7 Web law

We turn now to aspects of IT law which relate specifically to the internet, and mainly to the World Wide Web. We shall look at four topics:

- contract formation in internet trading
- the right to make links
- ownership of domain names
- Web 2.0 and defamation

7.1 The internet and contract

7.1.1 Trading needs contracts

Trading at a distance is surely the leading function of the Web for most businesses. (Its function as an information source is also important, though far less productive of legal issues.) Suddenly, many delays and difficulties associated with finding a suitable supplier and agreeing terms, using traditional communication channels, have been electronically annihilated.

For buying and selling, the central area of law is contract law. We have already seen that, in the eyes of the law, even the most trivial consumer purchase involves creating and fulfilling a contract. For trading to function smoothly over the Web, it is essential that the technology should not get in the way of the legal process of contract-formation – otherwise there would be business chaos, with individuals and organizations not knowing what their commitments were or who actually owned particular goods. When one buys a tin of beans in a corner shop, these issues are self-explanatory; with larger-scale transactions – particularly so-called "B2B" (business-to-business) trading, the total value of which is much larger than that of business-to-consumer retailing – they are not. The respective parties' commitments will often be far more complicated than "you give me this thing and I give you £X". The parties need to be clear about just how far their legal commitments extend; if one side is disappointed, the other side needs to know whether it was legally obliged to do better. The stage at which ownership of goods is legally transferred may be crucial, for instance to determine when the purchaser needs to take responsibility for insurance coverage. Readers will perhaps understand that internet trading cannot flourish unless contract law is able to apply successfully.

That said, for English contract law the internet creates fewer difficulties than one might imagine. In some countries there have been problems about "electronic signatures": the laws of those countries required signatures, in the sense of handwritten names on paper, to validate contracts of more than some fairly low threshold value, and clearly much of the advantage of internet trading would be lost if agreements formed electronically became legal only after paper documents had been exchanged through the post. Not only is the rapidity of internet communication a benefit to commerce, but in some cases (where the things traded are sufficiently standardized) we want the possibility of automated trading, with no human intervention on the supplier side – or even, perhaps, no human intervention on either side.

The EU issued an *Electronic Signatures Directive* in 1999 which aimed to guarantee the availability of a legally valid electronic alternative to handwritten signatures. But for English contract law that Directive was largely redundant; English law requires signatures only in a few special cases, and in any case English law has not been particular about what counts as a "signature". In a 1954 case a rubber stamp of a firm's name was accepted as a signature; in a 2004 case (not concerned with computing technology) a typewritten name on a telex was accepted as a signature. For English law, a "signature" is simply an objective indication of the signer's approval of the contents of a document. Consequently signatures have not been a stumbling block for internet trading. The Law Commission commented in 2000 that

> We do not believe that there is any doubt that clicking on a website button to confirm an order demonstrates the intent to enter into that contract…we suggest that the click can reasonably be regarded as the technological equivalent of a manuscript "X" signature [as made by illiterates]… clicking is therefore capable of satisfying a statutory signature requirement (in those rare cases in which such a requirement is imposed in the contract formation context).

There are issues about how one knows that a mouse-click, or some other electronic alternative to a handwritten signature, was made by the relevant person, and that what he understood he was doing was approving the contract terms – but these are essentially practical problems rather than legal problems, and they are problems which IT should be able to solve without excessive difficulty. What English law cares about is simply that the person has approved the terms.

So there is not much danger that people using the internet as a trading channel will fail to create a legal contract when they believe they have done so.[46] However, there is more risk the other way round: people might find themselves prematurely committed to a contract, when they think they are still in the negotiation phase without a binding commitment. Understanding how this can happen will also show us how contract law copes with automatic trading.

7.1.2 Offers v. invitations to treat

Under the Common Law, a contract comes into being when one party makes a definite offer to the other party (which must involve a swap – one cannot "contract" to make a free gift without return), and the second party signifies acceptance of the offer to the first. Once the offer is accepted, both parties are committed. In B2B trading, there may be many rounds of revised offers as the parties negotiate precise terms acceptable to both sides, but the contract is concluded when one side accepts the same terms that are currently offered by the other side.

In a shop (where haggling is not usual), the shopper is construed as "making an offer" by taking goods to the counter or the checkout and tendering money, and the shopkeeper or assistant "accepts the offer" by actions such as ringing the sale up on the till or passing the items over a barcode reader. This is different in some Continental countries, where the shop is construed as "making an offer" by displaying goods with marked prices, and the shopper "accepts" the offer by taking goods to the counter or checkout. But in English law, what the shop does in displaying priced goods is merely to issue what the law calls an *invitation to treat* – that is, it invites shoppers to enter into negotiations with a view to agreeing a contract of sale.

