SCRIPT-ed

Volume 1, Issue 3, September 2004

Editorial

The Changing Shape of Cyberlaw

September is traditionally the time when teachers of cyberlaw across the globe reconsider the shape of their discipline and how it has changed since the previous academic year. Cyberlaw is a young discipline – the first UK case properly so considered was probably Scotland's own *Shetland Times v Wills*[1] in 1996, while in the US, perhaps the earliest case to attract wide attention was the Internet libel case of *Cubby v CompuServe*[2] in 1991 - and one whose minutiae change dramatically from day to day if not hour to hour. In the struggle to keep up with the deluge of cyberlaw case law, statutes, regulations, commentaries, opinions from the technical, economic and political presses, international treaty activity, European Directives, rounds of government consultations, conference proceedings and industry Codes of Practice, it is often difficult for those who observe the domain to stop and look at the general trends which make cyberlaw in 2004 a very different animal from when this writer began teaching her first cyberlaw course in 1997.

But things are, indeed, very different. In 1997, cyberlaw disputes were mainly either private law disputes between individual users and other users or commercial operations, or public (mainly criminal law) disputes between individuals and states. Many of the latter cases quintessentially involved states attempting to exert sovereignty over foreign nationals and corporations whose Internet activities were impinging on the hallowed enclave of their national laws: in this vein, the defining criminal cyberlaw case of the 2000s has probably been the *Yahoo! case*[3], where

---

[1] 1997 SC 316.
[2] 776 F.Supp 135 (SDNY 1991).
[3] TGI Paris, Ordonnance de refere du 20 Nov 2000. This order confirmed the earlier decision issued on May 22 2000.

French interest groups successfully prosecuted Yahoo! US under French law for distributing Nazi memorabilia to French citizens, but then found that the US courts refused to enforce the French decree on US soil as against US fundamental tenets of free speech.[4]

The range of players on the cyberlaw stage has now however expanded. On-line intermediaries, for example, have always been crucial as gatekeepers to the Internet and as such frequently both the instigators and the targets of multiple law suits. But intermediaries now include not just the traditional Internet Service Providers (ISPs) of this world – the Demons, AOLs, CompuServes, Freeserves, et al – but a vast pack of new types of intermediaries whose influence on our life on-line is profound. No one reading this editorial for example, is unlikely to get through a day seeking information on the Net without resorting, thankfully, to Google. Search engines are the *sine qua non* of the information society. Aggregators, which combine information flows from multiple sources on a single page – eg, giving access to news headlines from the Guardian, the Scotsman and the New York Times in one place – may well become the primary conduit to knowledge as the number of on line sources to check out for current awareness becomes unmanageable. Price comparison meta-sites – which tell consumers where they can buy the cheapest travel tickets (say) by scanning 40 sites offering that service – are a key product to enable consumer choice and buying power on the Net. "Weblog"[5] sites – which enable thousands, sometimes millions, of people to deliver their thoughts on everything from politics to sex to recipes to the world – are becoming the new leading mass medium of communication which need not be filtered (for better or worse) through the power of an editor or publishing or broadcasting institution. The different roles these intermediaries play, and the different policy reasons for supporting them in law, may lead to a need to fundamentally reconsider existing laws on on-line intermediary liability.

And, of course, perhaps the most significant emergence in the intermediary field of the last five years has been the arrival of the peer to peer (P2P) sites which allow file swapping and sharing between individuals – the Napsters, KaZaas, EMules, Groksters and Morpheus's of the world. Although best known for (allegedly) facilitating the illegal downloading of music and films, P2P architectures have the potential for far more significant abuse – the anonymous and encrypted sharing of child pornography pictures, for example – or constructive use – the sharing of information between scholars, or across states to help the knowledge base of developing countries. As I write, Kazaa/Grokster has just been found not liable for contributing to the illegal copying of music files merely by providing tools which can be so used.[6] This decision poses yet again the fundamental question of whether new types of technology - and the new types of intermediaries which utilise it – should be encouraged by law in the interests of innovation, or restrained by law to preserve existing business models and social norms. The question is a difficult one, more political and social than legal or moral, and one which will undoubtedly not be solved any time soon.

The other new dimension for players on the cyberlaw stage is the international one. International bodies have, of course, always had a pivotal role in the development of

---

[4] *Yahoo! v La Ligue Contre Le Racisme et L'Antisemitisme* 169 F. Supp. 2d 1181 (N.D.Cal 2001). But see also now http://www.law.com/jsp/article.jsp?id=1090180400752 .

[5] See eg, Blogger, Moveable Type, LiveJournal.

