scripted

Volume 10, Issue 3, October2013

LOOKING BACK AT THE LAW OF THE HORSE: WHY CYBERLAW AND THE RULE OF LAW ARE IMPORTANT

Andrew Murray[*]

Abstract

A keynote speech delivered at the 2013 conference of the British & Irish Law, Education & Technology Association, on 11 April 2013, at the University of Liverpool.

DOI: 10.2966/scrip. 100313.310

[*] Professor, London School of Economics.

1. Opening

This is not the speech I planned to give - please accept my apologies. I had a great and rousing speech planned and I would write it between the 1st of February when I delivered the second edition of Information Technology Law to OUP and today. The problem was that the text delivery was delayed, isn't it always, and I eventually delivered it on the 3rd of March. This left not enough time to do everything I planned so instead today's speech is more of an outline or plan of where I see Cyberlaw research going rather than the original concept of delivering tangible results in this direction. For this I apologise and beg your indulgence.

The role of an opening keynote speaker is an important one. They set the tone for the conference by in essence "getting their view in first". It is an honour therefore to be given this role and it shows trust on the part of the conference organiser. I must therefore begin by thanking the conference organisers for trusting me with this role. In thirty minutes or so Joseph will know whether his decision has been vindicated, but the reward for me is greater as I will have completed my contribution to the conference programme and will be able to enjoy the remainder of the conference without wondering whether my paper will go down well. So if you enjoy the next thirty minutes or so, come up afterwards and let me know. If you didn't send me a note after the conference so that for two days at least I can imagine everyone liked what they heard.

I am following in a line of illustrious keynote speakers - in 2010 there was Josef Azizi, a Judge of the Court of the European Union, in 2011 Paul Maharg formerly BILETA executive chair and Iain Mitchell QC, UK representative on the IT Committee of the Bars and Law Societies of Europe. In 2012, the amazing double header of Professor Richard Susskind and Professor Chris Reed.

In truth to follow this line up seems impossible and I would have refused Joseph's invitation were it not for two things: (1) he asked so very nicely and (2) my memory of my very first BILETA conference in York in 1999, when one of the keynote speakers was Geoff Hoon, future Defence Secretary, Transport Secretary, Leader of the House of Commons and Labour Party Chief Whip. At the time, he was Minister of State in the Lord Chancellor's Office responsible for eCommerce. He gave an opening address which almost sent the audience to sleep at 10am on day one of the conference. So when Joseph asked, I thought even if it is the worst speech BILETA has ever heard there is a future in politics for me.

Anyway returning to my central theme – my own insecurities. I realised that while I may be better than Geoff Hoon, few in the room would remember that fateful day in York in 1999. Many would remember that last year in Newcastle, Chris Reed not only gave a talk he also entertained by playing the Ukulele. How does one follow a keynote speaker who not only plays a musical instrument but also makes them and flies gliders in his spare time?

I realised that today the renaissance law professor must do more than just teach and research. I also realised I had little skill in the usual fields. I have no artistic ability, am unmusical to the point where cats hide from my singing (really they do) and my dancing is so embarrassing that I simply don't dance ever. Realising I wouldn't get

very far on Britain's Got X-Talent Factor Voice, I turned to my wife of ten years to ask her what talents I had!.

She thought and said – you can tell stories. My first thought was – after ten years of marriage is that really the best thing she can say about me talent-wise? My second was great if Jackanory Idol ever gets made (I have it all planned out in my head the Judges would be Bernard Cribbins, Prunella Scales and the Ghost of Kenneth Williams) I'll be in with a shot of winning. Then I slept on it and thought about it some more and I realised she had paid me a compliment. Academia is all about communication and in particular the telling of complex tales though simple tropes. The better the story teller, the more equipped one is for academia. Thus today I'm going to do what I do best, I'm going to tell you a story, a story of how Cyberlaw started off on the wrong foot and has (arguably) been on the wrong foot ever since and how this conference could be a place to start thinking about our future as Cyberlawyers before we go the same way as railroad lawyers.