In the context of traditional shopping this distinction between making an offer and inviting to treat may appear an absurd piece of legal pedantry. But in the context of internet trading it is a point on which merchants can come badly unstuck.

The risk is that a commercial website may advertise goods or services, thinking that it is "inviting site visitors to treat", in such a way that legally it is actually "offering" contractual terms. Usually that would not matter, because the company behind the website wants to sell things on the advertised terms. But in some cases the company could get into difficulties – for instance if stock of the item in question is limited and more orders come in than can be fulfilled, or if by mistake a wrong (too low) price is advertised. If the selling webpage is an "invitation to treat", the vendor is allowed to say "sorry, we are out of stock" or "sorry, the price should have been shown as £X". But if it is an "offer", then customer orders are legally-binding acceptances, and the vendor must either fulfil the orders (perhaps by finding a new source for the goods at a higher price which leaves the vendor with a loss), or else be prepared to face legal actions for breach of contract.

This kind of débâcle can happen independently of the internet, of course. The most notorious example in British retailing history occurred in the early 1990s, when the vacuum cleaner and washing-machine manufacturer Hoover ran a sales promotion which offered free flights overseas with purchases over £100. Hoover budgeted £2 million as the cost of the promotion, completely failing to anticipate how popular the offer would be. Many people bought two vacuum cleaners just to get access to the flights; some retailers put their prices up to help buyers to qualify. When Hoover was unable to buy enough flights to fulfil the offer terms, it received 30,000 complaints and faced numerous lawsuits. It ended up paying out at least £50 million; the UK Hoover subsidiary responsible was split from its American parent and sold off at much less than its previous value. Senior managers lost their jobs.

In the early 1990s, Hoover's error did not involve the Web. But with e-commerce it is so easy to put up a selling page over-hastily, and there are so many possibilities of unexpected technical glitches, that comparable errors become more probable than with traditional trading.

An American example occurred in 2001, when a programming error on the United Airlines site caused ticket prices to be "zeroed out", so that people booking flights were charged only the minor additional costs (e.g. sales tax). After it discovered the error, United first responded by charging the full prices to customers' credit cards retrospectively, but after a storm of negative publicity it reversed its decision and let customers use the tickets at the bargain rate. United claimed that this was an act of grace, and that it would have been within its legal rights to insist on full payment (and it is true that companies in a situation like this often do give customers the benefit of the doubt, for a sound business reason: when selling to the public, the goodwill forfeited by sticking to the letter of the law may outweigh the monetary loss from a one-off mistake). However, legal commentators did not agree that a court would have allowed United to change the terms of the flight sales retrospectively – particularly since plenty of discounting and promotional offers were occurring in e-tailing, so United customers could plausibly have believed that the ultra-low fares were "for real". Since England shares the fundamentals of its contract law with the USA, a company making a similar mistake here would also probably be legally committed to honour the giveaway price.

Thus unwary contractual offers can be expensive or even survival-threatening for firms that make them. But, provided one is aware of the problem, there is no difficulty about avoiding it. In 2005 the Argos website mistakenly advertised a television plus DVD bundle for 49p (instead of £350). Not surprisingly, it quickly received thousands of orders. Argos refused to honour them and gave the would-be customers their 49p's back, but in this case it was unquestionably entitled to do so. The terms and conditions on the Argos site included a provision:

> While we try and ensure that all prices on our Web site are accurate, errors may occur. If we discover an error in the price of goods you have ordered we will inform you as soon as possible and give you the option of reconfirming your order at the correct price or cancelling it…

Anyone ordering from the Argos site must tick a box to confirm that they have read these terms and conditions. This is enough to ensure that offers on the site are "invitations to treat", not "offers of contract".