[6] *MGM v Grokster*, appeal to US Court of Appeal for 9th Circuit on August 19 2004. See http://www.eff.org/IP/P2P/MGM_v_Grokster/20040819_mgm_v_grokster_decision.pdf.

cyberlaw, given its global nature: intellectual property law has been driven by the World Intellectual Property Organisation (WIPO) while UNCITRAL and the OECD have played major roles in the harmonisation of parts of e-commerce and e-tax law. Outside of law, the crucial technical standards-setting organisations that shape the Internet – the Internet Society, the W3C, the IETF – have always had at least a theoretical internationality about them even if in practice they were mainly organised by, with and for Americans. But in the last few years we have seen the emergence of a truly global, not merely North American, non-governmental organisation (NGO) sector in the field of information society policy, concerned both generally with human rights on line, and with "digital divide" issues in particular. Here the turning point has been the World Summit on the Information Society in 2003 in Geneva[7] (the next stage being in Tunisia in 2005) which not only proved a focal point for digital rights activism groups but actually succeeded in producing a core declaration of principles[8] and a tentative action plan[9] for the future. What we are seeing here for the digital world is something akin to the emergence of the UN family of institutions in the post WWII period: and potentially something of as much importance for the lives of the ordinary citizen of the developing, if not the developed, nations.

It is not just the nature of the actors in cyberlaw that has changed. The pecking order in importance of the subjects that make up cyberlaw has too. Once upon a time, IT law was pretty much regarded as all about intellectual property (IP), really. No one would be foolish enough to say that IP has ceased to be a crucial part of the cyberlaw syllabus in these our days of open source, P2P litigation, Creative Commons[10], DRM systems[11] and the DMCA[12] - but since 9/11 (sadly perhaps) it is rivalled for concern by topics to do with privacy, security, surveillance and cyber-crime. E-commerce is another area which has gone from boom to bust to, perhaps, something approaching the normal expectations of a new industry sector[13], and the degree of legal attention paid to it has fluctuated accordingly, although with an inevitable degree - especially in Europe - of regulation-lag. (The crazy hype and inflated profit expectations of the dot.com years are now fluently transferring themselves to the nanotechnology sector. But that is another story for another editorial.) Whether the amount of law that still pours out of the European Union to regulate e-commerce can now be justified (and if it is helpful to an industry already drowning in red tape and struggling to get past the digital inertia of the average European consumer) is a question no one seems yet to have asked – perhaps because in Europe we never did live through the glory days of dot.com boom quite so fully, and thus the fall, like Icarus, back to earth has not been so shattering.[14]

There are also new topics in the cyberlaw canon: once infrastructure issues could be covered by a quick scamper through ISP liability; now cyberlawyers have to know

---

[7] http://www.itu.int/wsis/.
[8] http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc.
[9] http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!MSW-E.doc.
[10] http://creativecommons.org/. This editorial is not in fact, as you might perhaps expect, licensed under a Creative Commons license but under SCRIPT-ed's own open access license – see http://www.law.ed.ac.uk/ahrb/script-ed/sol.htm.
[11] Digital Rights Management.
[12] Digital Millennium Copyright Act.
[13] See *The Economist* "Paradise Lost" May 8 2003 at http://www.economist.com/surveys/displaystory.cfm?story_id=1747329.
[14] See further Edwards L ed *The New Legal Framework for E-Commerce in Europe*, forthcoming, Hart Publishing, February 2005.

about broadband policy, universal service requirements, telecoms regulation, European competition law and state aid, wireless technology and the basics of WTO law. By contrast, some topics that once looked destined to become hardy perennials of the curriculum are now looking increasingly cobwebbed and redundant. Digital signatures, at least as a consumer and small business tool, have still never really taken hold, despite being the first item on the legislative agenda of every developing country that decides to make a show of getting to grips with regulating the Internet. And digital cash, beloved of banks and merchants seeking to avoid chargeback losses after credit card fraud, and ignored by consumers who see no reason to pay by debit in a world of seemingly endless credit, has essentially died a quiet and unmourned death (just around the time the EC finally implemented its E-Money Directive[15].) Of course the wheel turns and we are now seeing a new and far more successful generation of on-line payment mechanisms in the form of PayPal, SimPay and their ilk – only they don't seem to fit into the E-Money Directive after all. The lesson seems to be not to draft your Directive till your technology has hatched.

