Internet Newsletter for Lawyers

Making the most of the legal web

July/August 2014

The future of law reporting

By Paul Magrath

The legal professions, however unwillingly, and indeed the English legal system itself, are undergoing profound changes. Law reporting is bound to adapt.

The range and type of information which needs to be published is changing. The model of a carefully curated selection of momentous precedents – cases which marked out a path of stepping stones in the development of the law – though still valuable, is no longer enough in an age of online aggregation and Big Data analytics.

Lawyers and students need cases for a variety of reasons, not just to witness a change in law. And, in electronic form, the storage and retrieval of vast hoards of information is both easy and cheap. This obviates the need and to some extent the rationale for only selecting and preserving the most important cases.

But is there still merit in the idea of selection, or at any rate some sort of evaluation system for judgments? And how else can a publisher of legal information add value in the digital age?

ICLR (www.iclr.co.uk) was founded in 1865 by lawyers frustrated by the inadequacies of the law reports then available. Next year marks the 150th anniversary of that foundation. It seems a good moment to re-examine ICLR's offering against the needs of the professions that were so instrumental in its birth.

The changing needs of practitioners

As users change, so do their needs and expectations. The changes to the legal professions are not, as some might hope, temporary constraints imposed by austerity.

Several forces are at work.

Funding

First, there has been a massive and irreversible reduction in public spending on the legal system. The Lord Chief Justice has spoken recently of a "period of significant retrenchment" of the state ("Reshaping Justice", 3 March 2014). The late 20th century model of a centrally funded legal aid system – something approaching a National Health Service in law – is in retreat, and the number of practitioners will shrink.

Regulation

Next, the deregulation of the professions. At first blush this looks paradoxical. The professions have never been so tightly regulated, with their independent disciplinary panels and their quality assurance schemes, and an uber-regulator (the Legal Services Board) to guard the guardians. But there's another force at work, which is the opening up of closed areas of competence for particular professions. Typical of this are rights of audience, which in the 1980s were extended from barristers to solicitors, in a process that has now reached the point where, in the Family Courts, unregulated and virtually unaccountable "professional McKenzie friends" (a somewhat oxymoronic description) are able to ply their trade, with the permission of the judge (for whom they may be preferable to a disorganised and panic-stricken litigant in person).

Lord Thomas (in the speech cited above) pointed out that the modern legal professions, and in particular their division into two main branches – barristers and solicitors – are a product of the sweeping changes made in a succession of reforms during the Victorian period. He seemed to be suggesting that a reorganisation of similar magnitude may well be occurring now, and things like alternative business structures are just the start of it. (That said, speaking as an ethical shareholder, I await with interest the day Tesco wins a pro bono legal award.)

Procedure

Of more concern, to a professional law reporter, were the Chief's remarks about the courts in many areas of law moving towards a more inquisitorial procedure. The development of the common law is dependent on adversarial argument, testing legal propositions before arriving at refinements of the law. How can that process continue in a non-adversarial environment? If the common law ceases to develop, then law reports cease to play the significant role they have occupied over the last several hundred years. That's not to devalue the function of making law available as information. But the primary function of law reporting has been that of keeping the profession up to date with the developing common law. (My blog on this is at www.iclr.co.uk/end-road-common-law.)

Technology

Another factor affecting the needs of users is, of course, technology. This, too, has been highlighted and indeed promoted by the Lord Chief Justice in the recent annual lecture to the Society for Computers and Law. This is not about accessing legal information using IT, or even about the MoJ's programme of installing wifi in all the courts (which is apparently going to take until 2017). It's the (long overdue) next stage of digitising the court process – to enable parties to file claims online, lawyers to exchange pleadings and bundles, and advocates to present written arguments using compound PDFs (eg as required by Supreme Court Practice Direction 14 – Electronic Bundles guidance).

How is ICLR responding?

To accommodate these changes, and make itself fit for the future, ICLR has embarked on an ambitious rethink of its entire operations, in four main areas: content, context, tools and access control.

Content

Before the internet, if a case was not reported, it was pretty well invisible. There were collections of transcripts, kept within the court libraries, and only accessible on special request; and transcripts of individual proceedings and judgments could be ordered (for a hefty fee) from the official shorthand writers or the mechanical recording department. But it was not until the development of BAILII and other online archives that the process of selecting a case for a law report ceased to be also a process of preserving the judgment itself for posterity. BAILII now gets 40,000 hits per day: it's become for a lot of users the go-to site for recent judgments, and is linked to by most media commentators and legal bloggers. Law reporters no longer occupy that rather lofty ideal of being the "guardians of precedent", saving the worthy new cases from the obscurity into which they would otherwise fall.

It's also worth bearing in mind that different users have different uses for legal information. Some need precedents, but some just need the "yardstick" cases which tell them what the current rates are for personal injury damages, or sentence for burglary, and a current awareness of the way the wind is blowing through the different divisions of the courts. Academics may choose to sift through hundreds of judgments to measure changes in the use of legal language. Legislators need help in finding and fashioning the language of new provisions, and in anticipating the courts' interpretation of their enactments.

It's as important to cater for all of these other uses, as well as those who simply want a collection of the critical precedents. And all of this militates against a purely selective approach. However, it makes sense to concentrate editorial resources on the cases that really matter. So ICLR will continue to do what it does best, and to give the most important cases the full treatment of the officially-approved series of The Law Reports, which are required by Practice Direction to be cited in preference for any other series on the same case. But it will also increase its coverage, using a "less-frills" approach, with full text reports of those cases which are of interest to practitioners in various areas of specialism, or because they contain small points or observations of more general interest. Then, for all the rest, the availability of a transcript, indexed and searchable, means nothing of possible use will be lost.

Context

Cases are not decided in isolation; the whole essence of the common law is its net-like interconnectedness. Earlier cases affect and are

Internet Newsletter for Lawyers is edited and published by Nick Holmes and Delia Venables
ISSN 2046-9284. Personal Print+PDF subscription (6 issues) £50. Personal PDF £30+VAT. Multi-use £80+VAT
Subscription information and online access are at www.infolaw.co.uk/newsletter
Subscription enquiries to infolaw subscribe@infolaw.co.uk 5 Coval Passage, London SW14 7RE Tel 020 8878 3033
Nick Holmes nickholmes@infolaw.co.uk (editorial, publishing) Delia Venables delia@venables.co.uk (editorial, advertising)

affected by later ones. For anyone researching case law, context is all. That is the value of Citator+, ICLR's powerful online index, which displays more than a century and a half's worth of editorial information about cases and about the relationship between cases - those published by ICLR and by other leading providers.