So it is straightforward to eliminate this kind of risk from e-commerce. This really is a case where commissioning a lawyer to check that wording is watertight is a small price to pay for a large gain in terms of peace of mind. Nevertheless, major players often fail to cover themselves. Struan Robertson, a technology lawyer who commented on the 2005 Argos case, added that he knew another large site which was trying to cancel orders for Sony Vaio laptops priced below £2, where the published conditions were so poorly worded that customers probably had the law on their side.[47]

7.1.3 Automated trading

Turning to transactions executed automatically: the relationship of these to contract law was considered long before the days of e-commerce. A classic discussion is found in Lord Denning's judgement in *Thornton* v. *Shoe Lane Parking* (1971), where a car-park was controlled by an automatic barrier rather than a human attendant:

> The customer pays his money and gets a ticket. He cannot refuse it. He may protest to the machine, even swear at it; but it will remain unmoved. He is committed beyond recall. He was committed at the very moment that he put his money in the machine. The contract was concluded at that time. It can be translated into offer and acceptance in this way. The offer is made when the proprietor of the machine holds it out as being ready to receive the money. The acceptance takes place when the customer puts his money into the slot.

(This might be read as implying that a selling webpage is making "offers" rather than "inviting to treat"; but Rowland and Macdonald (p. 274) point out that in 1971 Lord Denning would not have envisaged cases where the machine processes customers' orders in complex ways – they see no reason to doubt that a suitably-worded selling webpage expresses invitations to treat rather than offers.) The reason to quote Lord Denning is to show that, even though contracts are between people and/or organizations, not between machines, the fact of an offer being physically made by a machine does not stop English law regarding it as emanating legally from whoever is responsible for the working of the machine.

In the car-park case, the "attendant" was a robot but the motorist was human. But one can presumably extrapolate from *Thornton* v. *Shoe Lane* and see a contract which is physically arranged by machines on both sides as having been legally executed by the persons or organizations who control the respective machines. Having set the machines up, they will be bound by the contracts thus formed – even though they only find out about these contracts after they are already bound by them.

7.1.4 Time of contract conclusion

There are other ways in which e-commerce creates special issues for contract law. For instance, in B2B contracts it may matter exactly when the contract comes into being. In some kinds of business, trading conditions change frequently and abruptly; before a contract exists, its terms can be renegotiated if they cease to suit one side, but once the contract is in being then whichever side is disadvantaged by a change in conditions is out of luck.

In English law, the general rule is that a contract comes into being when the acceptance reaches the offerer, but there is a special rule about contracts that are concluded via the postal service, which come into being as soon as the acceptance goes into the post. With e-commerce, where the path taken by a communication is both complex and often mysterious to both parties, the law is not yet entirely clear about when a contract comes into being. The issue is complicated by the fact that an EU *Electronic Commerce Directive* was implemented in the UK in 2002 and is based in part on aspects of Continental contract laws that conflict with English Common Law. So this area is at present somewhat messy; but, having drawn attention to it, I do not believe it is significant enough for the readership of this book to examine in detail.

7.1.5 The right to link

Hypertext and the World Wide Web were invented by academics, for whom it is axiomatic that publicity for one's writings is desirable. There was no thought in the minds of the Web pioneers that anyone might wish to restrain others from creating hyperlinks into his site; the more incoming links, the better. Hence the HTML language is designed in such a way that creating a hyperlink from site A into site B requires action only by the site A webmaster.

Once the Web became commercially important, freedom to link ceased to be axiomatic. Businesses want traffic to their websites, but they want the right sort of traffic. There has been considerable legal wrangling over the issue of whether website owners have an untrammelled right to link into others' sites.[48]

One issue about the right to link is not very relevant for this textbook, so I shall mention it briefly in order to set it aside: that is the question whether people can be held responsible for illegal content in sites they link to, or at least forbidden to link to such sites. For instance, a Dutch site Indymedia.nl had links to mirror sites for an extremist German magazine, *Radikal*, carrying articles about how to sabotage railways. Deutsche Bahn (the German state railway company) took Indymedia to court in the Netherlands in 2002 and Indymedia was required to remove the links. It is not clear whether a British court would have made the same order, but for most businesses one hopes that the question is academic.

More interesting for us are situations where websites aim to control incoming links because they want:

- to reside in respectable cyber-neighbourhoods
- to prevent visitors bypassing material the site owner wants them to see
- to avoid negative publicity
- to prevent their material being misappropriated

7.1.6 Cyber-neighbourhoods

An upmarket bricks-and-mortar boutique naturally wants to locate itself in a respectable area; it would prefer not to be next door to a betting shop or tattoo parlour. In cyberspace, "neighbourhoods" are defined by links between sites, so businesses would like to avoid links from sites they find unsavoury.

