

Internet Newsletter for Lawyers

By Delia Venables

November/December 2003

On other pages....

Operation Ore:
An expert's Story
by Alistair Kelman 3

Hutton Enquiry:
How It's Done 4

The Jordans Group
by Nicola Webb and
Philip Wilmott 5

The Incorporated Council of
Law Reporting for England
& Wales
by Martha Hawting 6

Scottish Session Cases
by Anthony Kinahan 6

Domains are Hot Property
by Tim Brown 7

Practical Problems of
Digital Signatures
by Stephen Mason 9

How to Avoid Spam
Alan Tomlinson 11 & online

Electronic Irish Reports and
Digests on Justis.com
by Nuala Byrne 11 & online

Specialised Websites 11

Email – the New Law By Charles Black

On 11 December 2003 the Privacy and Electronic Communications (EC Directive) Regulations 2003 come into force. This legislation gives effect to the EU's Directive 2002/58/EC of 12 July 2002, introduced to provide additional laws to protect privacy in the light of new digital technologies. This article considers how the new law will affect email marketing campaigns undertaken by firms and chambers, and also whether the law will have any impact on controlling junk email.

Key points

The new Privacy Regulations add to the privacy laws created by the Data Protection Act and deal primarily with protecting privacy from intrusion by unsolicited communications by telephone, fax and email (including SMS messaging). The Regulations modify certain sections of the Data Protection Act and repeal the Telecommunications (Data Protection and Privacy) Regulations 1999 and 2000. A number of the Regulations relate to the obligations of telecom companies in relation to call identification, malicious and nuisance phone calls and other issues affecting an individual's right to privacy including unsolicited communications by fax and telephone. This article is concerned with Regulations 22 and 23 which deal with unsolicited email. Regulation 22(2) provides that

Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where -

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;
(b) the direct marketing is in respect of that person's similar products and services only;
and (c) the recipient has been given a simple means of refusing ... the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

The effect of Regulation 22 is that it is unlawful to send an email for direct marketing purposes unless the recipient has consented to receive it. The giving of consent would seem to require a positive action in that the recipient has to have "previously notified the sender" of their consent. The need for a positive action was plainly set out in the Directive which the Regulation implements, referring to obtaining "prior explicit consent".

Sub-section (3) deals with 'existing relationship' cases where the recipient is either a customer or potential customer. Initially sub-section (3) appears as a qualification to the general rule that consent is required before a direct marketing email can be sent to them. However, upon closer analysis this is not the case. There are 2 essential requirements to send direct marketing emails lawfully to existing relationship persons:

Firstly, the recipient still needs to have been given "a simple means of refusing ... the use of his contact details for the purpose of such direct marketing, at the time the details were initially collected...". If the details are collected via a web site enquiry form, this is dealt with by a simple check box which the user can tick to indicate their consent. However, if the recipient's email address is captured during a telephone conversation it seems that the user will have to be asked if they consent to their email being used for direct marketing purposes. Sales teams handling such enquiries need a way of recording this.

Read the Newsletter
on the web at
[www.venables.co.uk/
n0311mat.htm](http://www.venables.co.uk/n0311mat.htm)

ISSN 1467-3835

Delia Venables

10 Southway, Lewes
East Sussex BN7 1LU
phone and fax
01273 472424
delia@venables.co.uk
www.venables.co.uk

Secondly, even if the user consents to receive email for direct marketing purposes it is not permissible to then send an email to them marketing a dissimilar type of product – so solicitors firms and barristers chambers cannot market non-legal services to their clients or potential clients.

Consent is therefore the key to sending direct marketing emails legitimately. Recipients must have the opportunity to withdraw their consent at any time.

Regulation 23 makes it unlawful to send out direct marketing emails without showing the valid email address of the sender or without providing a valid email address to which the recipient can send a request to unsubscribe from receiving such emails in future.

Although the regulations require consent, there are no restrictions under sub-section (2) on the content of the email – so if you have the recipient's consent to receive marketing emails there are no restrictions on the products you can market or on who is actually selling the products. This means you can send out emails on behalf of third parties, promoting their products. Under sub-section (3) you can only send emails about your own products and services, so this clearly excludes sending emails on behalf of third parties.

The position on a business obtaining a mailing list or selling a mailing list to third parties is not all that clear. Consider a hypothetical example. A recipient has consented to receive emails from Company X. Also, they have ticked a checkbox to indicate they consent to receiving emails from any third parties selected by company X. Company X has, as a result, a mailing list of people who consent to receiving emails from any third parties selected by Company X. Company X is approached by Company Y to market Company Y's products to Company X's mailing list. In this scenario, Company X can clearly send out the email itself to its mailing list promoting Company Y's products. But can Company X hand over the mailing list to Company Y and allow Company Y to actually send out the email? The reference in Sub-section (2) to emails being sent "at the instigation of the sender" seems to imply that this is permissible. However, the consent has to have been notified to the sender, which in the scenario under consideration is Company Y. It is submitted that as consent is the key issue, provided the recipient has informed Company X that they are happy to receive emails from third parties then it is permissible.

Liability and enforcement

A breach of the Regulations does not give rise to any criminal penalties, only civil. Under Regulation 30, a person can commence proceedings for compensation against a person who has breached the Regulations. It is a defence for the person "to prove that he had taken such care as in all the circumstances was reasonably required to comply with the relevant requirement". The Information Commissioner (appointed under the Data Protection Act) has enforcement duties.

Practical guidelines for marketing emails

Case law will no doubt make the precise boundaries of what is permissible clearer, but in the meantime the following guidelines would appear to be sensible:

- * ensure that any marketing emails are sent only to users who have positively consented;
- * when capturing enquiries from potential clients via your web site, ensure the enquiry form gives the opportunity for the user to consent to receiving further marketing emails from you by providing a check box which they can tick; this

information should automatically be stored in the database used for your mailing list;

- * when capturing enquiries via the telephone ensure a way of recording that the user has been asked for their consent and for whether or not this is granted;
- * ensure any marketing email you send out enables the recipient to easily unsubscribe at any time;
- * ensure any email that is sent out shows the sender's email address (e.g. info@yourfirm.co.uk);
- * ensure that a valid email address is provided to which the recipient can send an email requesting that they be taken off your mailing list.

With the new Privacy Regulations in mind, my own company, Nasstar, has developed an online mailing application which a number of barristers chambers are using to market their services by email. The mailing application is easily managed via an online management system. With an infrastructure that can handle over 4 millions messages a day, Nasstar's mailing application ensures that each email sent has an unsubscribe link at the bottom enabling the user to unsubscribe easily.

The application also enables an authorised user on behalf of the sender to manually unsubscribe a particular recipient if they choose to telephone or email the sender requesting that they be removed (rather than following the unsubscribe link). The mailing application also ensures that the email address of the sender is shown.

The problem of junk email

The aim behind the new Privacy Regulations is to protect individuals from unsolicited bulk email – commonly referred to as spam or junk email. Will they do this?

In my opinion, the new law is unlikely to have any major impact in the battle against spam. Over 90% of junk email comes from the USA, and so the UK must wait to see what legal measures they take to tackle spam. At present the federal government is considering an opt-out law i.e. all spam is legal unless you have expressly opted out from receiving it. To combat spam, it seems that governmental co-operation on an international level may be required to create and police a standardized legal framework across the globe. Without such a legal framework it is technology rather than law that is providing effective solutions in the war against spam.