One of the ways in which ICLR will be expanding and extending the scope of Citator+ is through a joint Big Data for Law project with the National Archives (discussed in the March issue of the Newsletter). This will examine, among other things, the relationship between case law and statutes, and mine the former for links to and from the latter.

ICLR will also be expanding its links to case commentary from experienced legal bloggers and academic commentators, such as the UK Supreme Court blog (profiled in the March issue of the Newsletter) and the UK Human Rights blog.

Tools

From a user's point of view, it may not matter whether the vast range of content to which they wish to have access is all kept under one roof, or several. What matters is that they can go to one place to find it. The advantage of sucking in all the content your subscribers might want is obvious for a large commercial publisher with the resources to capture and keep it all. For ICLR, a charity of limited resources but hopefully not unlimited resourcefulness, the better solution is to provide a way of accessing content held on a range of different sites, without the need to perform more than one central search.

Thus ICLR plans to develop its search technology to enable users to find content not only within the various collections on the site but also those, like BAILII, EurLex and Hudoc, outside it. Most of this will be free content but held in different places. What will bring it together for the user will be a hub-like unified search.

Access

ICLR is not a profit-driven international publishing conglomerate whose subscriptions spiral ever upwards. Its articles of association require it to provide law reports "at a moderate price". It aims to be the "law service for the rest of us".

One of the ways ICLR currently acts in a pro bono capacity is by providing a free case law summary service – the WLR Daily – which includes a searchable online archive going back five years. Cases are selected on the basis that they will or may ultimately be reported in full by ICLR. There are links from BAILII and, via a widget on its main law page, *The Guardian*. For cash-strapped law centres and the increasingly numerous litigants in person, WLR Daily reports are – or should be – a godsend. Google will find them, of course, but only by name or citation. The free search on ICLR enables them to be found by subject matter, free text, judgment date, court etc as well.

ICLR is looking at other ways in which to provide some content for free, while also providing those who pay subscriptions with an even better service. It will do this by further developing its "freemium/premium" access model.

Thus for paying professional and academic subscribers, ICLR Online will be developing a number of its document management tools, so that busy users will be able to annotate, organise and file cases and other documents and incorporate them into an electronic bundle. It will be expanding the content available to subscribers, and the Citator+ overview in the context of which it can be viewed.

Conclusion

The legal world into which ICLR was born 150 years ago has changed beyond recognition, and the critical role played by ICLR, as the professionally founded and officially recognised provider of *The Law Reports*, setting a standard by which other series are judged, remains a key part of what it does.

Yet it is not the whole story. "Content is King", as potential subscribers keep telling us, but its value is only truly realised in a service that helps users find the content they need and displays it in the context of other relevant information and offers tools to enable users to manage and process it. With a balance of skilful selection and comprehensive accessibility, ICLR aims to add value rather than price in the digital age.

Paul Magrath is Head of Product Development and Online Content at ICLR (www.iclr.co.uk). He was formerly editor of the Business Law Reports and is now editor of the ICLR blog. He has written articles and reviews for The Times, The Independent, Counsel magazine and various journals.

Email Paul.Magrath@iclr.co.uk. Twitter @maggotlaw.

Illustration by Alex Williams (www.alex-williams.com) from the Queen's Counsel Cartoons series (www.qccartoon.com) © Alex Williams.

BYOD is no fun for SysAdmins

By David Flint

In the old days it was relatively easy to determine what devices were connected to the corporate network; they were large and cumbersome. Indeed, it was difficult for new devices to be connected to the network without the assistance of the corporate IT department; the confusing array of IP addresses and ports and the obscure art of modem configuration meant that it was well beyond most of us to do this.

For those who did require remote access, a pair of dedicated modems was needed and a telephone line which would remain stable and undropped for hours. I remember needing a line to remain connected for 7 hours, knowing that a click on the line meant that we would have to start again. Access to the network from outside could only be achieved through modems so, to ensure the integrity of the network, all that needed to be done was to check that there were no unexpected modems connected to phone sockets in the building.

If users were to be allowed mobile devices, these were in general confined to senior staff – none of whom could ever work out how to circumvent the controls. Mobile phones were just phones which were cordless. The IT department had total control over the devices used, what software was on them (if any) and nothing which was not IT controlled was allowed to access the network. Few users worked, or were expected to work, remotely.

Oh, how it has all changed!

As connectivity has improved and there has been more focus on work–life balance it has become more common for users to work remotely, whether from home or elsewhere. Users, particularly in the professional services market, are expected to be on call, or at least reading email, on an almost 24/7 basis.

As this explosion in connectivity has occurred, devices with the capability of being useful in a work context are no longer the preserve of a dedicated IT function. Most of us now have (several) computers at home, whether laptop or desktop, and it has become almost impossible to function in the 21st Century without access to the internet.

The IT department (or IT person) is faced with the challenge of users who need (or want) to access their corporate data remotely; the enterprise is unwilling, or unable, to provide every employee with a dedicated second computer for remote use and users in any case do not want to have a second machine lying unused for much of the time.

Add to that the fact that enterprises are generally slow to adopt the latest gadgets (recent statistics suggest that a significant number of enterprises are still using Windows XP, now 13 years old) and it is not difficult to see from whence pressures are coming.

In the mobile device space, the pressure is even greater; hardly a month passes without a super shiny new mobile phone (or "device") being announced; we are all subjected to the conundrum of contracts with our mobile phone providers being lengthened – 2 years now appears to be the norm – whilst few hip users would want to be seen with a phone which was as old as 2 years. No stylish individual wants to be seen with an (old) blackberry, when their friends, who are not constrained by an IT department, have the latest shiny toy. The suggestion of two phones – work and personal – is for many not an attractive option as it means carrying 2 devices, 2 chargers, 2 cables.

A BYOD policy

So, how can the enterprise meet the apparently conflicting challenges of corporate security and individual resistance? The individual would like to have a single, hip device; the enterprise, mindful of its obligations under the Data Protection Act, needs to ensure data security.

For all these reasons, an enterprise needs to have a BYOD (bring your own device) policy alongside its existing IT and data protection policies. Here are some of the requirements of such a policy.