2. The Chicago conference

The problem with my thesis is that the best storyteller sets the agenda and unfortunately there is some anecdotal evidence of this. The law evolves constantly but usually within defined substantive boundaries: criminal law, public law, torts, property and intellectual property, commercial law etc.

Occasionally an academic discipline will emerge which follows the vocational model, the most obvious being media law, telecommunications law and financial services law, but usually such vocational-driven academic models die out in a similar manner to railroad law, aviation law and space law.

The emergence of information technology and the Internet led to the slow evolution of Cyberlaw. Probably the first book on Computer Law (in the UK at least) was Colin Tapper's 1978 edition, it paved the way for others to follow like Chris Reed (1990); Ian Lloyd (1993) and David Bainbridge (1990). In each case though the common theme was a book which collected what one may call "computer world problems" which required the application of traditional legal norms – computer contracts, computer evidence, data protection, copyright etc. The argument could easily be made that there was no such thing as computer law (or Cyberlaw as it would become) as it was not a substantive legal subject, nor, unlike media law, telecommunications law or financial services law was it vocational.

It looked (and looks) like those subjects which no longer exist (or exist only in niches) railroad law, aviation law and space law: an area of legal study determined by technology rather than norms or industry.

This point was made forcefully by Professor Frank Easterbrook at the 1996 University of Chicago conference "Law of Cyberspace". Using powerful rhetoric he established himself clearly as the best storyteller in the room. Telling a vivid tale entitled "Cyberspace and The Law of the Horse" Easterbrook pretty much damned the nascent study of Cyberlaw with colourful flourishes:

> When asked to talk about "Property in Cyberspace," my immediate reaction was, "Isn't this just the law of the horse?" I don't know much about cyberspace; what I do know will be outdated in five years (if not five months!); and my predictions about the direction of change are worthless, making any effort to tailor the law to the subject futile. And if I did know

> something about computer networks, all I could do in discussing "Property in Cyberspace" would be to isolate the subject from the rest of the law of intellectual property, making the assessment weaker.

To make the point clear to anyone who missed the subtlety - Professor Easterbrook set out his argument in full (please excuse the rather long quote):

> When he was dean of this law school, Gerhard Casper was proud that the University of Chicago did not offer a course in The Law of the Horse. He did not mean by this that Illinois specializes in grain rather than livestock. His point, rather, was that "Law and . . .courses should be limited to subjects that could illuminate the entire law. Instead of offering courses suited to dilettantes". The University of Chicago offered courses in Law and Economics, and Law and Literature, taught by people who could be appointed to the world's top economics and literature departments—even win the Nobel Prize in economics, as Ronald Coase has done. I regret to report that no one at this Symposium is going to win a Nobel Prize any time soon for advances in computer science. We are at risk of multidisciplinary dilettantism, or, as one of my mentors called it, the cross sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds. Well, let me be modest. I am at risk of dilettantism, and I suspect that I am not alone. Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers.

Dean Casper's remark had a second meaning--that the best way to learn the law applicable to specialised endeavours is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on The Law of the Horse is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students - better, even, for those who plan to go into the horse trade - to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavours could one really understand the law about horses.

We can sit here and say this no longer applies – it is over sixteen years since Professor Easterbrook set out his manifesto. We can say that although we may not yet have a Nobel Prize for advances in computer science, we do have the Queen Elizabeth Prize for Engineering which was recently won by Tim Berners-Lee, Robert Kahn, Vint Cerf, Louis Pouzin and Marc Andreessen. To do so though would miss the point of Easterbrook's speech. The power was the rhetoric not the detail of the message. It was his storytelling, not his story that was important.

3. The shadow

Professor Easterbrook continues to cast a long shadow over us and our work. We continue to be, consciously or unconsciously affected by what he said that day. It has split us (that is mainstream Cyberlawyers as opposed to ICT legal educationalists) into two genera and within each genera into several species.

