the unlawful nature of the activity or information in question<sup>36</sup>.

3.10.7. **Burden of Proof:** In any prosecution for an offence arising out of a service provider's transmission, providing access to or storage of information or hosting material, it is enough for him to adduce sufficient evidence to raise an issue under one of the above defences. It is then for the prosecution to prove beyond reasonable doubt that the defence does not apply.<sup>37</sup>

3.11. **Dispute resolution:** The directive makes 2 sets of provisions with regard to dispute resolution:

3.11.1. **Court Proceedings:** Art. 18 (1) requires member states to ensure that court actions available under national law relating to information society service providers' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged wrongdoing and prevent any further impairment of the interests involved. In particular, stop orders must be available for breaches of the directive.

3.11.2. **ADR:** Art. 17 requires member states to:

- ensure that, their legislation does not hamper the use of out-of-court schemes for dispute settlement, including appropriate on-line dispute resolution;
- encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes, to operate in a way which provides adequate procedural guarantees for the parties concerned; and

---

<sup>35</sup> Reg. 20 (1) (a) provides: "(1) Nothing in regulations 17, 18 and 19 shall (a) prevent a person agreeing different contractual terms;"

<sup>36</sup> Reg. 22

<sup>37</sup> Reg. 21 (2)

- encourage bodies responsible for out-of-court dispute settlement to inform the Commission of any significant decisions they take regarding information society services and to transmit any other information on the practices, usages or customs relating to electronic commerce

3.11.3. Reg. 16 amends The Stop Now Orders (E.C. Directive) Regulations 2001<sup>38</sup> to enable the Director-General of Fair Trading to apply for injunctions to restrain breaches of the directive and regulations. The regulations make no provision for out of court dispute resolution as such, but the government relies on various ombudsman and arbitration schemes established by a number of industries and professions to meet its obligations under art 17 of the directive.<sup>39</sup>



---

<sup>38</sup> S.I. 2001/1422

<sup>39</sup> [http://europa.eu.int/comm/consumers/policy/developments/acce\\_just/acce\\_just04\\_uk\\_ccb\\_en.html](http://europa.eu.int/comm/consumers/policy/developments/acce_just/acce_just04_uk_ccb_en.html)

## 4. Domain Name Disputes

John Lambert

4. 1. **Domain Name System:** As everyone knows, the internet is a global network of networks exchanging information and sharing services throughout much of the world

4.1.1. **URL** . Files on the internet are located by universal resource locators ("**URL**"). Each URL consists of the following elements:

- a protocol such as "http"
- a server address such as www.nipclaw.com
- a file name which is usually identified by the suffix "htm".

4.1.2. **Domain Names:** Each computer on the internet is assigned a unique identifier consisting of 4 sets of numbers, each set divided by a point, called an IP (or internet protocol) number. The domain name is merely a mnemonic for this rather cumbersome set of numbers. A domain name consists of three parts, the server name, usually "www", a top level domain such as ".com", ".org", ".net", ".uk" or ".fr" and a second level domain such as "nipclaw" or "kingsgatechambers".

4.1.3. **Top Level Domains** There are 2 kinds of top level domains, namely "*generic top level domains*" ("**gTLDs**") like ".com", ".net", ".org" and ".biz" and "*country code top level domains*" ("**ccTLD**") such as ".uk", ".fr", ".de", ".it" and so forth.

4.2. **ICANN** *The Internet Corporation for Assigned Names and Numbers*<sup>1</sup> is a California not for profit corporation which was formed to oversee the allocation of certain gTLDs. It is responsible for ".aero", ".biz", ".com", ".info", ".name", ".net" and ".org" gTLDs. ICANN accredits a number of companies around the world to register names in one or more of those gTLDs<sup>2</sup> known as registrars. There are 9 accredited gTLD registrars in the UK<sup>3</sup>.

4.3. **Nominet**<sup>4</sup> Each ccTLD is administered by a national internet authority or "NIC". The internet authority for the UK is *Nominet UK*, a company limited by guarantee with about 2,000 members drawn from ISPs, the computer industry and others with an interest in the internet such as lawyers. Membership is open to anyone with £100 to spare.