Some organizations have tried to impose blanket bans on unauthorized incoming links. The US National Public Radio network (a non-profit organization producing cultural programming) stated on its site that "Linking to…any material on this site without the prior written consent of NPR is prohibited", and those wanting to link were asked to fill out a lengthy form. When challenged, NPR explained that it aimed to preserve its integrity as a non-commercial organ of journalism by avoiding the appearance of association with commercial organizations. After protests from those who felt that freedom to link was essential to the Web, in 2002 NPR ceased insisting on prior authorization, but continued to claim the right to ban specific links. However, it is not clear to American legal commentators whether it could actually force anyone to remove a link to its site. (While NPR may in practice have given up trying to ban inward links, others continue to do so; in 2008 Associated Press was reported as threatening legal action against bloggers who linked to headlines on its site.)

In other instances, rather than trying to impose any general policy on incoming links, an organization has objected to a particular link. In 2001 the Ford Motor Company objected to the hacker magazine *2600* creating a link to the Ford site from a site called fuckgeneralmotors.com. Ford and GM are two different companies, so the domain name did not directly insult Ford, but Ford did not want to be associated with vulgarity. Ford sued under trademark law, claiming that the link infringed and tarnished its trademark. Dan Burk, an American professor of internet law, explained that "Tarnishment happens when you juxtapose my trademark with something that is offensive or unsavory. It causes consumers to view my mark with distaste", and in this case "the vulgar word will be associated in the minds of consumers with the Ford site or arriving at the Ford site."[49] Burk saw Ford's legal case as strong. But the court dismissed the case, on the ground that infringing a trademark was a tort only if done in connexion with the infringer's own commercial activity, which was not true in this instance.

7.1.7 Deep links

Websites are standardly designed with the idea that visitors will begin at their home page. But it is equally easy for another site to link to an internal page; such an incoming link is called a *deep link*.

A frequent reason why website owners object to deep links is that their site contributes to their business by carrying advertising, and the adverts will typically be on or near the home page. Consider the California case of *Ticketmaster Corp*. v. Tickets.com (2003) – since the USA is a Common Law country, it is likely that the precedents this case set would be taken seriously by a British court.

Ticketmaster was an established business that sold tickets to various events (sports, entertainment, etc.) conventionally and online; it took a commission on tickets sold, and its website also generated advertising income based on numbers of visitors to its home page. Tickets.com was a newcomer, which aggregated information on its site about where tickets could be bought. It used a spider to extract information about events handled by Ticketmaster from the Ticketmaster site to display on its own site; rather than selling tickets for those events directly, it sent purchasers via a hyperlink to the relevant place in the Ticketmaster site (making it clear that this was a separate site). Tickets.com derived its income from advertising alone.

By bypassing the Ticketmaster home page, Tickets.com clearly threatened Ticketmaster's profits, so Ticketmaster tried to invoke the law against Tickets.com. It objected on three legal grounds: breach of copyright, "trespass to chattels", and breach of contract.

The copyright issue related to the way that Tickets.com derived event information from the Ticketmaster site; but in a preliminary hearing the California court dismissed this issue, mainly on the ground that copyright law does not protect purely factual data but only its arrangement into a "literary work" – Tickets.com had been throwing away the Ticketmaster formatting, and arranging the facts of date, prices, etc. into its own format. "Trespass to chattels" is a rather obscure Common Law concept: *chattels* are pieces of movable property (say, a vase, a car, but not land), and trespass to chattels means interfering with someone's movable property in a harmful way. Since the Tickets.com spider did not affect the use or operation of the Ticketmaster computer, this claim also failed.[50] The court did accept that there was an arguable case of breach of contract: a notice on Ticketmaster's home page stated that anyone penetrating beyond it to internal pages was thereby accepting conditions which would have forbidden Tickets.com's usage. (Compare the way that shrinkwrapped software often has a notice saying that opening the packaging implies accepting various small-print licence terms; but there has been much controversy about the legal validity of such notices.) It would have been for Ticketmaster to pursue the breach of contract issue in a further hearing (but it appears not to have done so).

There are other reasons for a site to resist unauthorized incoming links. John Corker was head of an Australian online legal practice, OzNetLaw, which wanted to ensure that all visitors were aware of its terms and conditions:

> The idea was aimed at managing liability from people suing us for providing advice. If people were deep linking, then someone might bypass the terms and conditions, so we thought a [linking] policy could offer some protection.[51]

But this was more a matter of enabling OzNetLaw to tell a court that it had done everything it could to ensure that visitors had read the conditions, than actively using the law to eliminate unwanted links – Corker saw the chance of that as "negligible".

7.1.8 Negative publicity

A straightforward example of a link which promotes negative publicity might be wording such as "click **here** to visit a crooked firm", with the link leading to company X's site. But that would not really be an issue about linking; the law would probably treat it as no different from saying "Company X is crooked" in so many words on one's own site. However, there are subtler examples.