Conclusion

The new privacy law means firms and chambers must have a system in place for managing their mailing list both in terms of collecting data and sending marketing emails to the list. Whilst the law should be welcomed as providing a framework for businesses sending out emails, the law is unlikely to have any practical effect on controlling junk email. The invasion of spam from international jurisdictions, particularly the USA, means that the law will not have any impact on the main source of spammers. The most effective solution for junk email remains the use of technology solutions, many of which were considered in the last issue (www.venables.co.uk/n0309joa.htm)

Charles Black is the founder and Managing Director of Nasstar, www.nasstar.com, a business ISP which provides web sites, content management systems, hosting, email solutions, broadband and networks to a large number of businesses including chambers and solicitor firms. Charles is also a qualified barrister having been called to the Bar in 1996 and having undertaken pupillage in 1997. Email charlesblack@nasstar.com

Operation Ore: An Expert's Story by Alistair Kelman

Having hung up my wig and gown in 2000 to concentrate on developing my e-commerce based patents and inventions I never anticipated being back in the courtroom. But today I find myself testifying as an Expert Witness in Child Pornography cases using my knowledge of computer evidence, chains of custody and the operation of the Internet. It was not work I initially sought or wanted. But the need for qualified independent Expert Witnesses in paedophilia cases is immense because of the volume of cases arising from Operation Ore. And with the nature of the Internet there is a genuine risk that people could be convicted of crimes they did not commit.

The UK "Operation Ore" grew out of "Operation Avalanche" in the USA. A U.S. postal worker had become suspicious of excess mail going to and from an address. On 8th September 1999 federal agents raided the home and offices of Thomas and Janice Reedy who operated an Internet business called Landslide Productions, which the FBI knew sold subscriptions to websites offering child pornography. The business was said to be the largest commercial child pornography enterprise ever uncovered, grossing as much as \$1.4 million in just one month.

After entering Landslide's child porn site, people were offered a menu advertising selections such as "children forced to porn", "child rape" and "children of God". Each selection cost \$29.95 for a month's subscription. To join up, each person needed to give their credit card details and choose a password. A separate site of "adult classifieds" included entries from fathers advertising their children for sex. The company's outgoings included payments to Russia and Indonesia, where the images originated. A USA judge sentenced Janice Reedy to 14 years in prison, and Thomas Reedy to 1,335 years in prison – reduced on appeal to about 170 years.

In the course of the raid the FBI discovered a database of the site's subscriber list, with the names and credit details of 250,000 subscribers in 60 countries. 7,272 of these were subscribers in the UK and these names are termed the Operation Ore suspects. The National Criminal Intelligence Service immediately started sifting through the UK names to prioritise who they considered were the worst offenders – an expensive and difficult task. By July, over 1,700 people had been arrested and/or questioned. Most investigations involve a raid on the home of the suspect and computer hard disks being "imaged" for subsequent forensic examination by specialist officers. The resources needed for this are immense – NCIS have said that every one of the 7,272 suspects will be investigated.

My cases tend to arise when people are charged with downloading child pornography images off the Internet. Many of them are Operation Ore suspects. If they say that they are innocent, or only looked at an image once then it is my job to ensure that the possibility that they are telling the truth is fully investigated and that the police evidence against them really does bear scrutiny. A standard personal

computer running Microsoft Windows keeps very detailed system logs of all downloading activities so frequently there is damning evidence against the defendant on his own hardware giving dates and times of every activity.

The penalties for downloading child pornography images are severe and the consequences that flow from a conviction are horrific. It is however legal to download most types of adult pornography images in the UK.

Let me outline one of my typical cases – with particular facts changed to protect all parties:

John was a Public Servant working in the Emergency Services. Using the Internet he investigated and collected a vast amount of adult pornography. Three or four years ago he became curious regarding child pornography and subscribed to a US service. In consequence his name came up as one of the Operation Ore suspects. In late 2002 the police raided his home where they found a computer connected to the Internet, which they seized, and a quantity of floppy disks relating to an earlier computer that they also seized. On these floppy disks were a few "child pornography" images. All the images found were naked teenage children in legitimate settings with no sexual activity. They were the kinds of things you might see if you walked through a public park in Berlin on a sunny afternoon. Additionally within the Internet cache of the computer the police found a few further images of naked children with no sexual activity involved. These were thumbnail images in pages that contained both nude adult images as well as pictures of nude children. There was however evidence that the defendant had clicked on a few of the thumbnail images of children to produce a larger picture. This activity alone is considered sufficient to make out the offence under the UK legislation. John, to his credit, did not keep permanent copies of any of these images.

John was charged with eleven counts of downloading child pornography. By careful scrutiny of the evidence I managed to get this reduced to 5 counts. However, because John has admitted in his taped interview that he had a few years ago become curious about child pornography and had signed up to a commercial service, there was no question that he had downloaded the images found on the floppy disks. The only question that remained in relation to these early images was whether the pictures in question were of children or were actually of young adults posing as teenage children. This was therefore going to be a jury question.

Regarding the later images found in the cache, these appeared initially to show that John had joined a commercial service that provided child pornography. All of these downloads came long after the Operation Ore database of sites had been closed down. A further investigation by me of their context showed that this "commercial service" was actually Usenet. "Usenet" is a world-wide discussion system. "Articles" or "messages" are "posted" to the newsgroups by people on computers with the appropriate software. Some newsgroups are "moderated" where the articles are first sent to a moderator for approval before appearing in the newsgroup.

Are you considering a Content Management Solution for your firm's website, extranet or intranet?

ActiveLawyer have the largest number of site developments in the legal community. We have a state-of-the-art Content Management solution that is built on the latest Microsoft .NET platform. This has proven to be a fast, easy to use and powerful solution designed by lawyers for lawyers.

ActiveLawyer
Mastered in minutes. Updates in seconds.

Visit www.activelawyer.com, contact Rick Brar on 020 7841 5180 or email rick.brar@activelawyer.com.

The service John had joined provided unfiltered access to Usenet, with no moderator involved. In context, what this meant was that it appeared likely that John had joined the service not to gain access to child pornography but to gain access to adult pornography images (i.e. not illegal) which he had said was the case from the start. While the evidence supported the fact that John had clicked on certain thumbnail images of nude teenage children it was clear from the system logs that within a few seconds of doing so he also clicked on thumbnail images of nude adults. The police had been highly selective in their compilation of the evidence and many adult images should have been included in the jury bundles so that the making of the child images were placed in proper context.

This was a case that a jury could well have found did not warrant convicting the Defendant. The real question was could John keep his nerve for going through a whole trial. He consulted his wife. Their joint decision, on being told by counsel that a custodial sentence was highly unlikely if he pleaded, was that he should plead guilty.

John received a fine of £500 (£100 on each count). As an automatic consequence of the fine he was placed on the Sex Offences Register for five years where he has to regularly notify the police of his whereabouts including his trips abroad. He was required to pay £1,400 towards the prosecution costs. His computer system was forfeit. He may well lose his job because of his conviction.