<sup>1</sup> <http://www.icann.org/>

<sup>2</sup> A list of registrars is available at <http://www.icann.org/registrars/accredited-list.html>

<sup>3</sup> Of which 6 appear to be operating

<sup>4</sup> <http://www.nic.uk/index.html>

**4.4. Domain Name Disputes:** The opportunities provided by the world wide web for marketing attracted business interest in the mid-1990s. Domain names, which had not been perceived as particularly vital for the first 25 years of the history of the internet, suddenly became a valuable asset. NICs tend to register domain names on a first come first served basis. Registration has always been fairly inexpensive. Not every business was astute enough to register its trade name or trade mark as a domain name. That left the door open for speculators (known as "cyber-squatters") to register names of well known companies as domain names. Cyber-squatters were encouraged by enormous ransoms occasionally paid.

**4.4.1. Early Cyber-squatting Cases:** Some businesses in the UK and elsewhere resorted to litigation but with varying success. Until the decision of the Court of Appeal in *British Telecommunications Plc v One in a Million Ltd.*<sup>5</sup> it was not clear that cyber-squatting was caught by any of the provisions of s.10 of the Trade Marks Act 1994 or even whether it amounted to passing off. Litigation was expensive and most cyber-squatters were unable to pay substantial costs. There was often a problem of bringing proceedings abroad or enforcing a judgment against a foreign defendant. Litigation never worked well in cases where companies of the same or similar name operating in different countries or industries collided. In one such case, the respondent, a medium size English computer company, was able to obtain an injunction to restrain groundless threats by a well-known US sports goods manufacturer under s.21 of the Trade Marks Act 1994.<sup>6</sup> The initial policy of Network Solutions (the first gTLD registrar) and NominetUK was to stay out of such conflicts so far as possible. Despite that, both registrars found themselves joined as defendants in the UK<sup>7</sup> and USA<sup>8</sup>.

**4.4.2. Mandatory Dispute Resolution:** One of the reasons for setting up ICANN was to provide machinery for resolving gTLD disputes. ICANN was mandated to require registrars to implement a domain name resolution procedure. Clause 3.8 of ICANN's registrar accreditation agreement<sup>9</sup> requires every registrar to have in place a policy and procedure for domain name dispute resolution.

**4.4.3. Nominet's Previous Dispute Resolution Procedure:** Between 1997 and 2001 Nominet offered mediation to resolve domain name disputes. It would suspend or even cancel registrations only where there was a clear risk of confusion or legal action had been taken.

---

<sup>5</sup> [1998] 4 All ER 476

<sup>6</sup> *Prince Plc v Prince Sports Group Inc.* [1998] FSR 16

<sup>7</sup> *Pitman Training Ltd. v Nominet UK and others* [1997] FSR 797

<sup>8</sup> *Lockheed Martin Corporation v Network Solutions Inc.* (USDC for CD California, 1997

<sup>9</sup> <http://www.icann.org/registrars/ra-agreement-17may01.htm>

#### 4.5. ICANN Uniform Dispute Resolution Policy:

Since 24 October 1999 every ICANN accredited registrar has been obliged to insert a clause<sup>10</sup> into every agreement for the registration of a second level domain name requiring the applicant to submit certain types of dispute to a "mandatory administrative proceeding" before an ICANN approved administrative-dispute-resolution service provider. This procedure is known as the ICANN Uniform Domain Name Dispute Resolution Policy ("**UDRP**").<sup>11</sup> The following is extracted from the Easyspace site<sup>12</sup>:

"All registrars in the .com, .net, and .org top-level domains follow the Uniform Domain-Name Dispute-Resolution Policy (often referred to as the "UDRP"). Under the policy, most types of trademark-based domain-name disputes must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name. Disputes alleged to arise from abusive registrations of domain names (for example, cybersquatting) may be addressed by expedited administrative proceedings that the holder of trademark rights initiates by filing a complaint with an approved dispute-resolution service provider.