Diebold Election Systems (since renamed Premier Election Solutions) was an Ohio-based company making voting machines. It put its archive of internal company memos on the internet, presumably to make it easier for staff members to consult; some students found material in which Diebold people had raised worries about product quality, and created links to these memos from their own sites. Diebold threatened to take the students, and their ISPs, to court for breach of copyright.

But this rebounded. The Online Policy Group, a Web-freedom pressure group, sued Diebold (which it saw as trying to suppress public discussion of the integrity of the democratic voting process) for issuing baseless threats; in 2004 Diebold lost, and had to pay damages and costs of $125,000.

7.1.9 Inlining and framing

In the Diebold case the real issue for the firm was not copyright but negative publicity. In many other cases, though, organizations object because outsiders are using hyperlinks to hitch "free rides" on work which the objector is using as an asset in its own business.

If A simply downloads a copy of material on B's website and places the copy on its (A's) own site, that is no different from copying and publishing a book for which another publisher holds the rights, and can be dealt with straightforwardly under copyright law. But, typically, that is not what happens. Rather, A uses hyperlinks to B's site, so that a visitor to A's site sees elements of B's site looking as though they are part of A's site. For instance, A's page may include an HTML "img" tag telling the visitor's browser to download graphic material from B's site (lawyers are calling this *inlining*), or A's page may show an entire page from B's site framed with a border featuring A's logo and/or advertising (*framing*). A does not "copy" anything; the only copying of B's material is from B's site to the visitor's machine – and B put his site up in order to enable copying in that direction to occur. So how can B complain that A has breached his copyright?

Many organizations in B's position have tried to force A to remove such links; alternatively, some have tried to charge for the links. But the attempts have not been very successful, except where B has folded up at the threats stage without fighting the issue out in court.

The earliest case to attract international attention arose in the Shetland Isles: *Shetland Times* v. *Willis* (1997). Unfortunately for the law, this case was technically rather "blurry". The *Shetland Times* was a long-established local paper, and Willis started an online competitor, the *Shetland News*, which displayed headlines copied from the *Times* that, when clicked, took the visitor to the relevant stories on the *Times* site. The judge accepted that there was a *prima facie* breach of copyright (whereupon the case was settled out of court rather than fought through to the end), but this ruling was based largely on the fact that the headlines, at least, were actually copied onto Willis's site. Likewise, in a larger-scale, recent case, *Copiepresse* v. *Google* (2006–07), a Belgian court found that Google News was breaching the copyrights of newspapers whose articles it linked to, by displaying headlines and short extracts on its own site.

Perhaps more clearcut was the case *Haymarket Magazines* v. *Burmah Castrol* (2001). Haymarket's portfolio of magazines included two on motoring and motor racing, *What Car?* and *Autosport*. The oil company Burmah Castrol had a "Complete Motoring" website which framed pages from Haymarket's site so that they appeared to be on "Castrol – What Car?" or "Castrol – Autosport" pages, and which for good measure corrupted the banner adverts that Haymarket ran on its site. Haymarket sued not just under copyright law but also under the special database law discussed in chapter 6, under the law of trademark infringement, and under the law of "passing off" (trading under the pretence of being someone else). This case also was settled out of court and thus created no legal precedent; still, Burmah Castrol agreed to desist from what it was doing, so it must have been advised that Haymarket had at least a good chance of winning (but under which law?)

There has been one Continental case, *Vriend* v. *Batavus* (2003), where the Dutch judge ruled that "framing" counted as breach of copyright, because it "creates the impression that the framed information belongs to the linking website". But a published comment on that was:

> This decision is confusing in its argument: copyright law considers objective, not subjective elements of a violation, hence, there is no place for "impressions".[52]

("Confusing" here is probably a polite lawyer's way of saying that the judge got it wrong.)

In another Continental case, *StepStone* v. *OFiR* (2001), the plaintiff won under the special database law rather than copyright law. StepStone was a German-based international company running an online recruitment service. OFiR, also German, systematically hyperlinked to StepStone's individual job-vacancy notices, bypassing StepStone's adverts, and it used figures on StepStone's vacancies in order to publish claims about the numbers of jobs OFiR had access to. The judge ruled that OFiR's deep links infringed StepStone's exclusive rights in its database. This led Anthony Misquitta, of the distinguished London law firm Farrers, to predict that under the database law most websites would count as "databases" and that making someone else's website contents available via hyperlinks would count as "unauthorized re-utilizing", banned under that law.[53]

(Misquitta added:

> The law of intellectual property has had a terrible time of applying its principles to the internet, largely because it has not had its fundamental philosophies questioned as much since the invention of the printing press. The law of copyright is terrified of the internet and runs screaming from the court every time it is asked to address it.