It was John's decision not to risk a jury trial – and it may have been right for him given his then mental state. However, unlike counsel, my job as an expert does not end with the trial. I am able to put a defendant's actions in context for disciplinary hearings. I have offered to write to John's employers in his attempt to keep his job. In this letter I will be able to compare John's activities with those of real child pornographers, show that he has been fully punished for his foolishness and hope that his employer can show the mercy which is outside of the power of the court system.

Saving court costs

In other more serious cases I have been able to take apart each and every purported defence put up by the accused by examination of the technical evidence. On realising that the evidence against them is sound all the defendants have pleaded guilty and shown remorse. All are now in treatment and the public purse has been saved the cost of Crown Court trials.

I live in hope. One day I hope to find a truly innocent defendant, for example, someone who has been framed by an angry ex-wife who is trying to stop him having access to their children. But all I can do for the moment is force the police and the prosecution to "raise their game", to only proceed when the evidence is truly sound and irrefutable and to ensure that everything is within its proper context.

Alistair Kelman is a director of Telepathic Industries Limited, www.telepathic.com, providing independent expert legal services on computer and Internet related matters. Until September 2001 he was also a Visiting Fellow at the LSE Computer Security Research Centre. He has an engineering degree and is a computer specialist as well as a barrister. From 1977 until 2000 he was in continuous practice at the English Bar specialising in cases involving computers which originally involved him in software copyright disputes and in dealing with disputes when computer systems did not work properly. He also became involved in criminal computing matters and successfully defended many young people in a variety of cases. Email A.Kelman@telepathic.com.

The Hutton Inquiry: How It's Done

"It is important that the public should know every word of evidence which is spoken at this Inquiry and should know the full contents of every document which is referred to in evidence."

Lord Hutton's Opening Statement

The Website - www.the-hutton-inquiry.org.uk Note from Mike Wicksteed of the DCA

The Prime Minister announced the setting up of Lord Hutton's Inquiry on 19th July. Officials in the Department for Constitutional Affairs (DCA) immediately took steps to build a website for the Inquiry which went live the following week - the aim being to keep it accessible and simple.

The web team is led by DCA's technical web manager, Catherine Arthur, and Phil Golding who is responsible for DCA Internet content management. They worked to create the Hutton website and have managed its daily running in addition to their normal DCA web responsibilities. In total about eight people (from the IT section at the Royal Courts of Justice, Hutton Inquiry secretariat officials and DCA web staff) have been involved off and on.

Systems for getting material onto the site were also kept simple. Personal information contained in documentary evidence was edited out by the Hutton Inquiry Secretariat, the files were then scanned into PDF format and passed to the web team to upload. An electronic format of the transcript of each morning and afternoon session was passed to the Inquiry web team for coding and posting onto the website with the aim of getting transcripts and daily evidence on the website within four hours of the end of each session. We mostly succeeded.

There are currently well in excess of 1,000 PDF documents on the Inquiry's website. Hearings started on 11 August and during August, daily unique accesses averaged about 13,500 and daily pages views around 200,000. There was a peak of 34,000 unique accesses and nearly 500,000 page views on 24th August when the first batch of full documentary evidence was posted up.

Transcription of the Hearings Note from Sarah Andrews, of WordWave

During the formal hearings, WordWave stenographers used their award-winning software LiveNote to produce highly accurate real-time transcripts, sent direct to participants' laptop computers as the evidence was given. Participants were also able to view documents, video links and other evidence easily throughout the proceedings.

At the end of each day, WordWave emailed the transcripts to the DCA web team, who published them on the web, giving the public and the media easy, speedy access to the Inquiry - of crucial importance in such a high-profile case.

Over the first 22 days of formal hearings, WordWave stenographers transcribed over 1 million words at speeds of up to 250 words per minute, maintaining an accuracy rating of 98 per cent - the gold standard for transcription.

Lord Hutton himself said "We have all greatly admired the remarkable skills of the stenographers in producing such an excellent and accurate record."

WordWave, (see www.wordwave.com) has also provided stenographers for the Shipman Inquiry, the Bloody Sunday Inquiry and, most recently, the Climbié Inquiry.

Two more in the series on publishers online

The Jordans Group

by Nicola Webb and Philip Wilmott

Jordans is one of the UK's leading professional services businesses: our strength lies in the range of services we offer. Some people know us as the leading independent law publisher and training provider in the UK; or the market leader in company formations; or leading providers of conveyancing and company searches and business information. The company was founded in 1863 in Bristol and now operates nationally (Bristol, London, Edinburgh and Cardiff), as well as internationally (British Virgin Islands, Cyprus, Gibraltar, and the Channel islands). The Group comprises several autonomous but linked companies: Jordans Limited (JL), Jordan Publishing Limited (JPL), and Oswalds - the trading name for Jordans (Scotland) Limited.

One thing the Group has in common is its early commitment to the online provision of its services. For example, Jordans Limited advised Companies House on its transfer to electronic filing in 1998 and was one of the first formations agents to be authorised to form companies electronically in 2001. Since then, the Group has launched a number of successful online products and those outlined below are just some of the key services it provides.

Jordans Limited

Jordans Limited's website is at www.jordans.co.uk.

Incorporator is JL's online incorporation module designed for users with volume formation needs (principally solicitors and accountants in private practice and in-house). There are no subscription charges; payment is by account number, with the price per formation charged being dependent on the annual volume. It was first launched in 1999 and there are now over 500 active users. The data capture screens are ordered in a logical process with useful aids like search and address look-up features. Users can choose from a range of Memorandum & Articles and we can also customise the software to include the user's own precedents, if preferred. The service is fully electronic, with printed forms and registers supplied (which can be stored electronically to minimise paper production). Orders are confirmed online and users are notified by email once their company has been incorporated (usually within 3-4 hours, depending on Companies House but always guaranteed within 24 hours).

PCSec is stand-alone PC-based software which provides an annual company secretarial service for multiple users (mainly company secretaries, solicitors and accountants). Launched in 1995, it now has over 400 active users. The software produces all the statutory documentation automatically, including forms, minutes, resolutions and notices to effect corporate changes, as well as providing guidance checklists and reminders of time critical events. It creates and maintains the statutory Registers automatically and statutory forms can be filed electronically.

JordanWatch is a leading online business information product. Users can search through the complete Companies Index of over 2 million records and access basic company details (address, telephone, turnover, number of employees and more) all at no cost.

Users wanting more information can buy online company profiles (analysed reports showing trends and performance levels over a number of years). Alternatively, they can order a company search, which is prepared by JL's team of specialists in Cardiff and emailed (or faxed/posted if

preferred) in a matter of hours. Payment is either by credit card or by account and password for regular users.

Jordans Property, www.jordansproperty.co.uk, is the conveyancing support services business within JL. It offers property-related searches and reports online and is the fastest-growing area of online business within the Group. The website provides simplicity and ease of use for online services, including various environmental reports, available within hours, which incorporate a professional opinion from one of the UK's leading firms of Chartered environmental surveyors; planning reports providing land use policies, planning applications and development proposals within the surrounding area; drainage searches and Personal Local Authority searches.