4.5.1. **Types of Dispute:** The UDRP does not cover all domain name disputes. An applicant is required to submit to a mandatory administrative proceeding only if a third party (a "**complainant**") asserts to the applicable dispute resolution provider in compliance with ICANN's rules of procedure, that:

- the registered domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
- the respondent has no rights or legitimate interests in respect of the domain name; and
- the domain name has been registered and is being used in bad faith.

The complainant must prove that and every one of those *probanda* and that is not always easy to do.

4.5.2. **Approved Service Providers:** There were as at 7 October 2002 the following such providers:

- Asian Domain Name Dispute Resolution Centre of Beijing and Hong Kong;
- CPR Institute for Dispute Resolution
- The National Arbitration Forum, and
- The World Intellectual Property Organization.

4.5.3. Each of those service providers has its own rules of procedure and fee structure:

---

<sup>10</sup> Clause 4

<sup>11</sup> <http://www.icann.org/dndr/udrp/policy.htm>

<sup>12</sup> <http://www.easyspace.com/faqs/disputeinfo.html>

- The WIPO charges US\$1,500 for a reference of up to 5 names to a single panellist and US\$3,000 to a 3 person tribunal, US\$2,000 for 6 to 10 to a single panellist and US\$4,000 to a 3 person tribunal<sup>13</sup>.
- The Hong Kong office of the Asian Domain Name Dispute Resolution Centre charges US\$1,000 for 1 to 2 names before a single panellist and US\$1,200 for 3 to 5.<sup>14</sup>
- CPR charges US\$2,000 for 1 to 2 names before a single panellist.<sup>15</sup>

4.5.4. **Procedure:** Every application must be lodged in accordance with the ICANN Rules of Procedure<sup>16</sup> as well as those of the authorized service provider.

4.6. **Complaint:** Rule 3 of the ICANN Rules require a complainant to submit a complaint to an authorized service provider in hard copy and electronic form. Such complaint must:

- request the complaint to be determined in accordance with the UDRP and ICANN Rules;
- provide the name, postal and e-mail addresses, telephone and fax numbers of the complainant and of any authorized representative;
- specify a preferred method for communicating with him;
- choose either a single or 3-member panel;
- identify the respondent and give his postal and e-mail addresses and telephone and fax numbers;
- specify the domain name(s) the subject of the complaint;
- identify the registrar(s) with whom the domain name(s) is/are registered at the time of filing;
- specify any trade or service mark on which the complaint is based and the goods and services for it is registered or to which it applies;
- set out the grounds on which the complaint is made including, in particular, the manner in which the domain name is identical or confusingly similar to a trade mark, why the respondent should be considered as having no rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and
- why the domain name(s) should be considered as having been registered and used in bad faith;
- specify, in accordance the remedies sought;
- identify any other legal proceedings that have been commenced or terminated in connection with, or relating to, any of the domain name(s) that are the subject of the complaint;
- state that a copy of the complaint, together with the cover sheet prescribed by the service provider has been sent or transmitted to the

<sup>13</sup> <http://arbiter.wipo.int/domains/fees/index.html>

<sup>14</sup> [http://www.adndrc.org/adndrc/hk\\_schedule\\_fees.html](http://www.adndrc.org/adndrc/hk_schedule_fees.html)

<sup>15</sup> [http://www.cpradr.org/ICANN\\_RulesAndFees.htm](http://www.cpradr.org/ICANN_RulesAndFees.htm)

<sup>16</sup> <http://www.icann.org/dndr/udrp/uniform-rules.htm>

<sup>17</sup> Rule 10 (a) WIPO Supplemental Rules

- respondent;
- state that complainant will submit, with respect to any challenges to a decision in the administrative proceeding cancelling or transferring the domain name, to the jurisdiction of the courts in at least one specified jurisdiction;
- conclude with a waiver of any claim against ICANN, the service provider, panellist, registrar, a certificate of truth and a statement that the claim is properly brought.