- it needs to address issues such as ensuring that corporate secrets (whether personal data or not) are protected;
- it needs to ensure that anything which the employee does in their own time (perhaps unprotected by the anti-virus activities of the corporate IT service) do not have the effect of introducing malware into the corporate network by the back door;
- it needs to ensure that, if the employee's personal device is lost or stolen (evidently 70 per cent of us will lose a mobile phone at some time), any personal or confidential data can be wiped remotely;
- the enterprise needs to advise employees what information can (and cannot) be processed on their personal devices.

Other factors to protect the enterprise

In terms of the Data Protection Act, the enterprise will be responsible as data controller for all its data, whether held on the enterprise network or on an employee's personal mobile phone. Best practice suggests that work data should be kept in a separate (password protected) folder and excluded from any cloud backup – easier to do on a laptop perhaps than on a mobile phone.

Remote access to enterprise resources should be through a secure channel (which almost certainly doesn't include your local coffee shop or hotel); VPN (virtual private network) software is readily and inexpensively available (whether as part of the operating system or standalone). A robust password policy will assist but not eliminate this problem. Evidently popular passwords include "password", "12345" and "monkey" – no I don't understand the last one either. There are many systems available which allow single or two factor authentication which protects the enterprise data. The problem, however, is the user. Most users cannot come up with a password of more than 8 characters, let alone remember it. Expecting them to deal with multi-factor authentication may be a step too far. Programs such as BitLocker or PGP Whole Disk Encryption or the free TrueCrypt offer solutions which can provide almost total protection. However, it comes at a cost, eg when the employee cannot remember their password and then blames IT for the fact that the data cannot be recovered. The problem with a TNO (trust no-one) solution is that users cannot be protected from themselves.

Of course, things will go wrong and users will lose mobile devices and leave laptops on buses; where that happens the enterprise needs to be able to respond quickly through a remote wipe of the device (assuming it is not wholly encrypted in a secure fashion). This needs to be possible outside the core hours of 9 to 5, given that many of such losses will happen in the evening and at weekends.

Perhaps the enterprise should keep a record of all the NIC addresses of devices which are permitted to access the network so that these can be blocked remotely so as at least to contain any risk. In appropriate cases, it is possible to set filters so that access cannot be had at particular times; few UK based employees really need access to the network at 2 am on a Sunday, and if they do an exception can be created for them.

If your policy does allow remote wiping of lost or compromised devices, this raises another other issue: what happens when the IT department wipe a lost device which, it transpires wasn't actually lost but just mislaid and which device contained the unbacked-up personal photos of some important event in the employee's life? Employees need to know that that is a consequence of mixed use and ideally should give an express written acknowledgement of that possibility, to avoid future disputes.

Of course, none of this works if the employees are not trained and told what they can and cannot do; my perception is that employees in enterprises are given mobile devices, often with access to the corporate network, with little or no guidance and very little (if any) training. Should a breach of the BYOD guidelines be considered a disciplinary matter? If so, that needs to be spelled out clearly.

ICO guidance and other issues

In March 2013, the ICO issued guidance on compliant BYOD schemes (at http://bit.ly/1nlFa89), which discusses many of these issues from a data protection perspective. For the enterprise, the issues go far wider than data protection and for many, there may be no personal data involved; however, the same issues arise and the guidance is a good starting point.

BYOD is not a static process; the capabilities and price point of the latest consumer electronics – mobile phone or laptop – surpass anything which could have been considered even five years ago; employees are accessing the internet (and that means enterprise resources) from a myriad of unexpected places; our corporate website (www.macroberts.com) is, according to the analytics, even accessed by users using an xBox (which is inexplicable and a little sad.). That means that any BYOD policy needs to be fluid enough to allow its development over time to ensure that it remains relevant and fit for purpose.

Other matters you might like to consider include cost reimbursement. If the individual is using their own device for enterprise purposes, should the enterprise bear any part of that cost – or is that the cost that the employee has to bear personally for the luxury of having a single device? What about data and particularly roaming data costs? If the employee is surcharged for exceeding a data cap, should the enterprise reimburse that? How is the excess cost to be shared? Is the amount up to the cap the employee's cost and the excess for the account of the enterprise? It's probably worth setting out these rules in advance.

For the enterprise, it is perceived that having employees with 24/7 access to enterprise resources may increase responsiveness and client service. In some jurisdictions in Europe, employees are not expected to deal with email outside contracted hours; in the US and UK, the opposite may be true, but either way there are employment law issues which should not be overlooked. If an employee has an enterprise-provided smartphone but misses a deadline on some important matter because they turned it off at 5 pm on a Friday and didn't re-engage before 9 am on the Monday, is that an issue?

Death and departure

Finally, some thought should be given to death and departure; not necessarily death of the employee, although the enterprise should also give some thought to that, but rather the death or replacement of the device. If one of the employee attractions in a BYOD situation is that they get to change the device for the latest model every 2 years (or whatever), the enterprise needs to give some thought to what is to happen to the old device. Does it get put in a drawer until it heads off to the local charity recycling service? If so, has all the data been wiped? It should have been, both for data protection and for confidential information reasons.

If the employee leaves, is anything done in relation to their devices? Hopefully network access will be revoked, but what of the terabytes of enterprise data held locally on the laptop or the information on the personal smartphone? Traditionally, the leaving meeting with HR involved the ceremonial handover of the access pass, keys and Blackberry. Perhaps in the 21st Century, more attention should be given to the information walking out of the door on the employees own smartphone.

Useful resources

Obviously the drafting of a BYOD policy is something that should be tailored to the needs of the business and relevant to the business, its employees and its devices. However, there is some useful guidance to be found from publicly available sources which at least point you in the right direction.

I like the tips from JD Supra at http://bit.ly/T9uIXZ and the (albeit US-centric) BYOD toolkit to be found on the White House website at http://1.usa.gov/1bNYx5t.

A quick Google search for "BYOD policy template" does bring up a large number of examples, but some of these do appear to be more wishful thinking than the reality of what is likely to happen.

David Flint is Senior Partner of MacRoberts LLP (www.macroberts.com), based in Glasgow, Edinburgh and Dundee.

Email df@macroberts.com. Twitter @dfscot.

Electronic evidence

By Stephen Mason

Electronic signatures and electronic evidence are central to our lives; we all use technology.