So, new players, new intermediaries, new topics, new priorities in the world of cyberlaw. But have the forms of regulation themselves changed? Not at first blush. We still live, as noted above, in a world where every day it seems there is a new case, a new Act, a new Directive, a new Convention which in some way attempts to regulate some aspect of the information society. The European Commission is itself so overwhelmed by this deluge of legislative activity that it amended its own Transparency Directive[16] so that EU member states come under an obligation to notify the Commission whenever they promulgate new acts affecting the information society. But look a little deeper and much has changed. As is now famously known, in 1999 Lawrence Lessig crystallised the elegant, not entirely original, but zeitgeist-capturing insight that in a world of technology, "code" – as in, primarily, software code – regulates the world as much as "code" in the old fashioned sense of legal code.[17] Since that time, we have seen examples again and again of law being "trumped" by code: most strikingly in the field of copyright law, but also elsewhere. In the IP domain, where traditional law, it at one point seemed, could do little to stop the Internet becoming "the death of copyright", "code", in the shape of encryption and DRM systems proved able to effectively prevent illegal copying by anyone but a skilled hacker. (Of course then code bit right back at the rights-holders, since whatever copyright work is once unlocked from the chains of DRM can now be swiftly shared round the world on P2P networks. Code is an unmanageable beast.) In the privacy domain, the law in the form of the EC Data Protection Directive aspires to give citizens rights to control collection and transfer of their personal information without their consent. But citizens and consumers find these rights almost impossible to enforce, even if they know they have them. By contrast, one CCTV camera – hardware "code" – can breach those rights in a moment, undetectably, and almost unstoppably. In the ubiquitous surveillance society we now unknowingly inhabit in the UK[18], code says we have little or no rights to privacy, whatever mere law may claim.

---

[15] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institution.
[16] Directive 98/34/EC as amended by Directive 89/48/EC/.
[17] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).
[18] See further Goold B J *CCTV and Policing* (Clarendon Studies in Criminology, OUP< 2004).

The implications of "code as law" for the development of cyberlaw are interesting. Take the problem of spam, or unsolicited emails. For the last five years we have seen attempts legally to control the spread of spam.[19] Spam now constitutes around 80% of all email traffic across the planet and is clogging up the bandwidth of the Internet as catastrophically as cholesterol blocks the arteries of human beings. So in the last few years from the US has brought forward the Federal Can the Spam Act[20] and from the EU, we see the Privacy and Electronic Communications Directive 2002.[21] Yet the overwhelming likelihood is that the eventual answer to spam will lie not in law but in code, by altering the nature of the Internet from an anonymous decentralised system to one which supports identification, central control and hence a "trusted email" system: something effectively acknowledged both by the IETF who control the fundamental architecture of the Internet, and the International Telecommunications Union at their recent joint WSIS meeting on spam in Geneva.[22] This writer, who (for her sins) is currently writing a chapter on the legal regulation of spam, strongly suspects that in perhaps five to ten years' time this will be a solved technical problem and no longer a legal concern at all. If this applies to other areas of cyberlaw as it does to spam, then we might expect to see cyberlaw begin to contract rather than exponentially expand as it has done so far. Yet if we so imagine we may also be falling foul of a sort of technology-supremacism which fails to fully appreciate the social as well as the technical dimension to many cyberlaw problems. What is essential is for legislators and judges to make sure that the future products of their labours are not "trumped" by code but work hand in hand with it.

And of course, "code" as law has engendered a new breed of law, law which in its turn attempts to tame code. So far, the most famous example of this breed is the US Digital Millennium Copyright Act, and its attempts to make it a crime to write or distribute code which hacks technological copy-protection mechanisms imposed by rights-holders. But there have been other examples of law which (tries to) regulate code: Lessig himself refers back in his early essay on "The Law of the Horse" to the US government's vain efforts in the 1990s to limit access to "strong" encryption via means such as imposing the "Clipper Chip" on encryption users.[23] In general, law which tries to trump code seems somewhat less successful than code which effortlessly trumps law. But it is all good news for lawyers and legislators, who need never fear an absence of work while this digital version of *la ronde* continues.

Lilian Edwards
Co-Director, AHRB Centre for IP and Technology Law, Edinburgh

---

[19] See this writer's early summary (for Europe/UK) of legal regulation of spam as of the year 2000: Edwards L "Canning The Spam" in Edwards L and Waelde C eds *Law and the Internet: A Framework for Electronic Commerce* (Hart, 2000).
[20] Which came into force on 1 January 2004.
[21] 2002/58/EC.
[22] See ITU WSIS Thematic Meeting on Countering Spam, Geneva, 7-9 July 2004.
[23] See Lessig L "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harvard Law Review 501 at 532ff; available at http://www.lessig.org/content/articles/works/finalhls.pdf. Lessig rather cutely describes this episode as an attempt by "East Coast Code" (Washington legislators) to compete with "West Coast Code" (encryption software writers in Silicon Valley).

DOI: 10.2966/scrip.010304.363

© Lilian Edwards 2004. This work is licensed through SCRIPT-ed Open Licence (SOL).