The complaint must annexe any documentary or other evidence, including a copy of the dispute resolution policy and trade mark certificate. The WIPO limits complaints to 5,000 words.<sup>17</sup>



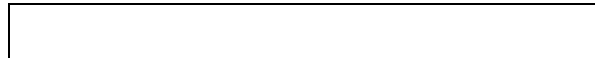
**4.7 Response:** The service provider is required to review the *complaint* to make sure everything is in order.<sup>18</sup> If it is, it will transmit the complaint to the respondent. If not it will give the complainant a limited time to correct the defect.

4.7.1. The respondent has 20 days in which to respond to the complaint in a pleading known as the response.<sup>19</sup>

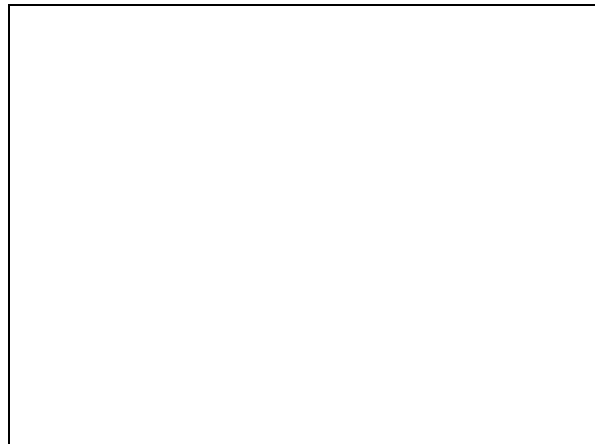
4.7.2. The response must respond specifically to the statements and allegations contained in the complaint and include any and all grounds for the respondent to retain registration and use of the disputed domain name. The other important part of the response is the election of a single or 3-member panel. If the respondent wants a 3-member panel he must contribute to the costs of the additional panellists. The WIPO supplemental rules also limit the response to 5,000 words.



**4.8. Reply:** The panel has discretion to permit further documents or statements.<sup>20</sup>



**4.9. Determination:** An independent and impartial tribunal is chosen from the service provider's list of panel members within 5 days of the response or expiry of the time for responding.<sup>21</sup> The panel is required to conduct the proceedings in such manner as it considers appropriate in accordance with the UDRP and Rules. The parties are to be treated with equality and given a fair opportunity to present their cases.<sup>22</sup> The panel must decide a complaint on the basis of the statements and documents submitted taking account of any rules and principles of law that it deems applicable. Absent exceptional circumstances, it must forward its decision on the complaint to within 14 days of appointment. The panel may reject the complaint or order the cancellation or transfer of the domain name.



<sup>18</sup> Rule 4 (a) of the ICANN Rules

<sup>19</sup> Rule 5 (a) *ibid*

<sup>20</sup> Rule 12 *ibid*

<sup>21</sup> Rule 6 (b), (d) and (e) *ibid*

<sup>22</sup> Rule 10 *ibid*

4.10. **Costs** Unless the respondent elects a 3-person tribunal and the complainant only 1, all fees are paid by the complainant. There is no provision for costs.

4.11. **Nominet Dispute Resolution Service:** Nominet contracts directly with every applicant for registration of a ".uk" domain name. Clause 7.1 of Nominet's terms and conditions incorporates its Dispute Resolution Policy and Procedure into the registration agreement. Applicants agree to be bound by the current policy and procedure.

4.11.1. **Applicable Disputes:** The dispute resolution policy applies where a complainant alleges that:

- he or she has "*Rights*"<sup>23</sup> in respect of a name or mark which is identical or similar to a Nominet registered domain name; and
- such domain name, in the hands of the respondent, is an "*Abusive Registration*".<sup>24</sup>

Both must be proved on the balance of probabilities.<sup>25</sup>

4.11.2. **Procedure** A complaint must be filed in accordance with Nominet's "*DRS Procedure*".<sup>26</sup> This is very similar to the ICANN Rules of Procedure. The main differences are that the parties are offered informal mediation before the case is referred to an expert for determination and they can appeal if dissatisfied. Nominet has said that many complainants (including some who are legally represented) fail to follow the DRS Procedure. It has promised to post model complaint and response forms which it will expect parties to follow.