Colourful language, from a lawyer!)

Something that seems strangely absent from most discussions of this area by lawyers (though computing people have often pointed it out) is that it is not hard to prevent outsiders creating deep links into one's site by technical means, if one really wants to do so. In the Diebold case, one might think it almost insane to place an archive of confidential messages on the public internet; someone ought to have mentioned the word "intranet" to Diebold's managers. But even when one wants one's webpages to be available to the public, it is not difficult to prevent them being accessed other than by the intended routes. Only the home page needs to remain in a fixed, known place, and there is usually no objection to links to one's home page. OK, defeating deep linking technically would take a little more effort than putting up a collection of pages and leaving them alone – but not nearly as much effort, expense, and uncertainty of outcome as taking linkers to court.

However, subsequently to *StepStone* this point was taken on board by the court hearing another German case, *Verlagsgruppe Handeslblatt* v. *Paperboy* (2003), where again the defendant's site was deep-linking directly to the plaintiff's newspaper articles, bypassing the newspaper home page. Contrary to Anthony Misquitta's prediction, the German Federal Court refused to treat this as unauthorized re-utilization of a database; it explicitly described deep links as important for the success of the internet, and ruled that it was down to sites which did not want them to block them by technical means.

Overall, then, the idea of controlling incoming hyperlinks by law has achieved little traction to date.

7.2 Ownership of domain names

The Western world has long-established trademark laws enabling firms to create strong brand images linked unambiguously to their identity. When URLs came along, the problem arose that bare sequences of characters offer much less scope for differentiation than traditional graphic trademarks. As one anonymous writer puts it:

> In the physical world, Cannon Towels, Cannon Fishmarket…and Robert Cannon can all co-exist peacefully. The trademarks at issue are distinct and not subject to confusion. But in the online world, only one gets the valuable cannon.com [domain name][54]

In the early years of the Web, trademark owners sought to insist that they were legally entitled to a given domain name – but in very many cases like "cannon", claims like that were mutually incompatible.[55]

One way in which this raises novel legal issues relates to the concept of the bottom-up Law Merchant, discussed in chapter 2. The domain name system is governed by the non-profit but private-sector ICANN (Internet Corporation for Assigned Names and Numbers), which delegates control over various high-level domains to different national or multinational organizations (*registries*) – for instance, the .uk domain is controlled by a non-profit organization called Nominet. Nominet and its sister registries have set up formal processes for arbitrating disputes over ownership of lower-level domains. ICANN monitors the activities of the registries, requires their dispute resolution services to harmonize with an agreed set of general principles, and occasionally it decides to take a top-level domain away from one registry and entrust it to another.

But where does the authority delegated by ICANN come from in the first place? The internet grew, historically, out of a US military and academic network, Arpanet, and domain names were initially allocated by an institute within the University of Southern California and then, from 1993, by various public- and (mostly) private-sector organizations under a contract with the US National Science Foundation. So decisions about domain names were at that time ultimately underpinned by the power of the American state.

As the internet grew into a commercially and socially crucial facility for the world as a whole, it was no longer acceptable for a single nation to control it. ICANN was established in 1998, largely in line with a memorandum published in the name of the "Internet Community"; the US government formally transferred responsibility for domain name allocation to ICANN. As a result, where authority over domain names ultimately stems from today is a rather nebulous issue. Lloyd (p. 464) comments about the UK Nominet organization that:

> As with much of the Internet, the legal basis for its actions is unclear, it being stated that Nominet UK derives its authority from the Internet industry in the UK and is recognised as the UK registry by [IANA, the immediate predecessor to ICANN] in the USA.

Quasi-legal rules which rest on the authority of an international "community" or "industry" sound very reminiscent of the mediaeval Law Merchant.