The key is in the genera. One genus is the regulatory cyberlawyer (it is to this genus that I myself belong); the other is the (for want of a better word) applied cyberlawyer. There are no doubt many of you in the room. You research in defined areas of intersection between law and cyberspace – cyber-defamation, cyber-privacy, cyber-indecency or perhaps eCommerce. Both genera operate within the long Easterbrookian shadow.

It is perhaps most obvious in the regulatory cyberlaw (or cyber governance) field. The spiritual leader of those of us in this field is of course Professor Lawrence Lessig who answered Professor Easterbrook's challenge in his "New Chicago School" model, found (among other places) in his Harvard Law Review paper The Law of the Horse: What Cyberlaw Might Teach. Lessig here introduces us to his now famous modalities of regulation thesis which posits that because cyberspace is distinct from realspace in the way it is designed, and in particular the malleability of the "code" – the design of the environment we learn as lawyers by studying cyberspace problems and therefore cyberspace law. Of course this massively simplifies Lessig's position but strictures of time requires that I do so here. As I have written elsewhere, it is my belief that Lessig failed to rebut the key indictments in Easterbrook's challenge to the Cyberlaw community, instead he simply pled "special circumstances". By demonstrating that the Cyber-regulatory community can give something back to the general legal debate Lessig bought some time for Cyberlawyers but I fear that time is almost up.

Others have attempted to rebut Easterbrook. I myself put forward my own answer to him in The Regulation of Cyberspace but I have come to believe that the outcome of the collected labours of Cyber-regulatory or Cybergovernance theorists including myself, Jon Bing, Lee Bygrave, Roger Brownsword, Tim Wu, Jack Goldsmith, Ian Brown, Chris Marsden, Han Somsen, Paul DeHert and too many others to name merely give strength to the Easterbrook argument.

Again and again we return to the same well. We discuss the unique characteristics of digitisation and cyberspace and argue our case for cyber-regulation or governance theory, we employ academic heavyweights – Michael Foucault, Bruno Latour, Niklas Luhmann – and a number of legal academic cruiserweights – Gunther Teubner, Cass Sunstein, Neil MacCormick – to make our point that cyberspace and cyber-regulation is special. The problem is we continue to use the language and rhetoric of social policy, sociology and political philosophy. We refer to the literature of communications theorists like Manuel Castells and Nicholas Negroponte, we apply Latourian, Foucaultian or Frankfurt School language to the study of our little part of the social world. We become social scientists not lawyers.

We make Easterbrook's argument for him – we are no longer cyberlawyers we are now cyber political scientists (or cyber political theorists). This was brought home to me recently when a colleague said to me quite baldly – what you do isn't law; you could be in almost any social science department and do the same research. I argued he was wrong, but he wasn't. The work I do is no different to that done by Robin Mansell (Media and Communications); Ian Brown (Information Systems) or John Naughton (Systems Engineering). The entire movement of Cyber-governance as populated by lawyers like myself, Jonathan Zittrain, Jack Goldsmith or Lee Bygrave demonstrates the need for cyberlawyers to justify themselves with reference to a wider debate; vitally a debate not founded on jurisprudence but upon other (non-legal) philosophical foundations. In so doing we differentiate ourselves from other lawyers.

A property law text is likely to cite Bentham, Birks, Dworkin, Hart, Hegel, Honore, Hohfeld, Hobbs, Kelsen, MacCormick, Posner, Raz and Waldron. A criminal law text is likely to cite Bentham, Blackstone, Denning, Garland, Hart, Honore, Horder, Kant, Locke and Williams. A cyberlaw text is significantly less likely to engage in this traditional jurisprudential debate. In the past we have told ourselves this is good. While our colleagues sit in the dark, narrow confines of legal orthodoxy we are in the light, taking an expansive, some may say cosmopolitan approach, but the truth is while we may say this inwardly, from the outside property lawyers and tax lawyers scratch their heads.