4.11.3. **Contents of Complaint:** Rule 3 (b) of the Procedure requires a complaint to be in hard copy and electronic form. It may not exceed 2000 words. The complaint must:

- specify whether the complainant wishes to be contacted direct or through an authorized representative, and set out the e-mail address, telephone number, fax number and postal address which should be used;
- set out any of the respondent's contact details that are known to the complainant;
- specify the domain name which is the subject of the dispute and the name or mark which is identical or similar to the domain name and in which the complainant asserts it has trade mark or other rights;
- state the grounds on which the complaint is made including, in particular, the rights that the complainant asserts in the name or mark, why the domain name should be considered an

<sup>23</sup> Clause 1 of the DRS Policy provides that "*Rights*" include, but are not limited to, rights enforceable under English law though a complainant may not rely on rights in a name or term which is wholly descriptive of his business. They would include but not be limited to registered trade marks but an unregistered mark to which goodwill is attached.

<sup>24</sup> An "*Abusive Registration*" is defined by clause 1 as a registered domain name which either:

- (i) was registered or otherwise acquired in a manner which, at the time when the registration or acquisition took place, took unfair advantage of or was unfairly detrimental to the complainant's Rights; OR
- (ii) has been used in a manner which took unfair advantage of or was unfairly detrimental to the complainant's Rights;

<sup>25</sup> Clause 2 DRS Policy <http://www.nic.uk/ref/drs-policy.html>

<sup>26</sup> <http://www.nic.uk/ref/drs-procedure.html>

- abusive registration in the hands of the respondent and any grounds of the assertion;
- specify whether the complainant is seeking to have the domain name transferred, suspended, cancelled or otherwise amended
  - state whether any legal proceedings have been commenced or terminated in connection with the domain name
  - state that the complainant will submit to the exclusive jurisdiction of the English courts with respect to any legal proceedings seeking to reverse the effect of a decision requiring the suspension, cancellation, transfer or other amendment to a domain name registration, and that the complainant agrees that any such legal proceedings will be governed by English law.

As under the ICANN procedure the complainant must disclaim any rights or remedies against Nominet or expert and verify the truth of the statement. The hard copy must annexe any trade mark certificates or other documentary evidence referred to in the complaint or otherwise relied upon.

4.11.4. **Processing:** Nominet will check the complaint and forward it to the respondent if it is in order or return it to the complainant for correction. He or she has 3 days in which to make the correction otherwise it will be deemed to have been withdrawn.<sup>27</sup>

4.11.5 **Response:** The respondent must respond within 15 days of service of the complaint.<sup>28</sup> That must also be in electronic form or hard copy and is again limited to 2,000 words.<sup>29</sup>

Such response must:

- include any grounds the respondent wishes to rely upon to rebut the complainant's assertions;
- specify whether he wishes to be contacted direct or through an authorized representative, and set out the e-mail address, telephone number, fax number and postal address which should be used; and
- state whether any legal proceedings have been commenced or terminated in connection with the domain name.

It must also contain a statement of truth and compliance with the DRS policy and procedure and applicable law and attach any documents relied upon.<sup>30</sup>

4.11.6. **Reply:** The complainant has 5 days in which to file a *reply* which yet again may not exceed 2,000 words.<sup>31</sup>

4.11.7. **Informal Mediation:** Nominet will then conduct informal mediation. If it is not completed within 10 days it will be referred to expert determination.<sup>32</sup>

---

<sup>27</sup> Rule 4 of the DRS Procedure

<sup>28</sup> Rule 5 (a) *ibid*

<sup>29</sup> Rule 5 (c) (i) *ibid*

<sup>30</sup> Rule 5 *ibid*

<sup>31</sup> Rule 6 *ibid*

<sup>32</sup> Rule 7 *ibid*

4.11.8. **Expert Determination:** The Expert will decide a complaint on the basis of the submissions, the policy and the procedure. Unless exceptional circumstances apply, he will forward his or her decision within 10 days of his or her appointment. The decision will be in writing and set out the reasons on which it is based.<sup>33</sup>

4.11.9. **Bad Faith:** An important and salutary provision of the Nominet Procedure is the power to make a finding that an application has been brought in bad faith. Rule 16 (d) provides that if after considering the submissions, the expert finds that the complaint was brought in bad faith, for example in an attempt at reverse domain name hijacking<sup>34</sup>, the expert shall state this finding in the decision. If the complainant is found on 3 separate occasions within a 2 year period to have brought a complaint in bad faith, Nominet will not accept any further complaints from that Complainant for a period of 2 years. A recent example of this is Stephen Maier's decision in *Cardpoint Plc v Riga Industries*<sup>35</sup> where the expert that though the complainant may have had rights there was no evidence of abusive registration and therefore the application had been brought in bad faith.

