scripted

Volume 9, Issue 2, August 2012

LAWYERS AND CYBERSPACE: SEEING THE ELEPHANT?

Martina Gillen [*]

Abstract

This paper considers the problem of Internet regulation, and how it has been exacerbated by poor theoretical models for cyberspace. Furthermore, it considers how the conceptual difficulties with regard to the nature of cyberspace have been replicated in formulation of regulation. Having identified the key areas of difficulty, this paper then explores a potential solution building on the regulatory work of Chris Reed and Christopher Marsden. Using autopoietic theory to fuse their understanding of both the human, and technological aspects of Internet regulation, this paper aims to generate one coherent theory that would offer a flexible, responsive and effective regulatory model for cyberspace.

DOI: 10.2966/scrip.090212.130

[*] Senior Lecturer, Oxford Brookes University

1. Introduction

"Seeing the elephant", is an American phrase that was commonly used in the mid to late 19th century. It refers to learning about a wondrous new thing (like seeing a circus elephant for the first time) and often, though not always, this knowledge is tinged with disappointment. Subsequently, historians have revived the phrase. One particularly apposite use is that of John Reid who used the phrase as the title for his work on the bringing of law to the Western frontier.[1] Elephant is used here to evoke all these images, excitement, deflation and the journey of law to new land. Internet Technology has now developed to the point that we are able to speak of multiple generations and kinds of networked technology. The Internet is now accessible via not just computers but also mobile phones, Netbooks and other wireless and wired devices (e.g. televisions and Ebook readers).

The Internet is also the subject of more legislation than at any time before and also subject to a broader range of regulatory activities than at any time before. Yet, despite this apparent colonisation of cyberspace by the legal realm, there are clear indicators that there is serious and meaningful conflict going on between traditional (and pseudo traditional) legal definitions and jurisdictional markers on the one hand, and technological development on the other.

The contention at the heart of this paper is that lawyers are not, as they might imagine, intrepid explorers who have successfully colonised a new territory, but are instead, like the folk tale of the blind men arguing over the nature of the elephant when they have only held a trunk or a tail. In other words, lawyers have struggled to develop a conceptual model of cyberspace that is in complete harmony with technological and social reality, and even where adequate conceptual models are developed they are applied within inadequate or inappropriate regulatory frameworks. With this problem in mind we shall build upon the work of Andrew Murray on law and autopoiesis in cyberspace regulation. This paper argues that an appropriate model can be found but only if the emphasis in the search shifts from asking either whether cyberspace constitutes a new and distinct jurisdiction or considering the relationships and human connections which occur when users are connected by networks, to a mode of analysis that recognises that both these elements are intrinsic parts of the system and takes advantage of them.

The advent of cyberspace into the day to day fabric of modern society has caused digital communications to become an important legislative and regulatory object. Lawyers and policy makers from a variety of philosophies and backgrounds have endeavoured to describe and conceptualise the nature of cyberspace. Thus, positions and perspectives on the issues have proliferated. The thesis at the heart of this paper is that legal theory and practice are currently lagging behind technological and social developments, because despite repeated attempts to do so, we have not yet developed an appropriate conception of cyberspace and its role in modern life which can be dovetailed into a functional regulatory model. This deficiency is partially the result of the genuine novelty of the technological phenomena, and partially the product of the

---

[1] J Reid, *Law for the Elephant: Property and Behaviour on the Overland Trail* (California: University of California Press, 1996).

legal tendency to reason from analogies to well-established phenomena, or earlier legal theories. This tendency, although not necessarily harmful in and of itself, can become damaging when an analogy is viewed as a like-for-like comparison, regardless of the actual degree of fit (likeness) with the phenomenon being analysed.

In this section we shall briefly explore the problems of conceptualising cyberspace, before considering the conceptions which have been adopted. We shall also consider the degree of fit that the common legal analogies have with technology. Ultimately, building on the work of Murray, we shall conclude with some suggestions of how to formulate a paradigm based upon autopoiesis which fits more completely with developing technologies and offers a path toward a functional and efficient mode of regulation