At present, there is no agreed term relating to the form of evidence that comes from our use of technology: specifically, software. For the sake of shorthand, the words "electronic" and "digital" are used interchangeably.

A change of outlook

Recording content on paper means the medium and the content are bound together. Digital information is completely different. At its basic level, "bits and bytes" comprise the content, ie 0s and 1s. In addition, the medium can be many disparate devices, and software written by human beings is required to read and interpret the data. This means it is necessary for a conceptual change. With its unique characteristics, complex questions about the integrity and security of electronic evidence may be raised, although the authentication of complex forms of electronic evidence will differ to less complex forms of electronic evidence, such as emails or text messages, for instance.

There are some areas of knowledge relating to electronic evidence that are not inherently necessary in a conventional text on evidence. For instance, a more considered approach is necessary regarding how digital evidence is seized, investigated and examined. This is because this initial process can be so flawed as to render the evidence inadmissible or open to challenges, especially regarding its authenticity. In addition, lawyers must not lose sight of where the burden of proof lies and whether the party with the burden has met it. This is because it might be necessary to take a determined stance at trial where it appears the judge has not quite fully grasped that the evidence is not sufficient to discharge the burden.

There is also a significant gap in the need to consider authenticity as between criminal proceedings and civil proceedings. This is because civil proceedings deal with the issue of authenticity under CPR 32.19, where each party is deemed to admit the authenticity of documents disclosed.

Understanding the digital realm

The fundamentals of digital evidence cover the characteristics and sources of digital evidence. Almost all evidence is now created digitally, and what we mean by "digital" is anything that has been created or stored on a computer or a computer-like device; this includes data from satellites, for instance. We are familiar with the fact that the volume of digital evidence continues to increase, and the ability to store large volumes of data means we communicate and exchange data in new ways. These changes have occurred in the last 20 years, and the world is, arguably, now truly global. This affects every aspect of evidence in digital format.

The characteristics of digital evidence can affect the authenticity and analysis of the evidence and includes the following, each of which merits a more detailed discussion: the dependency on machinery and software; the mediation of technology; the speed of change; volume and replication; metadata; storage media; illicitly obtaining confidential data; anti-forensics and the interpretation of evidence; falsifying data; hiding data; attacks against computer forensics and trail obfuscation. The practising lawyer needs to be alert to this list of potential problems where even a smidgeon of digital evidence is present.

The sources of electronic evidence may appear to be obvious, but include a wide range of possibilities, including: physical devices, such as computers, mobile telephones, smartphones, PDAs, tablets and such like; components, including hardware, the processor, storage, software (system software, application software), the clock, time stamps, storage media and memory and data formats; networks, such as the internet; corporate intranets, wireless networking, cellular networks and dial-up; and applications, including email, instant messaging, computer to computer (P2P, meaning peer-to-peer) and social networking.

The importance of the accuracy of the clock was discussed during the trial of Harold Shipman in 1999, and an illustration from the United States serves to highlight this issue. In the case of *Liser v Smith* 254 F.Supp.2d 89 (2003), Jason Liser was arrested for the murder of Vidalina Semino Door on 12 August 2000 after being identified as the man withdrawing money from a Bank of America ATM in a video surveillance photograph taken on the night of the murder. The police knew that the victim's ATM card had been used at that same machine shortly after her death. The police released the photograph to the public because its subject purported to match a description of an eyewitness of one of the suspects who had been seen fleeing from the scene of the crime. Mr Liser was subsequently released when it became apparent that the time indicated by the camera on the ATM was significantly inaccurate. Mr Liser had used the ATM before the murder took place. Two other men were arrested and convicted of the killing.

Authenticity

The question of the authenticity of digital evidence can be a vexed issue. There have been instances of lawyers claiming that because an email is easily forged, it follows that it is necessary to lay the appropriate evidential foundations to introduce the evidence – that is, to prove the authenticity of the document. In *R v Mawji (Rizwan)* [2003] EWCA Crim 3067, the appellant was convicted of making a threat to kill and part of the evidence included an email sent to the victim dated 31 July 2002, which read: "Hi Bitch, Don't think you're safe in the UK. I'm going to kill you. I will make sure I get my hands on you … waiting for you. Your loving husband, Riz."

A witness for the defence gave evidence to demonstrate how relatively easy it was to produce a document that was supposed to be an email, but which had nothing to do with the email account from which it purported to come. It was suggested that somebody else was responsible for sending the email in question. One of the grounds of appeal was that the email was secondary evidence (which is correct) if adduced in the form of a print-out and it was necessary to provide evidence of the audit trail or similar to show the authenticity of the document. The members of the Court of Appeal rejected this submission, indicating that the email did not have to be authenticated in the way suggested by the appellant because of the circumstances surrounding the events and the other evidence in the case. The internal evidence of the content of the email was similar to other evidence produced at trial, which went to show that the email was written and sent by the appellant and the members of the jury had to consider whether, in all the circumstances, it was possible that somebody else might have produced the email. The content of the email demonstrated its authenticity on the face of the totality of the evidence. If the email was fabricated, it had to be questioned why somebody should go to the length of forging the content of an email that was so obviously linked to the other evidence produced at trial.

Any form of evidence can be (and is) forged. A lawyer cannot use the argument that because an item of digital evidence is capable of being forged, it cannot be adduced into evidence without being authenticated fully. The proposition does not follow.

More serious issues may arise regarding the proof stage, encompassing the investigation, seizure and examination of digital evidence – which is demonstrated in the well-publicised 2007 case of *State of Connecticut v Julie Amero*.

The presumption of "reliability"

The common law presumption formulated by the Law Commission in their report *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No. 245, 1997) is as follows: "In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time." In criminal proceedings, s 129(2) of the Criminal Justice Act 2003 created a presumption that a mechanical device has been properly set or calibrated.

The problem with the presumption that a computer is deemed to be "in order", or "properly set or calibrated" is that software and the associated systems have become more complex. This means that it has become progressively more challenging to test software to reflect the way the users will use the product. This does not negate the fact that software written by human beings has always been – and continues to be – subject to errors. Care must be given to agreeing to the operation of this presumption regarding digital evidence, especially in the light of software errors. To this extent, consideration should be given to the five-part test for authentication, especially regarding complex evidence from banking systems.