4.11.10 **Appeal** Rule 18 provides a right to appeal a decision by submitting written grounds for appeal to us not exceeding 2000 words within 5 days of communication of the decision. The appeal will be determined as soon as possible by a panel of 3 experts from the list. The costs of an appeal are £3,000. So far there have been 3 appeals 2 of which were dismissed and 1 allowed.

4.12. **Summary** Both ICANN and Nominet schemes have proved very popular. As at 7 October 2002 there had been:

- 5954 determined proceedings before ICANN together with a further 721 that had been settled, 509 pending applications and 12 that had been terminated for recommencement; and
- 544 disputes lodged with Nominet of which 426 have been archived and 118 were continuing.

By contrast, there have been only a handful of domain disputes determined by litigation. The advantages of the schemes are speed, economy and effectiveness of the remedy. Neither procedure covers every type of claim. Fees have to be paid by the complainant up front and those fees and costs are irrecoverable.

---

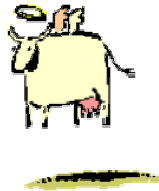
<sup>33</sup> Rule 16

<sup>34</sup> This is defined by rule 1 as using the Policy in bad faith in an attempt to deprive a registered domain-name holder of a domain name.

<sup>35</sup> 20 September 2002 <http://www.nic.uk/drs/decisions/cardpoint-v-riga.html>. The complainant's address was in Lytham St Anne's.

## Questions for Discussion

1. How far have the needs of business and private individuals been met by current e-commerce legislation? What else needs to be done? Is there too much legislation already?
2. Has the right balance been struck between protecting privacy and confidentiality in electronic communications on the one hand and detecting and preventing crime and antisocial behaviour on the other?
3. Will you need to change the wording on any of the following to take account of the Electronic Commerce (EC Directive) Regulations 2002:
  - (a) your firm's website;
  - (b) your firm's email header;
  - (c) your fax header sheet?If so, how? And, if not, why not?
4. What advice would you give to the following clients in respect of their websites in the light of the above Regulations:
  - (a) a mail order company which sells household goods, ladies and gentlemen's fashions, furnishings and other items over its website;
  - (b) a retailer of adult movies based in Amsterdam whose videos have English titles and are priced in sterling; and
  - (c) a family planning clinic which has received a growing number of enquiries from the Republic of Ireland?
5. Are the mere conduit, caching and hosting exemptions adequate for the needs of most ISPs?
6. Your client has bought £5,000 worth of defective software in an internet auction from a systems house in Denmark. What would you advise him to do about it?
7. Your client is a well-known dairy products wholesaler called "Happy Cow". About 18 months ago one of its junior employees who is interested in computers offered to create a website for the



company. Your client gratefully accepted the offer. The employee registered the domain names "happycow.com" and "happycow.co.uk" in his own name and at his own expense. He later set up a website advertising the products of the company.

Your client has dismissed the employee in order to save labour costs without first asking the employee to transfer the domain name to the company.

The employee has taken down the advertisements and uploaded material comparing "Happy Cow" products in price and quality to those of its competitors. The comparison in respect of each product is unflattering but not mendacious.

A dairy trade retailers' magazine has discovered [www.happycow.com](http://www.happycow.com) and [www.happycow.co.uk](http://www.happycow.co.uk) and has urged all its readers to visit. Many have done so and orders for Happy Cow cream cheese and yogurt have declined substantially. Your client is desperate. What would you advise him to do.

Would your answer be any different if the ex-employee used the site to libel the wife of the managing director of Happy Cow?