Jordan Publishing Limited

Jordan Publishing, www.jordanpublishing.co.uk, publishes under two separate imprints of Jordans and Family Law, and produces a diverse range of publications and conferences that can take you from company formation to family breakdown. As publishers of distinguished works such as *Gore-Browne on Companies*, *Children Law and Practice*, *Family Court Practice (Red Book)* and the *Family Law* journal and *Family Law Reports*, Jordan Publishing has a wealth of material being developed for online provision.

Law Reports Online, at www.lawreportsonline.co.uk, were launched in 2000 and host the full archive of our specialist law reports, including the *Family Law*, *Bankruptcy and Personal Insolvency*, and *Immigration and Nationality Law Reports*. As well as hosting the entire archive, *Law Reports Online* publishes the latest cases as soon as they have been prepared, often well in advance of the printed report. Free trials are available.

Free Family Law Resources, at www.familylaw.co.uk, provides two free online resources, the Family Law Online Index and Family Law Update. The former provides key details on all Articles, In Practice items and Case Reports published in Family Law since 1996. The Family Law Update service contains summaries of cases, legislation and practice developments of interest to family lawyers.

New Product Development: building on the success of the book comes the online version of Jordans *Civil Court Service* (Brown Book), now firmly established as one of the most widely used civil procedure texts. The online version is due to be launched in Spring 2004.

Journals Online: *Family Law* and *Child and Family Law Quarterly (CFLQ)* will soon be available online via journals aggregator, Ingenta. With over 5000 journals already available through Ingenta, the service will offer full text searching and downloading of the latest *Family Law* and *CFLQ* articles. It also allows non-subscribing customers to download journals on a pay-per-view basis. Ingenta will host all new issues, plus 2003 back issues. More details will be available from 2004.

Oswalds

Oswalds, www.oswalds.co.uk, provide a comprehensive company search and formation service which includes Sasine registry and land registry searches, company information and formation, shelf companies, conveyancing and conveyancing support services in Scotland.

Nicola Webb is Marketing Consultant, Jordans Limited and Philip Wilmott is Electronic Product Manager of Jordan Publishing Limited. Emails: nicola_webb@jordans.co.uk and philip_wilmott@jordanpublishing.co.uk.

The Incorporated Council of Law Reporting for England & Wales

By Martha Hawting

The Incorporated Council of Law Reporting for England and Wales (ICLR) is the publisher of the most authoritative law reports in the UK. The Council publishes The Weekly Law Reports, The Law Reports, which appear monthly with the addition of the argument of counsel, The Industrial Cases Reports, The Statutes & Public General Acts and The Consolidated Index. In addition ICLR provides The Daily Law Notes and The Industrial Cases Reports Express free of charge via the council's website (www.lawreports.co.uk). Here you can also find an online version of our free, thrice annual, student newsletter.

ICLR was founded by judicial and government officials in 1865 as a "not for profit" publisher, and the first volumes of the Law Reports appeared in 1866 by which time there were over 400 subscribers at 5 guineas a year. In 1870 the Council was incorporated under the Companies Act with the object of "*The preparation and publication, in a convenient form, at a moderate price, and under gratuitous professional control, of reports of judicial decisions of the superior and appellate courts in England.*" In 1970 the Council was registered as a Charity.

The Council now has subscribers in over 100 countries and its reports are published simultaneously in London, Delhi (for India, Pakistan, Bangladesh, and Sri Lanka) and Beijing for China except Hong Kong. The Council consists of members nominated by each of the 4 Inns of Court and by the General Council of the Bar. The two government law officers and the President of The Law Society are ex officio members. An executive committee sits once or twice a year and the full council meets once a year.

The Council is purposefully selective in choosing which cases to report selecting only those cases which set precedent, develop a point of law or raise interesting points from a legal perspective. All ICLR reporters are barristers or solicitors who are present in court for the hearing and handing down of judgment, the reports are submitted to the judges concerned for consideration prior to publication, and references and citations are carefully checked to ensure the highest levels of accuracy are maintained.

The Weekly Law Reports have been published by the ICLR since 1953. They are the only series of Law Reports to cover cases heard in the House of Lords, Privy Council, the Court of Appeal, all Divisions of the High Court and the relevant decisions of the Ecclesiastical Courts, the Employment Appeal Tribunal and the Court of Justice of the European Community. The Law Reports consist of the most important cases reported in volumes two and three of The Weekly Law Reports and are unique in that they include the arguments of Counsel. The Law Reports are the most authoritative reports and must always be cited in preference as required by the Supreme Court Practice Direction [2001] 1 WLR 194:

Citation of judgments in Court

3.1 For the avoidance of doubt, it should always be emphasised that both the High Court and the Court of Appeal require that where a case has been reported in the official Law Reports published by the Incorporated Council of Law Reporting for England and Wales it must be cited from that source. Other series of reports for England and Wales may only be used when a case is not reported in the Law Reports." Lord Woolf CJ.

The Industrial Cases Reports, published since 1972, are ICLR's only specialist series. They cover cases heard in the House of Lords, the Court of Appeal, the High Court, the Employment Appeal Tribunal and the European Court of Justice as well as cases of special interest from the Privy Council, The Court of Session and employment tribunals. The subject matter of the reports is wide ranging, covering all aspects of discrete Employment and Discrimination Law - in fact the ICR covers more cases than any other specialist series on Employment Law. The Recent Points section of the ICR summarises cases from the Employment Tribunals that are of interest but do not merit a full report. Combined with the Cumulative Indexes from 1972 to current, The Industrial Cases Reports are indispensable to any lawyer working in this field.

There are also CD-Rom and on-line editions of The Law Reports, The Weekly Law Reports and The Industrial Cases Reports, available via *Justis* (www.justis.com). The Law Reports Archive is also licensed to WestLaw, Lexis and Butterworths Direct.

Free Services

In addition to our core publications, our reporters produce The Daily Law Notes and The Industrial Cases Reports Express, found free of charge at www.lawreports.co.uk. The Daily Law Notes is a 24 hour service from the Royal Courts of Justice and European Court of Justice, bringing you the most important updates from the House of Lords, the Privy Council, the Court of Appeal and all divisions of the High Court. The cases reported have been summarised and are not the full text version that will appear in due course in The Weekly Law Reports, The Law Reports or The Industrial Cases Reports. What you will find here, however, is a precise and, above all, accurate summary of those cases deemed by our reporters and editorial team to be worthy of a fuller treatment and inclusion in The Weekly Law Reports.

The Industrial Cases Reports *Express* is designed to bring you previews of The Industrial Cases Reports before they become available in print form. They take the form of brief but considered summaries which give the ratio of the decision and are updated as soon as headnotes become available. This service is useful for keeping up to date with the very latest developments.

Martha Hawting is Marketing, Website and Education Co-ordinator at ICLR. Email MarthaH@iclr.co.uk

Scottish Session Cases Online

Note from Anthony Kinahan

Robert Reid's magnificent Upper Signet Library in Edinburgh saw the launch on 13 October by Context of Electronic Session Cases. During the past year The Scottish Council of Law reporting has developed a database of its *Session Cases* law reports back to 1930. This database has been licensed to a number of online data providers. Context are the first information provider to include *Session Cases* amongst their services and have now launched Electronic Session Cases as a library within their Justis range of electronic products.