1.1 The conceptual problems posed by cyberspace

To those already cognisant of this debate, the use of the term cyberspace itself pre-supposes a particular view of the environments created by networked technologies. However, the term cyberspace will be used in this paper because its meaning is generally clear, and the formulation of a truly neutral term would be difficult and cumbersome. In a general sense, the problem of the theorisation of cyberspace is that it exacerbates our difficulties of description and conceptualisation. Simply put, our ability to conceive something is limited by our language, our physical perceptions and our mode of reasoning.[2] When considering cyberspace the challenges faced by our conceptual tools are readily apparent, as there is a vast range of new types of communications, interactions, and activities possible and even technological and cultural experts cannot be appraised of all developments at all times. Legal modes of discourse have not acted as a panacea to this problem. Indeed, as Svantesson has noted, legal reasoning may be particularly vulnerable to these problems because of its lack of direct consideration of cyberspace in itself as opposed to cyberspace as a legal subject:

> ...faced with the task of evaluating the applicability of existing legal rules to fact scenarios involving Internet activities...it has been remarked that "[j]udges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average American five-year-old tosses about with breezy familiarity." ...one of the reasons why judges and legislators, as well as other legal professionals, struggle with the new technology, is that surprisingly little efforts have been directed at analysing what makes the Internet different.[3]

---

[2] This problem and the philosophical gap between the conception and the thing described have been explored at length in the work of A Korzybski, *Science and Sanity: An Introduction to Non-Aristotelian Systems and General Semantics* (Closter, NJ: Institute of General Semantics, 1995).

[3] D Svantesson, "The characteristics making Internet communication challenge traditional models of regulation: What every international jurist should know about the Internet" (2005) 13 *International Journal of Law and Information Technology* 39-69, at 40.

Whilst, ultimately, this article wishes to suggest methodologies for regulators to engage more directly with Internet technology and possible theoretical frameworks for doing so, it will first be necessary to explain the prevalent legal analogies for cyberspace and offer some illustrations of the mismatch between them and technological and social realities. It is hoped that this article would serve as a spark to ignite further thought in the area.

2. Prevalent analogies

The central question for lawyers, accustomed as we are to considering the world in terms of rules and the ability to apply them through the exercise of jurisdiction, is: "How will we control cyberspace?". Intrinsically linked with this question are the related queries: "Is cyberspace a new and different space to those we have experienced before?" and "Do we need new means of regulation to exercise our jurisdiction?" (readers should note that the legal discourse has been marked by a lack of consideration of the otherwise *a priori* question "Do we have jurisdiction?". Jurisdiction has been treated by legal commentators as something of a given, as we shall see when we look at the cyber-sceptic, and some elements of the cyber-conservationist approaches). Thus, we shall be considering how the core analogies conceptualise cyberspace as a space (or not) and the type of legislative response this engenders. It should be noted at this point that many of these modes of analysis were adopted in the mid to late 1990s, as affordable personal computers and Internet connections became more readily available in the home, and thus raised the profile of the Internet as a domestic regulatory issue. Many models have evolved little since then. As we shall see, the legal mode of discourse vacillates between concern with the "space" of cyberspace and the jurisdictional challenges it poses, and concern focusing purely on regulatory behaviours and how to control the interactions of users. In other words, the discourse has always been a focused on the appropriate reaction of legal/political institutions to cyberspace and the interactions that it facilitates not an examination of that space or those interactions for their own sake. This perspective has caused legal discourse to miss some of the self-regulatory potential of the sphere.

2.1 Cyber-libertarians

The essence of the cyber-libertarian approach is that cyberspace is a distinct new space and that it can (or should) not be regulated by the state.[4] This approach was first developed by the more thoughtful technologists among the early adopters of the Internet. It reflected their personal aspirations and attitudes. Furthermore, the

[4] It may be useful here to recall that many of these theories have an American origin and so the definition of libertarian used here means not only someone who focuses on the protection of freedoms but it is also coloured by that exclusively US brand of Libertarianism which focuses on the limitation of state power and emphasises that any power exercised by the state is enjoyed purely because of the voluntary consent of the governed. This US approach can lead the brand libertarian being applied to many thinkers who would be labelled conservative or reactionary elsewhere. This is not the case with cyber-libertarians but this has been part of the reasoning behind some of the categorisations used later in this article. For a discussion of the various forms of libertarianism prevalent in the US today an accessible biography of many of the main players can be found in W Block, "I Choose Liberty: Biographies of Contemporary Libertarians" (2010) available at http://www.mises.org/books/chose_liberty_block.pdf (accessed 20 July 2012).

technology, as they saw it, not only functioned better without centralised control but made such control impossible. A good example of this early form of cyber-libertarian thought is John Perry Barlow's "A Declaration of Independence of Cyberspace".[5] The "Declaration" is a polemic written after the American government passed telecommunications legislation which Barlow viewed as overly invasive. Its key points are firstly, that cyberspace is a new and distinct space, and secondly its denizens use technological means to develop their own form(s) of social contract independent of traditional established states and without the preconceptions caused by physical embodiment. Formal governments have, according to Barlow, no mandate for interference with such a sphere, nor indeed the ability to interfere in the normal way.

> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, There is no matter here...The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.[6]

Barlow himself described the language of the declaration as grandiose in the message preceding it. Despite Barlow's recognition that text was an aspirational document and not a practical manifesto it did provide the mode of thought underpinning the Electronic Frontier Foundation - a powerful cyberspace lobbying group. Lawyers were attracted by the resonances this radical agenda had for more classical libertarian views about personal freedom and democracy. The key work in this more legally oriented vein is Johnson and Post's *Law and Borders: The Rise of Law in Cyberspace*.[7] This paper agreed that centralised control in the form of the sovereign state was not workable in cyberspace. However, they also strongly believed that users would develop their own customary law organically as they selected rule sets and cyberspace zones suitable for their own needs; thus the only possible regulatory system was the one developed by the consent of the users.

> But when the 'persons' in question are not whole people, when their 'property' is intangible and portable, and when all concerned may readily escape a jurisdiction they do not find empowering, the relationship between the 'citizen' and the 'state' changes radically. Law, defined as a thoughtful group conversation about core values, will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically-defined territories.[8]

The cyber-libertarians face wide-reaching difficulties. The traditional,

---

[5] J Barlow, "A Declaration of Independence of Cyberspace" (1996) available at http://www.ibiblio.org/netchange/hotstuff/barlow.html (accessed 20 July 2012).

[6] *Ibid.*

[7] D Johnson and D Post, "Law and Borders: The Rise of Law in Cyberspace" (1996) 48 *Stanford Law Review* 1367-1402.

[8] *Ibid* VI.

technologically-focused branch of this school was correct in identifying that new methods of control outside the purview of the state would develop. However, as a rule these sorts of controls require technical power (the ability to silence other users, cancel their communications or exclude them from the space) or group sanction (flaming).[9] In practice this means they are often only available to enforce policies laid down by the cyberspace locations creator or controller, who have a privileged position to exercise such rights or to gather community support. Such mechanisms are often either inefficient or inaccessible for many users as they require contact with a technical controller or their representative, or stirring up group support. Furthermore, users might fear reprisal and an escalation of conflict.[10]

The more legally minded libertarian approaches wish to view cyberspace as a location with potential for re-invigoration of civil society and democracy through the development of mutually agreed rules about the rights and duties of individuals. This has had problems on two levels. The first level is in the balancing of interests or clash of rights.11 Prioritisation is a general difficulty with regard to human rights, but it holds particular problems for cyberspace because the current prioritisation of rights will always favour anything with an offline or corporeal element.[12] Naturally, the right to life and freedom from torture, and always should, trump expression in a real world context. However, is this a fair method of prioritisation in the on-line context where everything is expression? Many rights infringements that seriously impact on the quality of a person's cyber-life, for example, being cheated of virtual property in a game world, seem trivial or even absurd when viewed through the lens of standard rights analysis.[13] If legal scholars struggle with conceptualising and prioritising rights, how could user groups be expected to resolve this weighty dilemma for themselves as the cyber-libertarians suggest? Even if the obvious solution of treating all expressions as equal is adopted, this does not resolve the practical problem of the difficulty of accessing technical enforcement mechanisms.

Enforcement is at the core of the second issue with this type of theory. Who has the obligation to ensure we enjoy our rights online? Who has the duty that is the corollary of our individual rights? As citizens in the off-line world our rights are secured by the coercive power of the state, but there is no cyberstate government (nor would many of

---

[9] For an overview of this kind of control mechanism see T Maltz, "Customary Law & Power in Internet Communities" (1996) 2 *Journal of Computer-Mediated Communication* available at http://jcmc.indiana.edu/vol2/issue1/custom.html (accessed 20 July 2012).

[10] A useful critique of this approach to control can be found in N Netanal, "Cyberspace Self-Governance: A Sceptical View from Liberal Democratic Theory" (2000) 88 *California Law Review* 395-498.

[11] For a taste of how complex this issue can be see P Montague, "When Rights Conflict"' (2001) 7 *Legal Theory* 257–277.