So is the answer to be found in that other genus, the applied cyberlawyer? This is more difficult for me to answer as I'm less familiar with this branch of the family. As someone who has dabbled in this area though I feel the answer is no. Mainstream privacy lawyers do not disrespect cyberprivacy lawyers but at all times remember (not consciously) Easterbrook's charge (as amended) that "all I could do in discussing 'Privacy in Cyberspace' would be to isolate the subject from the rest of the law of privacy, making the assessment weaker".

The same is unfortunately true of all other applied areas. Mainstream privacy lawyers, property lawyers, criminal lawyers and commercial lawyers see the application of their discipline within the "cyber" realm as a case-study for their subject not a separate or viable freestanding topic of study. The cyberlawyer who studies online defamation is a valuable colleague who takes time to learn the technical parameters of ISPs, SNPs and blog hosts. It saves them the time of learning the peculiarities of this place but they are not seen to illuminate the wider sphere of libel and defamation law. Cases like *Tamiz v Google* are interesting but do not get to the heart of their subject.

In other words this genus of the Cyberlaw family fulfils Easterbrook's claim of multidisciplinary dilettantism, the cross sterilisation of ideas where one puts together two fields to get the worst of both worlds.

However one approaches cyberlaw in the traditional sense therefore one finds oneself in Easterbrook's shadow. You are either a multidisciplinary dilettante or an apologist in the Lessig vein: a political or social scientist masquerading as a lawyer. This is hard to hear but it is how many colleagues outwith the field of cyberlaw or IT Law view our work. Either too narrow to contribute meaningfully to the subject or too wide and therefore not grounded in jurisprudence.

4. The rule of law

I do not believe cyberlaw is a cul-de-sac subject. I don't believe we are destined to be as short lived a discipline as railroad law. As cyberspace becomes ever more central to our everyday lives the daily issues of indecency, harm, taxation, privacy, and security (both financial and personal) are discussed and legislated for.

In the media in the last week of March we find a discussion of the Spamhaus DDOS attack, the ACLU challenge to the deployment of IMSI capture under the 4th Amendment, copyright and online piracy, the sexualisation of children through online content, BitCoin online currency, the delivery of government services and the digital divide and the privacy challenge of Google glass.

Although cyberlaw issues may not yet displace Kim Kardashian and Justin Bieber in the affections of tabloid newspaper editors, public discourse in the subjects we have been discussing for twenty years is at an all time high.

Regulators are also aware of the issues and have been quietly building a legal framework to manage these issues. To give but one example, let's take the measures introduced by the UK government to attempt to stem the tide of illegal file sharing and other forms of online copyright infringement (the issue is not whether these provisions will be effective just to examine why they were created).

The key support of the government's strategy is the Digital Economy Act (at least it was prior to the Newzbin litigation). How did this come about? More pertinently what was the input of the Cyberlawyer – surely the expert in this area? Well as we know the catalyst for the Digital Economy Act was the Digital Britain report. This was produced by a committee chaired by Lord Carter of Barnes, Minister for Communications, Technology and Broadcasting, who although he has an LLB spent his entire professional career in advertising and marketing before becoming Chief Executive of OFCOM. He was assisted by a team of twenty five civil servants and a steering board of industry experts. They were Peter Black (network engineer); Tanya Byron (clinical psychologist); Francesco Caio (banker/telecommunications executive); Andrew Chitty (digital media production); Barry Cox (Journalist/Broadcaster); Matthew d'Ancona (Journalist); Robin Foster (Economist); Andrew Gowers (Journalist/Banker); Ian McCulloch (Broadcaster); Peter Phillips (Ofcom) and Stephen Temple (electrical engineer). Note that while there were three journalists and two bankers on the steering panel there were no cyberlawyers.

Regulators do not see cyberlawyers as central to the debate on the regulation of activity in cyberspace. This can be seen in the activity of the Joint Committee on Privacy and Injunctions where one of the driving forces behind the formation of the committee was the events of spring 2011 – what one may call the Twitter spring – in which privacy injunctions were breached on an almost daily basis by Twitter users (as well as on Facebook, Wikipedia and other social platforms). This committee was assisted by three specialist advisers: Professor Eric Barendt, Emeritus Professor of Media Law at University College London; Sir Charles Gray, former High Court judge who specialised in media work; and Paul Potts CBE, Visiting Professor of Journalism at Sheffield University and former chief executive of the Press Association.