The SCLR (see www.scottishlawreports.org.uk for their new website) is a non-profit making body, founded in 1957 to manage the publication of *Session Cases*, Scotland's 'official' and most authoritative series of law reports.

It is the Council's plan to extend coverage of the *Session Cases* database back in time as funds become available.

Domains Are Hot Property by Tim Brown

After the dot com bubble popped in the late nineties many commentators wrote off the Internet as a dead duck. The seeming myriad of "we-sell-aardvarks2u.com" e-businesses gave it a bad name. The Internet wasn't considered a serious player in the global economy and therefore its legal setup, matters of policy and governance were consigned to the back-burner by mainstream business as something of little interest or concern.

Skip forward to 2003 and where are we now? The Internet is ubiquitous. Mainstream commercial activity has become dependent upon email and, to a lesser but still significant extent, the web. Ask yourself what it would be like to be without access to your favourite business websites and your corporate email, even just for a day. So what is all this resting on? The domain name system. Meanwhile, how that system is governed and operated, and by whom, has now become of vital importance.

Matters of Internet policy and governance are controlled by a diverse range of different organisations – some, like IANA (Internet Assigned Numbers Authority) are concerned with purely technical matters of policy; others, like Nominet in the UK, have jurisdiction over a country's domain names; and other organisations are concerned with managing policy relating to generic top level domains like .com which affect all global Internet users.

Such is the lack of attention to Internet policy in general that the biggest recent story was Microsoft's decision to close down some of its chatroom services. Yet while the media decided to cover this largely irrelevant and public relations-induced announcement, a major fight was breaking out over actual control of the domain name system itself, following a fundamental change which had quietly been made to the entire Internet - affecting every browser and email client worldwide. This story, and one or two other current policy and governance developments, are covered below.

Trouble at the top - SiteFinder

September saw perhaps the most controversial issue relating to Internet policy ever to have struck the Internet. This was the unilateral introduction of a new "Site Finder" service by Verisign (the operator of the global .com and .net registries) raising questions as to which body is ultimately in control of the Internet. Verisign's "Site Finder" service began to operate on 15th September and resulted in users who mistyped .com or .net domains in their browser being redirected to a web site run by Verisign, rather than receiving a standard error message or one generated by the browser.

The Site Finder page suggested a list of related domains that the user might have been trying to reach and provided a directory of web sites. Verisign claimed that this service was provided to help Internet users find the sites they were looking for. However, it was also noted that the directory of web sites included sponsored links and other advertising which was generating revenue for Verisign.

To enable the service, Verisign used its position as the .com and .net registry operator to create a "wildcard address record" so that all attempts to reach a site, except those with valid domain names, resulted in redirection to Site Finder. Registries are the entities that ultimately run top level domains by maintaining the DNS databases which act like giant Internet phone books. The database matches the domain you type into your browser with the IP address for

the computer you are attempting to contact. As there can only be one such database for each top level domain, companies like Verisign have a monopoly position by virtue of technical necessity.

The launch of Site Finder proved extremely controversial – a non-technical analogy might be if a telephone provider with a monopoly position in the marketplace suddenly changed their standard message: "the number you have dialled has not been recognised" to a message stating "the number has not been recognised but here are some other numbers which you might have been trying to reach [and some advertisements as well]". Imagine, too, that this message is provided only in English all across the world regardless of the local language of the telephone user.

SiteFinder raised a number of technical concerns as, in effect, every possible domain in the .com and .net space now appeared to be registered – breaking some anti-Spam software and other applications. There were also privacy concerns in that misdirected email would be "bounced" by Verisign's servers rather than simply generating an error message. In theory such emails could be monitored, archived or otherwise used by Verisign – although they had no plans to do this at launch.

In addition, some commentators noted potential intellectual property difficulties in that by redirecting misspellings of domain names corresponding to trade marks Verisign could somehow be passing off.

In light of these concerns the body charged with matters of Internet policy and governance, the Internet Corporation of Assigned Names and Numbers (ICANN), requested that Verisign suspend the service pending further investigation of its possible effects. Verisign, however, refused to do so, leading to a Wild West showdown. After an initial exchange of correspondence and a brief standoff, ICANN gave Verisign an ultimatum with a time limit - although what they were going to do if Verisign did not comply was very much in doubt. Some commentators thought that ICANN might not be able to enforce the registry operator's contract against Verisign - the only option which it had in reserve.

While Verisign finally backed down by ICANN's final deadline on 4th October, it is highly significant that the registry felt it could challenge ICANN's authority by refusing to remove the SiteFinder service for nearly two weeks after the initial request – a move which affected millions of Internet users and sent Internet Service Providers scurrying to rework their network architecture.

There have been other challenges to ICANN's authority over the last year or so and mutterings throughout the Internet community that perhaps other bodies, such as ITU (International Telecommunication Union) could do a better job. However, the US Department of Commerce, which awards the contract to govern the Internet, has renewed ICANN's contract for another three years. So at least for the time-being ICANN is here to stay.

Domain disputes

Another area of interest is the development of dispute policies by generic and country code domain operators. This is of great importance to lawyers and others wanting to protect their intellectual property rights on the Internet and especially when enforcing rights against cybersquatters or domain speculators. Dispute policies vary enormously in both application and effectiveness. Two contrasting examples may be taken from Nominet's approach in the UK and that of DENIC in Germany.

Nominet's Dispute Resolution Service (DRS) is one of the most admired and successful domain mediation and arbitration procedures. Since its launch in September 2001 approximately 1,000 complaints have been received by Nominet with a sizeable proportion of these being settled at the first informal mediation stage and around 160 cases being referred to an independent expert for decision. The system is seen by many commentators as a cost-effective way to challenge conflicting domains and the quality of decision is generally seen as impressive. In addition, the DRS is also one of very few domain arbitration systems that includes an appeals system – where decisions by the first instance expert can be reviewed by a three member panel. Ultimately a successful complainant may receive a transfer of the disputed domain name - in a step that takes place directly at the registry zone file, so that issues of foreign jurisdiction or remote registrants are minimised.

By contrast, the German naming authority DENIC does not have any system of domain arbitration. Conflicts over domain names must be thrashed out in the courts. On application and with supporting evidence of a trade mark conflict the German naming authority may be prepared to mark a domain "under dispute" which prevents the name being transferred to another user. However, this is a relatively neutral step which does not stop the current user from operating the domain for web or email services. Some therefore regard such a notification policy as rather toothless. However, the Italian country code registry has the best of both worlds - a "dispute marking" system and an arbitration procedure.

The contrast between the UK and German systems exemplifies the problems with global brand enforcement – there are over 250 different country code and generic top level domains, many with their own dispute system. Some countries, such as Ireland, the Netherlands and Switzerland have recently introduced new dispute policies while others have plans to do so in the future; still more are sitting on the fence. It has become increasingly difficult for intellectual property practitioners to keep abreast of the changes to each country code regime and it does not look like the operators are set to consolidate their policies or approaches any time soon.

IDN's

Another developing area of interest concerns Internationalised Domain Names (IDN's). These are domain names which can include non-standard character sets - accents, umlauts, non-western language alphabets etc. They present particular problems in terms of Internet policy and intellectual property enforcement because of the conflicts that can arise. For example, in a system where both café.com and cafe.com can co-exist, problems are perhaps inevitable.