[12] A simple but illustrative example of this can be found in the European Convention of Human Rights. The absolute rights are largely of a physical nature, for example the right to life, freedom from torture and slavery etc. The limited or qualified rights deal with intangibles and focus on physical things necessary to take part in the life of a democratic society (freedom of assembly and expression (the emphasis being on political protest). Clearly, this prioritisation favours physical embodiment.

[13] See S Wolfendale, "Virtual Harm and Attachment" (2009) available at www.aifs.gov.au/acssa/pubs/newsletter/n21pdf/n21d.pdf (accessed 20 July 2012) and A Arias, "*Life, Liberty, and the Pursuit of Swords and Armour: Regulating the Theft of Virtual Goods"* (2007-2008) 57 Emory Law Journal *1301-1346.*

those espousing user empowerment in this space wish there to be). Self-regulation mechanisms can work quite well, but only where there is a clear context and description of the rights and obligations involved (for example the voluntary arbitration schemes used by many online market places). However, not all interactions are so clear cut. A single interaction may involve multiple users across a range of countries, inhabiting different personae to those recognised as bearing rights as citizens by their states. Rights need to be re-conceptualised for cyberspace, not simply applied to it. Communication and expression need to be given their proper weight for this sphere. It is not clear, how user-led cyber-democracies on their own, can create a functional and legitimate rights enforcement mechanism, beyond the limited scenarios already discussed. An assertion that this will evolve organically will not actually cause this to happen and it certainly will not cause it to happen in a sustainable and appropriate way.

2.2 Cyber-sceptics

As the name suggests the cyber-sceptics do not agree that cyberspace is a distinct jurisdiction; for them it is the same as any other human technology and those who purport to find such a new phenomenon in cyberspace are mere meddlers and dilettantes. Rather, academics would be better spending their time diligently pursuing the study of traditional legal subjects and, in understanding them, the appropriate principles to apply to cyberspace (or indeed any other new social phenomenon) would become apparent. Thus, as Easterbrook put it, since there was no law of the horse (the horse being a vital element in the colonisation and transformation of) there was not nor should there be law of cyberspace:[14]

> ...the best way to learn the law applicable to specialized 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, 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.[15]

This thinking is similar to the jurisprudence of Ronald Dworkin.[16] Dworkin has

---

[14] F Easterbrook, "Cyberspace and the Law of the Horse" (1996) available at http://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf (accessed 20 July 2012).

[15] *Ibid*, 207ff.

[16] R Dworkin *Taking Rights Seriously* (Bristol: Gerald Duckworth & co., 1996).

hypothesised an idealised judge called Hercules, who extrapolates the correct answer to "hard" (morally complex and/or legally unprecedented) cases by using his encyclopaedic knowledge of the law to work out what the "correct" resolution should be, based on the established principles of the legal system. Dworkin persists in the validity of the model despite the fact that Hercules is an idealised figure and no real human judge, no matter how learned, could possess the required degree of knowledge. The theory does, however, illustrate the tendency in legal thought to value consistency and conformity with established rules as the way to find the "right" answer to new problems rather than innovation or re-conceptualisation.

The major benefit of this kind of approach, from a lawyer's perspective, is that it permits a shift of focus and allows the issues around cyberspace to become legal rather than technological or social questions, thereby rendering them more amenable to regulation. In other words, the problems of cyberspace can be made to seem soluble by the application of established legal principles, and not as novel issues which need to be understood in their sociological or technological context. This approach fits well with the tendency identified by Shklar (which in some senses underpins this article) for lawyers to favour legal modes of discourse and to interpret actions and inter-relations in terms of already established legal rules and analogies.[17] However, as a corollary of that, this approach would seem to be particularly vulnerable with regard to Svantesson's critique already mentioned: that it is technology which is the under-examined aspect of the problem. Thus, further study of the law would be of little assistance as it does not help us identify the salient aspects of the technology.