When ICANN was established, domain name allocation was a deeply sensitive and controversial area. The other thing to say about it, though, is that the heat has now been somewhat drained out of it by the rise of search technology. While the normal way to access a site was to type its URL manually, it was crucial to have a snappy, memorable domain name. Television commercials and print adverts do still display URLs that have to be remembered and typed in, but by now it is commoner for a visitor to be led to a website via Google or another search engine. Someone who surfs that way clicks on a link rather than typing in the URL – he may not even notice what the URL is. So this is not an area of computing law which I would expect to develop to any great extent in future.[56]

7.3 Web 2.0 and defamation

7.3.1 Slander and libel

English law distinguishes two kinds of defamation: *slander* (in speech) and *libel* (in writing); because writing is permanent, libel is treated as being more seriously damaging than slander. E-mails and the like are often composed as casually and carelessly as spoken remarks, but they can be preserved indefinitely and so the applicable law is libel law.

English libel law is strict: compared to other countries, it is easy for someone who feels damaged by the written word to win a case against whoever is responsible, and awards for loss of reputation have traditionally been large (though recent changes have moderated that to some extent).

As business first used the Web, libel law was scarcely relevant. Commercial websites were concerned with promoting their own businesses, not normally with knocking their competitors. But the Web is coming to be used in new ways. We have heard a great deal recently about "Web 2.0". This is a vague, hype-laden piece of terminology, but one thing it commonly refers to is the idea that websites – including commercial websites – are ceasing to be outlets for one-way communication exclusively, and turning into two-way, conversational affairs, where for instance a company will draw its customers and other interested parties into participation via blogs, chatrooms, and similar mechanisms.

There are several business reasons why the "virtual communities" fostered by interactive websites are potentially beneficial for a company. However, if members of the public are encouraged to post material on a company website, the legal danger is that some individuals' postings might include defamatory remarks about third parties. We know that electronic communication tends to encourage a kind of "flaming" that is rare in other media. For the firm owning the website, it would be regrettable enough to find one of its customers having to defend a lawsuit as a consequence of contributing to a blog which that firm had set up. Even worse would be the possibility of itself defending a defamation suit, if it is held responsible for others' contributions to its site. A plaintiff who hopes for a large damages award will be more interested in going after the firm than the individual; the firm is more likely to be able to pay.

So the question arises what legal responsibility a website owner has for material posted by others.

7.3.2 Distributors and publishers

Questions like this arose before Web 2.0 days, in connexion with ISPs and operators of bulletin boards. One way that lawyers think about the issue is to compare that kind of electronic communication infrastructure with the world of newspapers and magazines, and to ask whether the organizations are more like distributors (such as newsagents) or publishers. If a newspaper contains a libellous article, the newsagents who sell the paper to readers would not normally be held liable – they have no control over what appears in the paper and may not even be aware of it; but the newspaper publisher has editorial control over what its journalists write, so will routinely be treated as equally responsible with them for any libel.

In the case of electronic bulletin boards, some are moderated and others not. Ironically, although providing moderation would normally be seen as the responsible thing for a bulletin board operator to do, legally it might be a rather dangerous thing to do: it implies taking on a role more like publisher than distributor.

In the USA (although libel law is far milder there) this situation was seen as creating such risks for organizations which undertake the socially-valuable task of promoting electronic communication that the risks were eliminated by statute (section 230 of the *Telecommunications Act 1996*). This broadly says that service providers are not to be held responsible for content posted by others, and that no liability arises from the moderating role.

Without a blanket exemption such as American law provides, a website run by a commercial firm would be more likely to be held responsible for its contents than some bulletin board run by amateur enthusiasts – the site contributes to business profits, so there would be little excuse for not taking the trouble to moderate it. English law contains nothing parallel to §230 of the US Telecommunications Act. Our *Defamation Act 1996* provides that no-one is liable for the contents of electronic communications if they act purely as unwitting distributors, but if they act as "publishers" they are liable; a commercial website owner, like a newspaper publisher, would have a duty to take reasonable care about what it publishes.

7.3.3 Godfrey v. Demon

Even an ISP, with no commercial interest of its own in the contents of material it hosts, will probably not escape liability under the 1996 Act if it has been told about defamatory material on its servers (so that it can no longer claim to be an unwitting distributor). Consider Godfrey v. Demon Internet Ltd (1999).

Dr Godfrey was a British computer science lecturer who allegedly made a hobby of starting online flame wars and then bringing libel actions when people responded to his flames by being nasty about him. In 1997 he faxed the MD of the leading British ISP Demon demanding the removal of a scurrilous newsgroup posting which had come in from the USA. Demon routinely deleted newsgroup postings after a fortnight, so the issue concerned only the ten days between Godfrey's fax and the normal deletion date; during that period, Demon failed to act (apparently the fax never reached the MD's desk). In view of this delay, the court found in preliminary hearings in 1999 that Demon could not satisfy the requirement about taking reasonable care – at which point Demon threw in the towel and settled out of court, paying Godfrey about a quarter of a million pounds.