Support for IDNs is mixed, with Afilias – the body that runs the .info generic top level domain – recently announcing the introduction of umlauts for .info. By contrast, the French naming authority – AFNIC – has come out both for and against IDNs, on the one hand welcoming their ability to recognise French language characters, yet also warning that they may lead to spiralling costs for businesses trying to protect their intellectual property by buying every possible combination of domain that might be similar to their trade marks.

Some registries are considering 'bundling' IDNs by offering them to the existing registrant of the corresponding standard character-set domain. This in itself may open a can of worms, bearing in mind the potential competing claims to the bundled names. Similarly, businesses are

having to decide whether they want to convert their name directly into local language scripts in order to effect blocking registrations or whether, culturally speaking, an IDN should reflect a more descriptive approach to the mark. This would represent the difference between Lloyds TSB registering a transliterated version of their name in Chinese characters or registering 'big black horse' (or whatever the appropriate cultural descriptive for their business might be in China) or indeed both.

Given that English is not the first language for vast numbers of Internet users, IDNs are an inevitable development which is here to stay; how the law and policy will develop is not at all clear.

New TLD's

As noted above, there are over 250 country code and generic top level domains, each with their own changing policies and governing bodies, and with varying approaches to disputes. If this were not enough to contend with there are plans to introduce more domains over the next few years.

For example, the President of ICANN hinted heavily earlier in the year that three new generic top level domains would be introduced to complement existing gTLDs like .com and .net. In addition, the European Union was given the go-ahead to introduce the new .eu domain (technically, for Internet governance purposes, a country code - one wonders what the Euro-skeptics would think if they knew!) which is provisionally due to be launched later this year.

The rules concerning how these new domains will work, who can apply for them and how disputes will be settled are still developing. One topic under discussion has been whether there should be a 'taxonomy' for the Internet domain name space - accepted categories of new domains to be introduced. There are very strong views both for and against and the ultimate decision may affect the whole appearance of the domain name space for years to come.

.eu will be especially important in the UK when it is finally launched. We know from the European legislation (and in this fuzzy world of Internet governance it is relatively unusual to have any legislation underpinning the introduction of a domain name) that there will be a 'sunrise period' where existing trade mark holders may apply for a corresponding domain name, but the seniority of marks and the timing of the launch are still wide open.

The future

With all these areas still under development, the Internet is undoubtedly in its infancy. Perhaps it is unfair to expect significant maturity where, for example, the domain dispute regime is some three years old compared to over a century of trade mark policy, legislation and experience. However, never before has a technology so important, so global and so central to modern living arisen so quickly; there is little place for the rather considered, reactive approach of the traditional global policy makers.

As the fight between ICANN and Verisign illustrates, before the Internet fully matures we must expect a few years of teenage rebellion.

Tim Brown is a Senior Domain Name Consultant with Edinburgh-based Demys Limited (www.demys.com). Demys handle Internet brand matters for an international client base and publish a free domain news service for business at www.demys.net. Email t.brown@demys.com

Practical Problems of Digital Signatures by Stephen Mason

The move towards e-conveyancing will require practitioners to use digital signatures and obtain separate insurance to cover the security of the computer system they use.

A digital signature can comprise three elements, a key pair (a private key and a public key) and a certificate, which is usually issued by a third party such as a certification authority. When an electronic document or message (hereinafter only a message will be referred to) is signed with a digital signature, the private key is used to associate a value with the message using an algorithm. The computer undertakes this task. The value, the message and a certificate linking the private key to the named person or entity, is then sent to the recipient. The recipient uses the public key to check the value is correct by 'unlocking' the value created by the algorithm. A computer undertakes the entire operation of affixing a digital signature by a sender, and the checking of a digital signature by the recipient. The only action required of the human being (in theory) is to cause the computer to associate the digital signature to the message. Depending on the software used, the recipient is not be required to do anything other than open the document, and the computer will do the rest.

Most computers now have the ability to generate a key pair, although if you generate your own key pair, you will then need to distribute the public key. Alternatively, you can subscribe to a certification authority for the provisions of a certificate, and either the certification authority will generate a key pair, or more often, a specialist trusted key generation company undertake this task. Digital signatures can be obtained in the name of an individual or a body corporate.

A certification authority acts as a trusted third party. Depending on the nature of the certificate, it may verify the identity of the party applying for a certificate. The certificate is then linked to the private key, and the public key is placed in a public depository, thus eliminating the need to distribute the public key. A person wishing to obtain the public key downloads a copy. The certificate associates the private key with the subscribing party. When a certificate is revoked for some reason (where it has been compromised, for instance, or has expired), the certification authority places a notice to this effect in a certification revocation list.

Storage and security

Any person using a private key must pay careful attention to storage and security. The private key should be stored in the computer in such a way that only the owner has access to it. The prevention of unauthorized access is usually effected by way of a password or series of passwords, but can also include the use of a physical token, such as a smart card or a biometric measurement, such as a fingerprint measurement (although the use of biometric measurements is very dangerous, since the person whose measurement has been taken will be exposed to difficulties in the future if their measurement is stolen and used without their knowledge).

Where an outsider intends to attack the computer or system, the first line of attack will be to crack a password. This is relatively easy for any attacker to accomplish, given the propensity of most users to use words that are susceptible to automated attack, such as dictionary attacks. Thereafter, weaknesses can be manipulated in the security system itself by a hacker, whereby a hacker enters the system and leaves a Trojan horse that permits them to activate the computer and gain entry to the files at a time of their choosing, and to use the private key to send messages that are signed with a digital signature.

A range of attacks are theoretically possible, not all of which are associated with taking over the computer of the sending party. For instance, the 'root' key of the certification authority can be replicated, which means it is possible to make the recipient believe they are communicating with the legitimate sending party, when they are, in fact, communicating with an impostor. Private keys are also prone to being misused by employees or contractors, which means appropriate security should also include provisions against such risks.

For those using Microsoft software, if you look in Outlook Express: Tools – Options – Security, you will probably find a number of certificates relating to various certification authorities already loaded into the computer. The certificates are relatively easy to navigate, depending on the version of software on your system. If you want to use a digital signature, it is probable that you will have to ask somebody to help you install one, although some users may be familiar with how to undertake this task.

International Commercial Arbitration from **Westlaw UK**

Sweet & Maxwell has just announced the launch of a new service, Westlaw UK International Commercial Arbitration. Containing over 100 UK and International databases, all interlinked and fully cross-referenced, this unique service provides you with fast, easy access to the most authoritative materials available.

For your 30 day free trial of **Westlaw UK International Commercial Arbitration**, or for further information, please call 0800 028 2200 or email enquiries@westlaw.co.uk.

“The indispensable resource for any arbitration practitioner”

Service includes:

- * Leading commentary from the pre-eminent text *Law & Practice of International Commercial Arbitration* by Redfern and Hunter
- * The latest news, cases and international case summaries from the *International Arbitration Law Review*
- * UK and International Commercial Arbitration case locators and legislation locators - everything you need to know in one place
- * Legal Journals Index - international commercial arbitration articles from over 800 journals, with links to the full text
- * Current Awareness - tailored summaries of the day's developments in arbitration law and practice by 9 am, with updates throughout the day
- * Plus hundreds of international databases.