In some senses, the weaknesses of a system which refuses to recognise the novelty of a so transparently socially transformative technology should be readily apparent. Furthermore, we do have law for particular physical zones and spheres (maritime law and aviation law), therefore the "law of the horse" argument may just be another instance of embodiment bias and is certainly not definitive. The main reason for critiquing this model, however, is that the reification of legal rules and norms can lead to absurd results. A good example is the classification of removal of DRM (Digital Rights Management), or similar technologies, as a computer security/misuse offence. In other words, placing DRM removal within the class of activities which cause criminal harm to computers and networked systems (see the recent guidance on applying the Computer Misuse Act[18]). DRM systems limit the functionality of content files in accordance with the wishes of the original creator, and therefore, in a purely technical sense, actually prevent a computer from performing the full potential range of actions upon the file (for example copying or sharing). Given the obvious fact, that increasing a system's functionality is the exact opposite of causing it harm, this illustrates the danger of legal debates which are not firmly grounded in technological reality. Due to purely legal considerations a copyright protection mechanism, inserted into systems purely to secure proprietary rights, can be given the same protection as something which is essential for safe functioning. Furthermore, this is despite the fact that many in the IT industry agree that DRM is a poor copyright protection system, in that it is both technically vulnerable and allows copyright holders to extend their rights beyond that afforded by copyright law (the so called "paracopyright"

---

[17] J Shklar, *Legalism* (Cambridge, MA.: Harvard University Press, 1964).

[18] Crown Prosecution Service, "Computer Misuse Act 1990: Guidance" available at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/index.html (accessed 20 July 2012).

protections). Therefore even the arguments to offer it legal protection on the basis of proprietary rights alone cannot really be justified.[19] Legal modes of analysis clearly do not always fit with cyberspace.[20] Cyberspace needs theory which allows it to be viewed as something affected by law without becoming solely defined by it and subject to it.

2.3 Cyber-conservationists

The label used for this section may be considered somewhat controversial due to the thinkers it brings together, since they are often viewed as being at opposite ends of the political spectrum. Nevertheless, there are two reasons for the adoption of this approach. The first, and most compelling, is that both schools of thought adopt a viewpoint based upon the need to protect some component of the cyberspace equation from harm. Specifically, protecting unsuspecting users, menaced by the shadowy lurkers in the underbelly of the Net, or in contrast, protecting the much vaunted public forum of the Net itself, from the machinations of States and corporations. The second reason is that the libertarian approaches here are more strongly tinted by the conservatism inherent in the US definition of libertarianism we discussed above at footnote four. This re-classification highlights resonances between these two approaches that might otherwise be ignored as a result of their apparent political difference.

The first conservationist approach is usually espoused by those from the political centre to right, who insist that cyberspace is a dangerous space, and therefore that asserting control and normalising (or perhaps more correctly rendering it into established legal terms and categories) cyberspace, is necessary to protect national and user interests.[21]

The second conservationist approach, which is usually adopted by those from the middle to left of the political spectrum, takes the view that cyberspace is not a dangerous but rather an endangered space (a view linked to the cyber-libertarian approach). These conservationists argue that the customs and values inherent in cyberspace need legal regulatory protection in order to preserve what is liberal and democratic about cyberspace from damaging external encroachment. This is an inherently precarious position and slightly self-contradictory from a purely logical

---

[19] e.g. D Burk, "Anti-Circumvention Misuse" (2002) available at http://ssrn.com/abstract_id=320961 (accessed 20 July 2012).

[20] In order to maintain the focus of this work, I have chosen not to raise the question of the validity of applying copyright to software in this article. Nevertheless, the widespread debate about this question and Open and Free Software practices do add weight to the present argument that legal norms are out of step with technological considerations and non-traditional legal solutions should be favoured for technological and social reasons.

[21] An excellent example of this approach can be found in the extreme pornography laws in s63 of the United Kingdom's Criminal Justice and Immigration Act 2008. Although critics could dismiss this as a unique response to a tragic set of circumstances, when taken in conjunction with anti-grooming laws (the Sexual Offence Act 2003 makes specific reference to grooming), public information campaigns on cyber-safety for children and the prevalence of media reports highlighting the deleterious impact of social networking software on society, it becomes clear that there is a widely held view, influencing the public sphere, that cyberspace is inherently chaotic and dangerous and in need of control in order to protect both individuals and society.

perspective, but if the right balance of the competing interests is maintained it can work in practice. The key aspect in this conception is that the user is not treated as a vulnerable being who is potential prey to the dangers of this pervasive and pernicious space, but rather as an empowered and rational agent capable of choosing how to act. As an empowered actor the user is capable of making meaningful contributions to their virtual society through networking and the other technical opportunities that cyberspace offers. The goal then becomes to protect the elements of cyberspace which encourage and enable this capacity, in both individuals and groups. Thus, these thinkers become the environmentalists of cyberspace. From the legal perspective the best known thinker in this group is probably Lawrence Lessig. Lessig initially became concerned with intellectual property law and cyberspace because of his ideas about constitutional authenticity and the reasoning behind the ban on perpetual copyrights in the United States Constitution which seemed to be under attack from modern copyright practices (he has in fact now returned to constitutional law after many years of work on cyberspace and the development of the Creative Commons Licensing regime).[22] The stated aim of Creative Commons is to:

> ...use private rights to create public goods: creative works set free for certain uses. Like the free software and open-source movements, our ends are cooperative and community-minded, but our means are voluntary and libertarian. We work to offer creators a best-of-both-worlds way to protect their works while encouraging certain uses of them – to declare 'some rights reserved'.[23]

The theoretical problems facing these conservationist approaches are fundamental. Despite their apparent differences they share the common element that, as the name suggests, they wish some element of human/technological interaction to remain stable and unchanged. Since technology is constantly advancing, and the underlying purpose of cyberspace is to facilitate communications and interactions, which given their social proliferation seem to include an ever expanding range of human activities, these approaches seem almost destined to fail because change is part of the essential nature of the cyberspace experience they wish to conserve. Furthermore, their definitions of what needs to be conserved either become stultified and unfeasibly restrictive, or evolve and change and thus defeat their own original goal of resisting change. To give a simple example, imagine as a libertarian conservationist one wished to preserve the democratic potential of a particular form of group self-governance online, and therefore, offered some form of legal support, like making community arbitrations legally binding. This would put a legal barrier in place to discourage communities from altering their own governance. This is surely contrary to the democratic principle one was trying to preserve. On the other hand if the protectionist school of cyber-conservation wished to protect users from a potential email scam and thus legally mandated the use of a certain type of filter, technological change would quickly make it redundant and leave users vulnerable and possibly with the false

---

[22] L Lessig, "Free Culture lecture" (31 Jan 2008) available at http://blip.tv/esfwork/lawrence-lessig-january-31st-2008-stanford-university-686508 (accessed 20 July 2012).

[23] Creative Commons, "Some Rights Reserved: Building a Layer of Reasonable Copyright" (April 2010) available at http://wiki.creativecommons.org/History (accessed 20 July 2012).

sense of security because of the filter law.

The global nature of the cyberspace phenomenon means that there are legal enforceability issues for those who view cyberspace as dangerous (we shall return to the problems of technical enforceability later). In addition, there is also the clash of societal norms that such enforceability would cause. For those who wish to preserve cyberspace, viewing it as endangered by government encroachment, the hard truth is that the change in user demographics (the expansion of accessibility of the Internet from an educational and technological elite to large swathes of the population in developed nations) now means that cyberspace will be of prime concern to all national governments.[24] Also the degree of knowledge and agency on the part of the user traditionally presupposed by this model is no longer tenable (hence the increased governmental interest). Cyberspace needs theory which allows the proper weighing and balancing of the factors influencing its self-creation in a dynamic fashion to be observed and taken into account.

2.4 Politico-legal mappers

These theorists begin to move beyond the idea of cyberspace as a space, into the consideration of cyberspace as a range of complex relationships. This approach can be seen as prefiguring and informing the position advocated in this paper, which hopes to build upon the strengths of this approach, by using an understanding of cyberspace interactions to inform the regulatory framework. The notion of treating cyberspace as a cartography of political relations mediated by technology began with Jeremy Crampton's seminal work The Political Mapping of Cyberspace. Crampton is primarily a critical cartographer, who follows Foucauldian thought in holding cyberspace to be a space which simultaneously produces and is produced by human subjects. For the purposes of this paper Crampton's work has two main themes. Firstly, examining how users create themselves in cyberspace based on Heidegger's critique of the "metaphysics of presence".

> Instead of practices which produce the truth concerning oneself in a field of normalization (traditional of juridico-religious confession) cyberspace can be the ground for self-writing in communities which effect an ethos of care of the self.[25]

Secondly, Crampton then considers how cyberspace technologies have become disciplinary technologies. He explores how their increased use as tools of penality, (and therefore as limiters of self-creation), has had negative effects on the privacy of the general population. This has caused the technologies to become an arena of political struggle.

The major legal mapping analysis of cyberspace is that of Andrew Chadwick. In

---

[24] The World Bank gives clear evidence of this in its World development Indicators. In the UK for example there was less than 1% of the population with access to the Internet in 1990, which rose to just short of 85% in 2010 available at http://data.worldbank.org/indicator/IT.NET.USER.P2 (accessed 20 July 2012).