Hearsay

Digital evidence can be categorised as:

(1) The records of activities that contain content written by one or more people. Examples include email messages, word processing files and instant messages. As evidence, it may be necessary to demonstrate that the content of the document is a reliable record of the human statement that can be trusted.

(2) Records generated by a computer that have not had any input from a human. Examples include data logs, connections made by telephones and ATM transactions. It might be necessary to demonstrate that the computer program that generated the record was functioning consistently at the material time.

(3) Records comprising a mix of human input and calculations generated and stored by software written by a human. Examples include financial spreadsheet that contains human statements (input to the spreadsheet program) and computer processing (mathematical calculations performed by the spreadsheet program). As evidence, it might be necessary to establish whether the person inputting the data or the writer of the software created the content of the record and how much of the content was created by the writer of the software and how much by the person inputting the data.

In general terms, hearsay may not necessarily be a substantial issue, even in criminal proceedings. Where hearsay is important is where reliance is made on the output of a computer to prove the truth that, eg, £500 in cash was removed from an ATM – in the absence of a human being capable of giving evidence that the machine actually did dispense the money.

Stephen Mason (www.stephenmason.eu) is a barrister and author of a number of books on electronic evidence, including *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012). He has conducted training on the subject for judges and lawyers at universities, legal professional organisations and ministries of justice in several countries.

Email stephenmason@stephenmason.eu.

Are blogs any use to law firms?

By Joe Reevy

I have recently spent some time looking at the blogs on law firm websites. I looked at more than 1,000 blog postings on more than 100 websites. They all had one thing in common: zero visible engagement. Not a single one had had a comment added to it.

I think there are a lot of reasons why people wouldn't want to comment in a public forum about legal issues that affect them and few reasons why they would, so lack of visible engagement is no surprise at all. Besides, from the firm's point of view, to start an online conversation with a browser to your site has clear risks and also may lock up valuable fee-earner time. However, the lack of engagement does raise the question: is blogging worthwhile for solicitors?

Indeed, if firms are diverting staff time from earning profits to creating web content, there has to be a good reason for it. Several of the firms I looked at were clearly investing (in opportunity cost terms) many thousands of pounds per partner per year in the production of web content which was neither particularly accessible for the reader (generally, way too much legalese) nor had any evident marketing purpose. Rule 1 of web content marketing, by the way, may be that the purpose of your web content is not to sell, but inform ... but the ultimate object is to increase the probability that the browser will pick up the phone to your firm, not to one of the two or three other firms whose websites they have also viewed.

Creating the legal material for blogging can be expensive. One of our clients reckons that even a short piece of content created in house costs them at least £130 to post: one per day would need to obtain nearly £70,000 in new fees a year to break even.

I'd bet my socks that, for at least 80 per cent of all UK law firms, blogging activity decreases the profits of the firm rather than increasing it and, as more and more firms pile into the blogging/social media marketing bun fight, this will be getting worse. We saw the same thing happen with SEO, where returns have fallen rapidly as more and more firms use SEO.

Additionally, the window of opportunity for content to be seen in any social area is quite small: even on LinkedIn an item will typically disappear off my screen within 7 minutes during the day. The message has to be very well designed to be noticed at all.

So, should you abandon blogging and social sharing? No, not at all: get these right and they can work very well. The fact that most firms aren't doing it profitably does not mean that it can't be done.

Strategies for success

How should you go about upping your game? Here are three easy strategies that can be really effective.

Be a local hero

A local hero is the "go to" firm in the local area. This can be the hardest to do, but is also normally the most effective.

Did you know (Google tells us) that 86 per cent of searches for legal services have a place name attached? If you are big in your locality, you probably don't need a national presence but you do need to develop your local profile.

How to do this? Identify local targets and spread the word to and via them and their networks. Share space/content with other organisations in your area: the chamber of trade, local charities, schools, estate agents, even larger clients. If you give commentary etc to them, you can add value to their proposition and put your brand (and wisdom) in front of qualified prospects who are local. Join their groups, comment on them.

Be an industry hero

An industry hero is the expert in an industry. Larger law firms are doing this well in industries such as haulage, medical and hospitality.

If you read the trade press, you will understand the market and its issues, speak their language and make intelligent comments in their industry forums (trade pages and social networking groups), you'll start to be seen as the industry expert. It isn't fast, but it really works.

There are still really good industries to get at and even where the national reputation has been cornered, you can still become a regional expert.

Be a work-type hero

This is where the type of work you do is highly specialised. In this, you are probably going after the professional market rather than the public one. This not only makes identifying the people who you want to see your thoughts (and their online discussion forums) easier, it also is amenable to success via SEO in a way a broader-based practice is normally not: the demand here is for expertise rather than accessibility.

You also need to cut costs

If you do not have a natural marketing person amongst your lawyers, consider outsourcing your blogging and social media to one of the many legal marketing companies which now offer this type of service. You can still provide the legal content and the ideas you want to share, but finding the right words (or 140 characters, in the case of Twitter) to make a connection with the viewer, can be a real challenge.

If you are going to continue to do it all yourself, do learn all you can – from social media of course. Most of the best people who advise solicitors on social media are active members of the Social Media for Solicitors group in LinkedIn. At the time of writing, it only has 325 members, but really works for some of the contributors because it is so tightly targeted. And you can find out who are the leaders in the field.

In any case, do not waste fee-earner time on the technical side of content/blog creation, recreating your content for each social media outlet separately. You can automate the networking of your content by using applications like Bloggerapp or Hootsuite to automatically distribute your posts to the social networks as well as your blog.

Joe Reevy is the MD of www.legalrss.co.uk and www.words4business.com and he is also the driving force behind the www.myinfonet.co.uk automated marketing platform.

Email joe@bestpracticeonline.com. Twitter @joereevy.

A court reporting restriction database

By Judith Townend

The Law Commission has recently recommended the introduction of an online database of "postponement" orders. What are its chances of success?

The legal framework around contempt of court puts the onus on court reporters to ascertain the terms of relevant reporting restriction orders in given criminal cases. They are expected to be familiar with the automatic restrictions, and to find out details of the discretionary postponement orders in place – orders which prevent publication of material until a set date, or the end of specified proceedings, under s 4(2) of the Contempt of Court Act 1981. However, the latter can present difficulties.