The relevant legislation

In the United Kingdom, the Electronic Communications Act 2000 applies to electronic signatures, and the Electronic Commerce Act 2000 applies in Ireland. By s10(1)(c) of the Electronic Commerce Act 2000, the provisions relating to electronic signatures do not apply to the creation, acquisition, disposal or registration of land in Ireland, although the Minister has the authority to make regulations under s3 of the Act.

Electronic conveyancing

With respect to electronic conveyancing, those intending to contemplate providing an electronic conveyancing service should carefully study the provisions of Part 8 s91 of the Land Registration Act 2002. It is not quite clear what the provisions of this section actually mean, although there are a number of options:

1. The combination of s91(3)(b) and s91(4) could be construed as an irrebuttable presumption that the purported signatory did in fact sign an electronic document.
2. Alternatively, these provisions can be construed that the document has in it or associated with it something that, at common law, is the signature of the relevant party.
3. Further in the alternative, by reference to s91(10) and ss7(1) and 15(2)(a) of the Electronic Communications Act 2000, for an electronic signature to be effective, it may be necessary to demonstrate that it came from each person by whom the document purports to be authenticated, and the use of the electronic signature was intended to have a legal effect.

It is not clear what meaning to attribute to the provisions of s91, but what is obvious, is if a practitioner intends to spend the money with the Land Registry and offer electronic conveyancing, they must sign up to the land registry network by way of a network access agreement. The practitioner will be required to have separate, compulsory, insurance cover for the security of their computer system, in accordance with the provisions of schedule 5 paragraph 11(3)(c). As it is difficult, if not impossible to quantify the potential losses, and as both the largest firm and the single practitioner can suffer from the same attacks, the cost of such insurance will fall disproportionately on the smaller firm. Unless there is any evidence to the contrary, the introduction of electronic conveyancing will significantly increase the costs of conveying property.

Assumptions about digital signatures

A number of assumptions are made about the process of using a digital signature:

1. Where a person has a digital signature, they cause the signature to be associated with the message.
2. A recipient, when they open a message that has been signed with a digital signature, can be sure that the sender actually caused the digital signature to be associated with the message.
3. The certificate that accompanies the digital signature confirms the link between the private key of the sender and the certificate, and therefore confirms that the message was sent by the person whose private key was used.

None of these assertions are true. In addition, these assertions are very difficult to prove using the present infrastructure. The only way of ensuring the sender actually caused their computer to associate their digital signature with the message in question, is for the sender to confirm

they signed the message, preferably in writing, by way of e-mail, facsimile transmission or letter.

The risks

The sender: Where a digital signature is used, it is crucial to ensure the private key is stored with maximum security. Unauthorized use of a private key to create a digital signature could cause the sender to demonstrate they were negligent in securing the private key, should they wish to disassociate themselves from the content of any message signed with their private key. This will be expensive, time consuming and embarrassing. The ability of a determined attacker (whether from the insider or externally) to use a private key may be such that any private key, however it appears to be secure, will be exposed to unauthorized use. Thus it cannot be said with any certainty that every digital signature associated with a message was necessarily sent by a sending party.

The recipient: Whilst the sending party will, in most cases, be contractually bound to provide for the security of their private key, the recipient of a message signed with a digital signature is not so bound. Certification authorities, in order to shift liability, make it a condition of reliance on the certificate, that a recipient becomes a verifying party, and thereby a relying party. A certification authority will normally have a document called a 'Relying Party Agreement', which purports to require the recipient to undertake a significant number of checks to verify the authenticity of the certificate that accompanies the digital signature before they can rely on the information contained in the certificate. Even if a recipient undertakes this task comprehensively and successfully, the only guarantee they have from the certification authority is this: that there is a link between the person or entity named in the certificate and the existence of their private key. There is no assertion that the owner of the private key that was used to associate the digital signature to the message actually caused the digital signature to be associated with the message. This means the recipient must still telephone or write to the sending party to confirm they sent the message.

The uses of digital signatures

If you have a sophisticated infrastructure and regularly need to send information to recipients that do not believe you sent the message just because your name is typed at the bottom of the e-mail, then you may consider that the use of digital signatures, despite their risks, are of some use. One use of digital signatures is where a big organization wants its employees to gain access to the corporate infrastructure remotely. A virtual private network (VPN) is created, by which the two computers exchange a protocol to authenticate each machine. The user then authenticates themselves, usually with a password. However, if an attacker has gained access to the relevant passwords, the person logging on remotely may not necessarily be an authorized employee.

When you send an e-mail, you add your name to the e-mail. This is a form of electronic signature, and binds you to the message in the same way as a digital signature. If a recipient doubts that you sent the message, they can always telephone you to confirm it was sent by you.

© Stephen Mason 2003. Stephen Mason practices from St Pauls Chambers, Leeds and specialises in authentication, electronic signatures, e-business, e-mail, e-risks and commercial law. Stephen's book "Electronic Signatures in Law" is to be published by Butterworths in the autumn of 2003, see www.butterworths.co.uk. Email stephenmason@stephenmason.co.uk.

How to Avoid Spam by Alan Tomlinson

Whilst time wasting is the main Spam related complaint of most email users, the volume of this irrelevant and sometimes offensive material has other implications. To the IT Manager or Service provider, Spam takes up 'bandwidth' and thus has a bad effect on the performance and cost of its network infrastructure. Whilst everyone wants to keep users happy, to simply treat the symptoms is to miss the point, and uses up yet more network resources. Providers of desktop Anti-Virus & Anti-Spam products and services will whistle all the way to the bank whilst wholesale methods of prevention continue to be largely overlooked.

Various Anti-Spam organisations exist to try to curb unsolicited mail. When specific servers are reported to these organisations, they ultimately become 'blacklisted' and ISPs can then use the lists to block mail from offenders to their customers. If Spam is properly reported and the lists are responsibly used, this is very effective and can stop the problem at its root. ISPs who become listed due to the activity of their customers must take responsibility to find and suspend the offending user accounts very quickly.

'Spammers' can, however, avoid becoming 'blacklisted' themselves by using other people's servers & Internet connections to relay mail on their behalf. By sending a few short commands over the Internet, improperly configured servers belonging to unsuspecting Internet users can be made to distribute junk mail. Such misconfigured servers are disturbingly common, in fact until quite recently the default setting for MS was to act as an 'Open Mail Relay'. This effectively allows anyone with sufficient knowledge to send their Spam at little or no cost, or risk of being identified. Many IT companies despite impressive looking certification by software manufacturers, are guilty of failing to secure servers by not changing default software settings, and/or not keeping them up to date on security service packs & patches.

ISPs with customers running 'Open Mail Relays' face the very real prospect of being blacklisted, whilst the real offenders remain unhindered, other than having to find new servers to do their dirty work. In reality organisations responsible for spamming, compile lists of servers they can use in much the same way that they harvest email addresses. If this ability to hide their identity were curtailed, sources of spam would be relatively easy to detect and thus filter. To this end responsible parties, Lawyers Online included, have systems to scan for 'Open Mail relays' among those attempting to send mail across their networks. The owners of such servers can be told get them properly configured or even reported directly to 'blacklists'.