Although Godfrey v. Demon set no formal legal precedent (because it was settled rather than fought out to a conclusion), the terms on which it was settled sent a thrill of fear through the industry. It seems that (unless an ISP is prepared to investigate and satisfy itself that a complaint is legally unfounded, which would often be difficult or impossible for it to achieve), its only safe response to any complaint will be automatically to take down the material complained about. This is what British ISPs have been tending to do.

Indeed, they sometimes censor material before it is received. Outcast was a small-circulation magazine for homosexuals; its February 2000 issue contained material alleging financial irregularities at the company Mardi Gras 2000 Ltd, part-owned by a group of "gay press barons". No actual libel action arose from that, but after receiving a complaint Outcast's ISP, NetBenefit, required Outcast to satisfy it that arrangements were in place to avoid possible future libel. When Outcast were unable to comply within a two-hour deadline from receipt of their letter, NetBenefit took their entire website down. Commentators objected to this "censorship" of the Web; but NetBenefit explained that it would otherwise be exposed to unacceptable legal risks. It invited Outcast to "campaign on the real issue: the need for a change in the law to allow [ISPs] to provide the service Outcast and others are seeking."[57] Legal commentators see NetBenefit's attitude as entirely understandable given English law as it stands.

7.3.4 The *Mumsnet* case

If a neutral ISP, which simply offers Web hosting services to all comers, can be this vulnerable, an organization inviting website postings by its clients will surely be even more so. The classic example is *Gina Ford* v. *Mumsnet*, settled out of court in 2007.

Gina Ford is a well-known but controversial author of books about childrearing, who advocates methods much stricter than those which used to be in vogue. Mumsnet is a parenting website run as a part-time activity by seven mothers, which includes chatrooms. Gina Ford's lawyers sought to have the entire Mumsnet site taken down, because the chatrooms contained defamatory remarks about her, ranging from what sound like defensible opinions (Gina Ford must be cruel and uncaring, because her *Contented Little Baby Book* recommends leaving a five-month-old to cry for three hours at a time) to ridiculous flames (Gina Ford straps babies to rockets and fires them into south Lebanon). Mumsnet took down individual postings whenever Gina Ford complained about them, but it admitted that it could not comprehensively monitor 15,000 postings a day. In the attempt to placate Gina Ford, Mumsnet banned its users from mentioning her, though it had been neither a pro- or an anti-Gina Ford site – "the pro voices met the antis" – and it saw banning mention of her as "a bit like barring discussion of Manchester United from a football phone-in".[58] It matters how babies are treated; many Mumsnet mothers were outraged at not being allowed to discuss this freely.

Under the settlement, Mumsnet formally apologized to Gina Ford and paid a five-figure sum in damages (though the website continues in being). Again, because it was settled the case does not constitute a legal precedent, but it shows that website owners do not feel legally secure with respect to material posted on their sites by others.

7.3.5 Weak protection

The year after *Godfrey* v. *Demon*, the EU *Directive on Electronic Commerce* (2000) seemed set to offer ISPs a measure of protection. It required national laws, among many other things, to hold distributors of electronic communications immune from liability provided they are mere distributors. However, this was not to apply if they "select or modify the information contained in the transmission" (i.e. moderate the postings). The Directive was implemented in Britain by the *Electronic Commerce (EC Directive) Regulations 2002*. A Law Commission report looked at these Regulations, and concluded that they did not clearly offer an ISP any greater protection in practice than it had under the 1996 Defamation Act.

ISPs took some comfort from a 2006 decision, in *Bunt* v. *Tilley & ors*. John Bunt regarded himself as defamed by material in Usenet postings by David Tilley and two other individuals; he sued not only these individuals but also the ISPs (AOL, Tiscali, and BT) which they used to transmit the material. The issue decided in 2006 was whether the ISPs shared any responsibility for the postings. The court found in the first place that an ISP which passively provides an avenue of access to the internet is not a "publisher" in Common Law, and also that the ISPs were exempted under the European Regulations from responsibility for the contents of material they transmit to and from the internet.

However, this protection was limited. It depended on the ISPs acting only as transmitters rather than hosts, so it would not have helped Demon Internet to defend itself against Godfrey; the *Mumsnet* settlement came after the *Bunt* precedent was already established.

Evidently, companies need to be wary of setting out to reap the commercial advantages envisaged by enthusiasts for "Web 2.0".