Media representatives responding to the Law Commission's consultation on contempt said that they struggled to obtain information about whether an order has been made and its terms "because there is no formal system for notifying the media of their existence". As a BBC response suggested, the current system for communicating orders is "ad hoc, inconsistent from court to court, and often lacks clarity".

An online list of orders

Inspired by the Scottish Courts' simple online list which records cases with active contempt orders, the Law Commission ran a successful pilot in seven crown courts – including England's busiest, the Central Criminal Court. This data collection exercise produced a list of cases with active postponement orders.

The administrative burden was far from onerous despite the concerns of some of the consultation respondents. In fact, the Law Commission, recommending the introduction of such a list for England and Wales, considered that once it was set up, administration would only take three to four hours per month for the designated person or body. Systems are already in place for internally recording these types of orders so sending them for publication is a straightforward task for individual courts.

The terms of orders

This list would be a useful tool for researchers and journalists but does not resolve the problem of discovering the terms of orders. To this end, the Law Commission also recommended the creation of a closed database: users would pay a small fee to access the details of restrictions.

Clearly if this database was completely open it would undermine the purpose of the orders it was designed to protect. The Law Commission proposal does not, however, consider other key operational questions such as how much; and who would be allowed access: people who present themselves as professional media, or any interested member of the public?

The cost could be the first stumbling point and, indeed, the headline observation in the limited industry coverage of the Commission's report. A similar scheme had fallen by the wayside by 2010, after a commercial contractor reportedly suggested an “eye-watering” cost to media organisations. To avoid this happening again, it would be advisable for the Ministry of Justice digital services team to develop the list and database in-house, cheaply and efficiently.

The question of membership is a curious one, and one that is dealt with inadequately in recent procedural developments around courts access.

The media vs the public

Procedural guidelines for tweeting from court give “a representative of the media or a legal commentator” the right to tweet without making an application, whereas a member of the public must seek special permission. Similarly, the Judicial College’s 2014 guidance on reporting restrictions in the criminal courts suggests that “court staff should respond positively to **media organisations’** requests for assistance in relation to the existence or terms of reporting restriction orders” (my emphasis).

However, Criminal Practice Direction 16.B.6 and 16.B.7 directs that a copy of the order “should be provided to **any person** known to have an interest in reporting the proceedings”. This ambiguity around the treatment of media and ordinary members of the public should be addressed, with view to introducing a consistent approach.

Knowledge

The Law Commission’s report also raises another interesting legal uncertainty which deserves further attention: it is unclear, it suggests, whether a publisher’s knowledge of a reporting restriction is required to establish contempt. What is the “mental element” required for liability?

The preferred approach seems to be that “in addition to knowledge of the order, it is necessary to intend to prejudice the administration of justice” but the position lacks clarity. While this uncertainty is “unfortunate”, the Law Commission suggests that its list would make the system fairer, and also provide a means of establishing recklessness (it would be possible to see whether an order appeared on the list or not at the time of the breach).

If so, it would be essential that the courts kept such a list up to date and accurate.

Further development

Although the Law Commission only recommends a list for s 4(2) orders, it suggests that if such a list is set up, it could be used as a pilot for a “more ambitious system for publicising all reporting restrictions”.

What are the chances of the scheme’s implementation? The report mentions that HMCTS is currently looking at the issue as part of its wider redevelopment of IT systems. However, that bigger project is likely to move slowly: it would be sensible to move the Law Commission’s plan along speedily and use it as a testing ground for a wider reporting restrictions list and database.

Administrative concerns about the reliability of the list and database, as mentioned in the Law Commission’s report, should be overcome as well: if journalists and members of the public are obliged by law to adhere to stringent orders, the judiciary and courts service should also have a responsibility to provide the necessary information.

There is also the possibility that a lack of momentum and interest may thwart or delay the scheme – a pity if so. There was a fairly muted response to the report, which was published in March 2014, with limited mainstream media pick up. That is not due to a lack of interest in contempt: conversely, the proposed role for the Attorney General in directing the removal of news archive material during courts proceedings, as set out in the Criminal Justice and Courts Bill 2013–14, is generating critical coverage.

Similar schemes have been discussed elsewhere: a national public register has been proposed in Australia, although Australia’s Right To Know coalition would prefer a “publicly accessible register containing information that does not breach the order with additional information that is only accessible by authorised media representatives” – not dissimilar from the Law Commission’s two-tier model. The concern is that a bare bones public register would have very little practical purpose, and that it is the details of the full order that are crucial.

Process scrutiny

Some information is justifiably restricted in the courts process but as the former Master of the Rolls, Lord Neuberger, has argued, open justice must “yield no more than strictly necessary to secure the achievement of the proper administration of justice … Where it goes beyond what is strictly necessary then we run the risk that the courts are no longer open to proper scrutiny, that their role in supporting democracy and the rule of law is undermined”.

The restriction of information must also be subject to this “proper scrutiny”; legal researchers and journalists must be able to monitor whether restrictions are “strictly necessary” and in accordance with legal procedural guidelines and statutory provisions. Without the development of efficient systems to record restrictions, it is difficult to see how they can perform this role.

Conclusion

The Law Commission’s scheme would perform a dual purpose in upholding the principle of open justice: first, it would enable journalists and other types of court reporters proper and fair access to the provisions to which they are expected to abide; and second, it would allow researchers, journalists and other relevant parties to monitor the process and product of restriction.

Contempt of Court (2): Court Reporting (Law Com No 344) is published at http://bit.ly/P4VDlT.

Judith Townend is a lecturer in journalism at City University London and research associate at University of Westminster. She was invited to discuss the Law Commission’s proposals ahead of the publication of its report and would welcome comments and suggestions to inform her future research in this area.

Email judith.townend.1@city.ac.uk. Twitter @jtownend.

Legal news and resources in the USA

By Delia Venables

USA legal news sources

Since many of the legal issues of today were already active, yesterday, in the USA, it is often worth keeping up to date with USA legal news sources. Here are some of the key ones.

Law.com (www.law.com) is an extensive source of legal news (and nice pictures). This site, part of the ALM Group (American Lawyer Media) has now “gathered up” a number of previously independent legal web sites and businesses. The site covers national and regional news by practice area. Other sites in the group cover legal jobs, legal training, directories of attorneys and various legal data bases.