The article continues with detailed suggestions as to how to avoid being spammed when building a web site or when using other peoples' web sites; also what to do with received spam. Download the full article as a Microsoft Word document from www.venables.co.uk/n0311mat.htm.

Alan Tomlinson is Business Director of Lawyers Online Ltd, www.lawysonline.co.uk, email alant@lawysonline.co.uk. Lawyers Online was founded in 1998 by a busy Sole Practitioner, Rosie Houghton, who was dissatisfied with the range of substandard and/or overpriced 'professional' ISP services for Lawyers. The company has grown to provide 1500+ multi-user Firms, Chambers and Legal IT companies with Dial-up, ISDN & Broadband Connections, as well as bespoke Mail delivery, Web programming and IP Security services. The company remains privately owned and is managed by Directors Alan Tomlinson and Bill Naylor.

The Electronic Irish Reports and Digests on Justis.com by Nuala Byrne

The *Irish Reports* and *Irish Digests* are published by The Incorporated Council of Law Reporting for Ireland. The *Electronic Irish Reports and Digests* have been available from Context on CD-ROM since May 2000 and in March 2003 were included in the online service Justis.com.

Nuala Byrne's review of this product can be found at www.venables.co.uk/n0311mat.htm. She concludes that "the Justis products are well designed with the end user in mind" and that "there are many features incorporated into the technology to help with the search process".

Nuala Byrne has been the Law Librarian of the Director of Public Prosecutions in Dublin since 2001. The Library is on two sites, with 6 staff members. Before that, she was Business Librarian at Dublin City University. Email nbyrne@dppireland.ie.

More Specialised Websites by Delia Venables

In the last issue (see www.venables.co.uk/n0309joa.htm), Lorraine Chapman of Field Fisher Waterhouse, described the specialised websites developed by her firm, including sites for brand protection, equity incentives, employment, European franchising, public sector, patents and sports business. These sites enable the firm to provide focused information in a style appropriate to that industry sector, matching the concept of a specialist shop; you would not go to a supermarket for some jewellery, she said.

Whilst few other firms have developed quite such a series of specialised sites, it seems as if many firms are trying out the concept of specialised sites along the lines of "If you've got it, flaunt it".

Here are some of the sites which have appeared over the last couple of months, and which show the very wide variety of topics which can be adopted for this approach. Some of these allow for actual purchases of services from the site but most simply lay out the expertise without too heavy a sales presence. (For an extended version of this article and web addresses, see www.venables.co.uk/n0311mat.htm)

Iraq Information is a site set up by international law firm Bryan Cave to assist companies wishing to obtain contracts for the redevelopment of Iraq.

drinkslaw.com is a site from Howes Percival intended as a source of information on the new Licensing Act and an On-line Liquor Licensing Ordering Service.

Shareholder Rights is a new site set up by Brabners Chaffe Street which aims to outline the legal position of shareholders in a Private Limited Company.

frenchpropertylaw.co.uk is a site from Russell-Cooke all about French property purchases.

abuselaw.co.uk is a site provided by solicitors Stewarts of London and Leeds to provide information for child and adult survivors of physical, sexual and psychological abuse.

These are just the most recent ones! There are dozens more specialised sites listed on my own website at www.venables.co.uk/firmsx.htm.

EGi's Legal Service - fully briefed on property law

EGi's Legal Service at www.egi.co.uk is the UK's leading online news, research and information service for property law professionals. Offering fast and easy access, their extensive databases provide:

- * Case Summaries
- * Estates Gazette Law Reports & Planning law Reports
- * Property Law News
- * Property Legislation
- * Estates Gazette Legal Articles
- * Claims
- * Lands Tribunal
- * Practice Points - Expert commentary on recent property issues

EGi also offers a range of additional researched services that concentrate on specific areas and sectors of the property market including Shopping Centre Research, London Office Database and Distribution Database.

For more information or to request a free trial please call us free on 0500 557788 quoting ref:003.

JustCite from Context - your window on to a world of legal information!

JustCite, the legal citator from Context, is the only tool that gives you fast and easy access to full-text documents on a variety of leading services, including Butterworths, Justis and many more. With JustCite, you can...

- √ identify a specific case and view its subject matter and parallel citations;
 - √ link directly to other cases and legislation judicially considered on the service of your choice;
 - √ find a UK Statutory Instrument and link to its enabling Act, amended and amending legislation;
 - √ identify UK Acts of Parliament, view their profiles and link to related case law and legislation; ..and much more!
- Contact us quoting VEN5 and receive a free no-obligation trial.

For further information, visit JustCite www.justcite.com, call 020 7284 8080 or email sales@context.co.uk.

Jordans - Market Leaders

In the market for a formation? Choose the UK's leading supplier...

- * You can provide formation details online or by phone, email or fax
- * Your data is filed electronically at Companies House
- * No paper forms to complete
- * 87% of our clients are repeat purchasers and 98% are happy to recommend us to others
- * We offer ongoing business support via our company secretarial, legal, accounting and intellectual property protection services.

For further information, visit www.jordans.co.uk, contact Mark Bevan quoting reference INL03 on +44 (0)20 7400 3316 or email mark_bevan@jordans.co.uk. Jordans Limited, 20-22 Bedford Row, London, WC1R 4JS.

The 8th Annual Intellectual Property Law Conference from CLT

27th January 2004, Berners Hotel, London

All the important cases, statutory developments and legal trends.

Chaired by Jeremy Phillips, Slaughter and May.

- * The year in perspective - a global overview
- * Confidence, privacy and the Human Rights Act
- * Copyright
- * Patents
- * Round-up of trade mark developments
- * The new European law on trade mark infringement
- * Recent developments and trends in IP litigation.

For more information, or to book, visit www.clt.co.uk, email registrar@centlaw.com or ring 0121 355 0900.

The 6th Annual Information Technology Law Conference from CLT

26th January 2004, Berners Hotel, London

Reviews the important developments in e-commerce and information technology

Chaired by Jeremy Phillips, Slaughter and May.

- * Domain names and cybersquatting
- * E-commerce
- * Computer viruses: legal, liability, redress and enforcement
- * IT, surveillance and confidentiality
- * Internet service providers and the content they carry
- * Damages for internet-related IP infringement: the position after Reed v Reed

For more information, or to book, visit www.clt.co.uk, email registrar@centlaw.com or ring 0121 355 0900.

Make the most of your website with emis intellectual technology!

The right website can immeasurably strengthen client relationships. From the simple provision of information to fully interactive services: If your website is up to date and informative, your clients will know that they are dealing with a professional firm that puts its clients at the heart of everything that is done.

emis intellectual technology offers a wide range of services to help you make the most of your website, all tailored to your needs. emis can:

- * Design your site
- * Update an existing site
- * Write the content
- * Provide monthly digests of legal information
- * Set up online quoting for your services
- * Set up file status reports for your clients

Choose whichever service suits you best, and emis will fully project manage the work.

Call emis intellectual technology on 0845 120 5206, e-mail enquiries@emisit.com or visit www.emisit.com.