Again mainstream "old" media is represented throughout but cyberlawyers are conspicuously absent. In the evidence-gathering phase twenty seven days were given over to "old media" interests and three days to "new media". We are in danger of being marginalised by both academic colleagues and regulators unless we make ourselves relevant

How does one reset this? It is time for the rousing music and the beating of battle drums. Many of the markers for the future of Cyberlaw are already in place: we just need the confidence to follow them. The key is to re-engage with traditional jurisprudential models and thus to make ourselves relevant to lawmakers and lawyers in the way media lawyers have done.

Chris Reed began this with the work he did in the lead up to his book *Making Laws for Cyberspace* and in his keynote address here last year. Reed reintroduces legal positivism and perhaps rather counter intuitively given that, brings Lon Fuller and more intuitively Joseph Raz into the Cyberlaw analysis. I think to be honest in introducing elements of Raz and Fuller in a single text he offered an exciting opportunity but in his final analysis he was unfortunately rather timid.

His Modern Law Review article *How to Make Bad Law: Lessons from Cyberspace* was in many elements a more successful synthesis of the Fuller application at least. Here Reed attempts to deal with that most difficult question of Cyberlaw, or indeed any law question, what makes a law or lawmaker legitimate? This, as we all know is a particularly pertinent problem in cyberspace (see David Post) but of course is also a perennial jurisprudential question.

Reed focuses on Fuller's Morality of Law and notes that "Fuller has asserted that a minimum internal morality is a necessary prerequisite for a purported law-system to be effective in 'the enterprise of subjecting human conduct to the governance of rules.'" He points out that in Cyberlaw much applicable law (or rules) breaches three of Fuller's eight basic principles of internal morality.

> Principle 4: The law's rules should be understandable by those who have to comply with them
>
> Principle 5: Rules should not be contradictory, and
>
> Principle 7: Rules must not be changed too frequently to permit compliance

From this Reed draws general principles of good lawmaking, applicable in general, from the lessons and failures of Cyberspace concluding that "an alternative approach to lawmaking which addresses human behaviour and beliefs, rather than specifying compliance in precise and detailed terms, can produce a law which is not immediately implausible and which more closely meets the test for quality."

For me, this conclusion is gratifying as it is not dissimilar to the foundations of my symbiotic regulation model. Reed of course does not fully agree with symbiotic regulation, and neither he should, for it is a regulatory not a legal model. And so in many ways Reed shows us the past, but for me with two vital weaknesses - (1) in both the article and in his book, to me, he underplays Raz and the rule of law analysis and (2) he falls into the Lessig apologist position - the study of Cyberlaw is important because it illuminates the law elsewhere.

5. Cyberlaw and the rule of the law

To justify and the subject of Cyberlaw as a standalone legal subject we must stop apologising and start engaging jurisprudentially. To begin, I think the basic question of legitimacy and the rule of law in cyberspace offers a unique opportunity to kick start this discussion and to prove our worth to regulators. Regulators are regulating on the assumption that they have legitimacy and the right to do so. I saw this first hand at the Joint Parliamentary Committee on Privacy and Injunctions when Ian Brown and myself caused a senior Parliamentarian to turn puce with rage at the suggestion that "Her Majesty's Government for the United Kingdom of Great Britain and Northern Ireland were not vested with the authority to regulate activities in the wider Internet of UK citizens". The Rule of Law question - which should be primary and prior is being assumed based on historical sovereignty.

I think an analysis of the actions of regulatory actors online applying both Raz and Fuller is long overdue- this is the project I hoped to report on here but instead deliver an outline in the hope of inspiring others. Raz identified several principles that may be associated with the Rule of Law in some (but not all) societies.