FindLaw’s Legal News (http://legalnews.findlaw.com) provides a wide range of current legal news stories, grouped by major heading, eg US Supreme Court, Business, Civil Rights, Crime, and so on. FindLaw started in 1996 when two attorneys compiled a list of Internet resources for a group of law librarians in northern California. FindLaw is now owned by Thomson Reuters.

JURIST (www.jurist.org) is a web-based legal news and real-time legal research service powered by a mostly-volunteer team of over 60 part-time law student reporters, editors and web developers at the University of Pittsburgh. They track important legal news stories and materials and aim to cover stories based on their substantive importance rather than on their mass-market or commercial appeal.

LLRX (www.llrx.com) (Law Library Resource Xchange) is a free, independent, Web journal providing information on a wide range of Internet research and technology-related issues, applications, resources and tools. LLRX is in its 18th year of continuous publication, with a diverse, professional, highly engaged and expert global readership.

Apple, Google Make Peace in Patent War

NewsLinx (www.newslinx.com) provides “Information Technology headlines from around the web” (not specifically legal ones). This site provides everything you could want (and more).

bizjournals (www.bizjournals.com) provides business news “from around the country” linked with many local news sources.

Institutions and resources

The United States House of Representatives (www.house.gov) provides a major source of information on many topics, including:

- The schedule of bills, resolutions, and other legislative issues before the House
- The Library of Congress with Information about the US Congress legislative process, bills, the Congressional Record, committee information, and historical documents
- Information on committee meetings.
- Contacts - Constituents may identify and/or contact their elected Member
- Access to the basic documents of US law. Full text searchable copies of the US Code (a consolidation and codification by subject matter of the general and permanent laws of the US).

Many of the House proceedings can now be watched online.

The United States Senate (www.senate.gov) provides web pages for all senators and email addresses and also information on the various functions and committees of the Senate. There is information about the legislative process and about the current state of Bills.

PI BRIEF UPDATE
& PI Brief Update Law Journal
Kevan and Ellis on Credit Hire, 4th Edition: Chapter Three - Mitigation of Loss

The White House (www.whitehouse.gov) provides information speeches and plans for legislation relating to the president. There is also a history of past presidents and of the White House itself and of the American system of Government.

US Department of Justice (www.justice.gov) sets out its aims as “To enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.” There are links to government departments and agencies relating to legal matters as well as press release and reports relating to issues of current interest.

The Library of Congress (www.loc.gov) is the nation’s oldest federal cultural institution and serves as the research arm of Congress. The Law Library is the world’s largest law library, with a collection of over three million volumes spanning the ages and covering virtually every jurisdiction in the world. The Library’s mission is to support the Congress in fulfilling its constitutional duties and to further the progress of knowledge and creativity for the benefit of the American people. The site is designed both for lawyers and for members of the public. As well as serious legal material, it has several unique public-oriented features including “American Memory” Exhibits, a searching engine called **Thomas** (after Jefferson) and current and changing events and exhibits. In the section for **finding legal resources in a global contex**t (www.loc.gov/law/find/global.php) there are various resources including:

- **Global Legal Information Network** (GLIN) (www.glin.gov) a database of laws, regulations, judicial decisions and related legal sources from around the globe. Documents are submitted in their original language with English summaries available. However, the GLIN network is “undergoing a transition” and is not available at the moment.
- **The Guide to Law Online** (www.loc.gov/law/help/guide.php) provides a vast network of links to content-based Web sites of primary and secondary legal and legislative information services from 193 nations and all US federal, state and territorial government entities.
- **The Multinational Reference** (www.loc.gov/law/help/guide/multiref.php) lists items which reprint the laws and regulations of international jurisdictions on a particular legal topic, comparative in nature.

FirstGov (www.usa.gov) is the US Government’s “portal” to all the other government and “official” sites in the USA, both Federal and local. It is aimed at the citizen and tries to make sense of the many sources of information available, grouping them by topic. It also provides links to the sites covering “public safety and law” including Courts and Legislatures, Federal and state laws, courts, legislatures, Crime, Prisons and lots more.

Google Scholar (http://scholar.google.co.uk) “provides a simple way to broadly search for scholarly literature. From one place, you can search across many disciplines and sources: articles, theses, books, abstracts and court opinions, from academic publishers, professional societies, online repositories, universities and other web sites. Google Scholar helps you find relevant work across the world of scholarly research.” (Choose “Case Law”). A search here opens up access to full text legal opinions from US federal and state district, appellate and supreme courts and (via a “Cited By” feature) links to other cases and articles on Google Scholar that cite them. Though court opinions in the US are not protected by copyright, they were hitherto only readily available for comprehensive searching via subscription services such as Lexis and Westlaw. You can also use Google Scholar / Legal Opinions to follow up citations of judgments that are not themselves indexed in full text, including those from other jurisdictions.

Internet Library of Law and Court Decisions (www.internetlibrary.com) authored by Martin H. Samson, features extensive summaries of over 600 court decisions shaping the law of the web; providing facts, analysis and pertinent quotes from cases of interest to those who do business on the Internet and in New Media.