Raz's principles encompass the requirements of guiding the individual's behaviour and minimising the danger that results from the exercise of discretionary power in an

arbitrary fashion. In this last respect he shares common ground with the constitutional theorists A. V. Dicey, Friedrich Hayek and E. P. Thompson. Raz's principles are:

- Laws should be prospective rather than retroactive.
- Laws should be stable and not changed too frequently, as lack of awareness of the law prevents one from being guided by it.
- There should be clear rules and procedures for making laws.
- The independence of the judiciary has to be guaranteed.
- The principles of natural justice should be observed, particularly those concerning the right to a fair hearing.
- The courts should have the power of judicial review over the way in which the other principles are implemented.
- The courts should be accessible; no man may be denied justice.
- The discretion of law enforcement and crime prevention agencies should not be allowed to pervert the law.

According to Raz, the validity of these principles depends upon the particular circumstances of different societies, whereas the rule of law, generally "is not to be confused with democracy, justice, equality (before the law or otherwise), human rights of any kind or respect for persons or for the dignity of man".

If the cyberlibertarians are right though there is no "law" for Cyberspace thus no "rule of law". To now turn Raz on his head we can look again at Lon Fuller and his eight routes of failure for any legal system:

- The lack of rules or law, which leads to ad-hoc and inconsistent adjudication.
- Failure to publicise or make known the rules of law.
- Unclear or obscure legislation that is impossible to understand.
- Retroactive legislation.
- Contradictions in the law.
- Demands that are beyond the power of the subjects and the ruled.
- Unstable legislation (ex. daily revisions of laws).
- Divergence between adjudication/administration and legislation.

It appears that there may commonly exist failures 1,5,6,7 in Cyberspace and maybe also failure 2 as given multiple jurisdictions one cannot know all relevant rules of law.

Thus both Raz and Fuller suggest problems with the Rule of Law and principles of natural justice - yet all too often regulators assume historical jurisdiction gives them extensive, expansive and legitimate authority to regulate activity online (without determining the spillover effects of their actions) - as Ian Brown and I saw first hand.

Questions should be asked afresh of regulators of all types: Interstate actors such as ISOC, ICANN, WSIS and WIPO; Supranational bodies such as the EU, EEA or MERCOSUR, to non-state actors such as Google, Microsoft or Apple and most pertinently and importantly to States Regulators such as the UK Parliament, OFCOM or to the Courts who act from historical authority and legitimacy - are your actions

legitimate, proportionate, and in accordance with the Rule of Law? In particular can you be sure your acts only affect individuals within your jurisdictional authority?

The problem it seems to me is that we have mostly thought of Cyberspace as a single place – a monolithic place which can be defined rather than a world populated by divergent communities and cultures and representative of (mostly) a domestic space. Regulators imagine it as a (more) fragmented environment - if you will a UK Cyberspace, a French Cyberspace, a Greek Cyberspace etc. each within their jurisdictional remit and each within their sovereign right to rule. This is the root of laws such as the Digital Economy Act or the HADOPI Law. It is this which leads to the Defamation Bill and the Data Protection Regulation. The problem with this fragmentation approach is overlapping controls and over regulation arguably in breach of Raz's and Fuller's principles.

Against the fragmented background - it is easy to imagine legal rules (and systems) which comply with both Fuller and Raz but we must not assume all laws passed by traditionally sovereign lawmakers automatically make the grade.

There can be, and indeed is, a functioning positivistic legal system for Cyberspace. Our role now is to be part of the debate, and not just as activists. By discussing the rule of law and its role online we can reposition ourselves as lawyers in the Cyberlaw environment who have a role in the lawmaking process - that is the domestic lawmaking process and how it affects us online.

The question of whether cyberspace is regulable is in the past for lawmakers and regulators. The question is how to most efficiently and effectively regulate it by law. Our role must be to ensure the rule of law is preserved. We must move to the fourth wave of Cyberlaw research and development. The first wave was cyberlibertarianism. The second wave was cyberpaternalism. The third wave was decentred regulation and regulatory theory – it is time to move to the fourth wave – Cyberlaw.