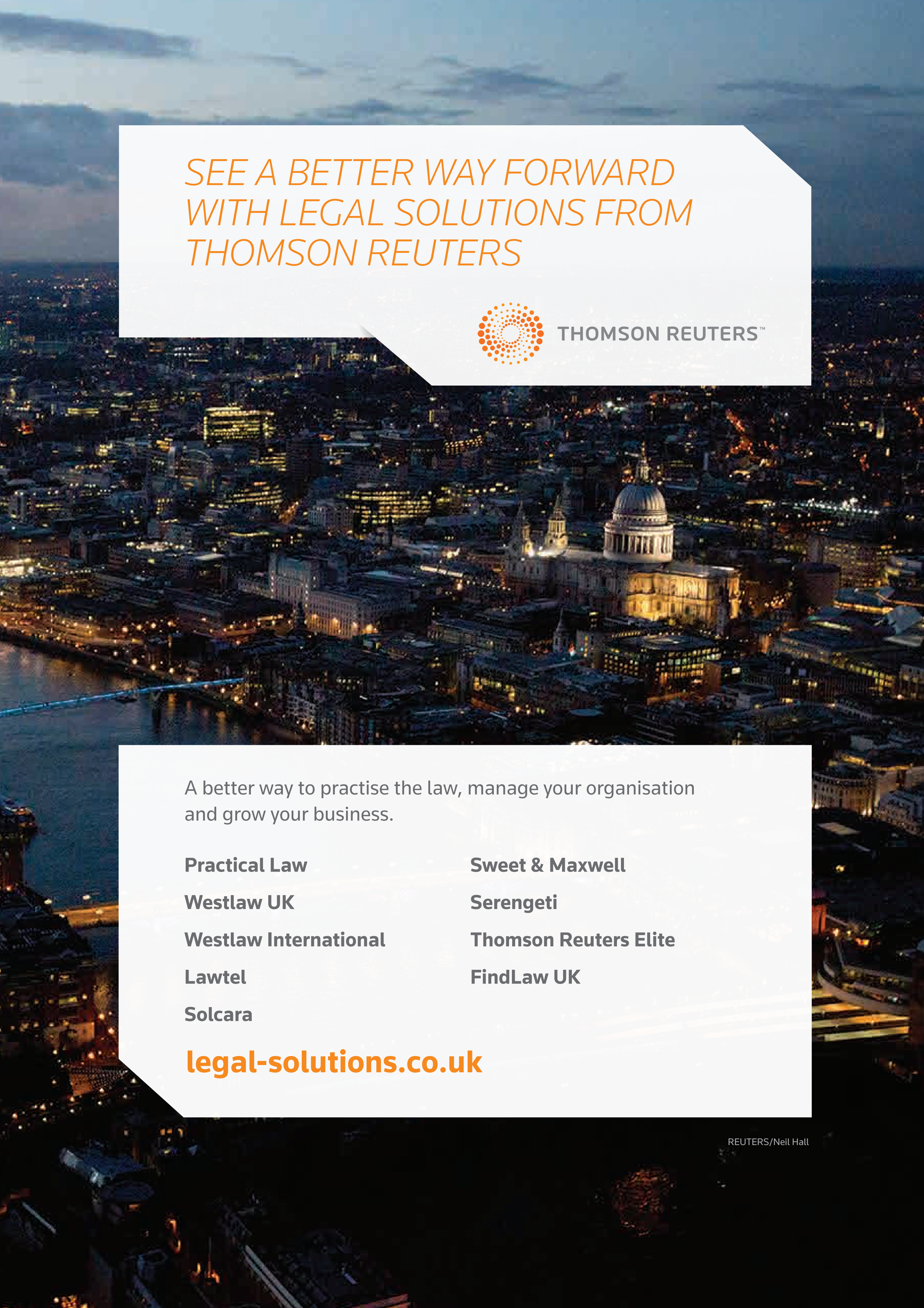
American Law Sources Online (www.lawsource.com/also/) is a useful new source of law for the USA, Canada and Mexico. There are sections offering federal, state or province law sources, as well as commentaries and practice aids.

The Legal Information Institute (www.law.cornell.edu) at Cornell University Law School aims to ensure that the law remains free and open to everyone, which includes supporting global expansion of the free access to law movement, serving government, empowering citizens, serving the legal profession, and developing web science for the law. They offer the Institute’s collection of recent and historic Supreme Court decisions, its hypertext versions of the full US Code, US Constitution, Federal Rules of Evidence and Civil Procedure, recent opinions of the New York Court of Appeals and other federal, state, and international material.

The Internet Legal Resource Guide (www.ilrg.com), based at the University of Texas, is a categorized index of more than 4000 select web sites in 238 nations, islands, and territories, as well as thousands of locally stored web pages, legal forms, and downloadable files. The site includes lists of **Law Related Newsgroups** (www.ilrg.com/ng.html) and **Law Firms and Lawyers** (www.ilrg.com/lawyers.html). Both of these are USA based of course.

There are further USA resources described on my site at www.venables.co.uk/USA.htm.

Delia Venables is joint editor of this Newsletter. Email delia@venables.co.uk. Twitter @deliavenables.



REUTERS/Neil Hall

CPD Courses for Lawyers for 2014

from Nick Holmes and Delia Venables

Make the most of the Legal Web and earn CPD at the same time

Social Media and eBusiness for Solicitors

1. Introduction to the main types of social media used in a business context
2. All about Google+, LinkedIn and Twitter - and how to make the most of them
3. Make your website a marketing tool, and getting local clients with local SEO
4. Social media monitoring – what are they saying about you online? And battling with Google
5. eCommerce projects (and successes) for law firms – selling documents and developing software

Guide to Legal Web Resources

1. Legal commentaries online, provided free by chambers and publishers
2. Justice resources from Government; and electronic evidence – where we are now
3. European primary law resources on Eur-Lex and European institutions and legal resources
4. Legal news and resources in the USA, worldwide resources, and languages for lawyers
5. A review of the most useful internet skills for lawyers and particularly the benefits of RSS

Guide to Legal Web Issues

1. Media law issues: the future of privacy and restrictions on court reporting
2. Where we are (and the future) of digital copyright, and how fair use relates to this
3. Website legal issues, including copyright of website images and SEO law and good practice
4. Digital currencies (all about Bitcoin) and the problems of BYOD (bring your own device)
5. Access to law, including Big Data for Law and the future of law reporting

Full details and online purchase at www.infolaw.co.uk/cpd

Accreditation

All three courses are accredited for **5 hours CPD each** from the SRA.

Guide to Legal Web Resources and Guide to Legal Web Issues have been accredited by the Bar Standards Board for 5 hours CPD each.

All online

You buy these courses online, you access the material online and you complete a set of questions online. It is all straightforward and (if necessary) Nick and Delia will assist.

Cost and access

Each course costs £80 plus VAT and qualifies (after taking the online test) for 5 CPD hours.

There is a special combo price for any two courses purchased together of £120 plus VAT.

A multi–use licence for one course for up to 5 people costs £200 plus VAT; for 2 courses £300 plus VAT. Larger group pricing available.

Straightforward process

To complete a course each person has to answer a set of questions online. There are ten questions, two for each of the five chapters. You email your answers to Delia who will reply to you by email, usually within two working days, to confirm whether you have passed the test.

Quick steps to 5 points per course

1. Purchase the course online
2. Read the materials online or offline (pdf)
3. Answer 10 straightforward questions
4. Receive confirmation from Delia by email

Purchase the courses for immediate access at www.infolaw.co.uk/cpd.

Special bonus

Anyone taking one or more of these courses in 2014 will receive the pdf version of the Internet Newsletter for Lawyers free for 2015. That will help you on your way to next year's CPD courses!