[25] J Crampton, *The Political Mapping of Cyberspace* (Edinburgh: Edinburgh University Press, 2003), at 98.

Internet Politics: States, Citizens, and New Communication Technologies, after introducing the reader to cyberspace, he picks up the twin themes of both user empowerment and also the important role of state policy in shaping users' rights. Almost inevitably this leads to a consideration of the economic power of copyright holders and how it is being mediated by International law.

Chadwick argues that the propaganda which surrounds the notion of the information society, the so-called new "information age", is used to reinforce the myth of inevitability. Inevitability, in this context, means that the symbols of the information society generate a mythical future, which is then turned into the natural and inescapable endpoint of technological progression. The information society becomes a self-fulfilling prophecy, demanding actions to deal with an impending social change, actions which actually produce the predicted social change. His argument is that the Internet allows for a new "electronic face" of government, which has previously been unavailable. Although there are clearly areas of tension and disjuncture (as with surveillance for example) Chadwick predicts that social and technological change will largely be managed by the increasingly media savvy governments, in the same way that they have traditionally handled these issues.

This seems like a true case of lawyers "seeing the elephant" of cyberspace. Initial optimism about the capacity of the Internet to revive/transform civil society (so called e-democracy) and user empowerment, has gradually been displaced by the deflation associated with the continued reality of government business proceeding as usual (albeit with more superficial attempts at consultation).

> Such developments might suggest that the major liberal democracies will soon converge on a Singapore-style model. The authoritarian city-state has long been perceived as the acme of managerial e-government, with a ruthless focus on using IT to stamp out waste and duplication. However, perhaps this assumption is misleading, because Singapore has recently developed the successful online Government Consultation Portal....[26]

Thus, we can see that the twin themes of the mapping theorists are not, ironically enough, centred around the "spaceness" of cyberspace, but around its use as a technology of self-creation and as a tool for state proliferation into, and control of, that sphere.

The strength of these theories is that they identify the human element of the cybersystem and consider how it interacts with technologies. However, because they are engaged in the act of mapping, these images are a freeze frame of certain sections of this relationship at any given time. Also, like a real map, they are constrained by the lines of latitude and longitude they lay down for themselves. In this instance they are circumscribed by a predetermination to examine particular legal and political questions. They are descriptive rather than explanatory and as such cannot be used to direct or shape policy.

2.5 Regulators

---

[26] A Chadwick, *Internet Politics: States, Citizens, and New Communication Technologies* (Oxford: OUP, 2006), at 323.

If the rise of the home PC opened the door of cyberspace to regulators, then wireless technologies, Web 2.0 software development techniques, and IPv6 wedged it wide open. In April 2012 there were more than 670 million websites (including sub pages) with domain names and content on the Net.[27] Compared to just 18,000 in August 1995,[28] this is a total increase of more than 3.7 million percent over the last 17 years. However, a significant share of this increase was only generated over the last two to three years.[29] This exponential increase has moved cyberspace to the top of the regulatory agenda. This increase coupled with the insights gained by the mappers discussed above has also lead current theorists to change how they consider cyberspace. Now instead of debating the nature of the space and whether or not it is a new legal entity, they are concerned with controlling the access to data and potential for interactions it provides. Thus, we see a marked increase in debates about content regulation over a rage of legal fields,[30] cyber-security[31] and ecommerce[32] in legal discourse, whilst the practical management of the infrastructure is left to non-governmental technical agencies like Internet Engineering task force.[33] Furthermore, in practice regulators often subdivide issues and spread them across departments and discourses. Klimburg and Mirtl's comment on cybersecurity encapsulate the wider problem:

> Within the general context of discussing "national cybersecurity" it is very important to keep in mind that it is not one single subject matter. Rather, it is possible to split the issue of national cybersecurity into five distinct perspectives or "mandates", each of them usually covered by different government departments. This is not an ideal state. Unfortunately, there is normally always a significant lack of co-ordination between these organisations, and this lack of coordination is perhaps one of the most serious organisational challenges within the domain of national cybersecurity. Furthermore, overlap between themes and ambiguity is the rule, not the exception, in cybersecurity. The physical reality of national cybersecurity is that all these topics overlap to a large extent, however the bureaucratic reality as lived in nearly all national governments is that these subject areas are kept separate from each other in distinct "mandates". Each of these mandates has

---

[27] Netcraft, "April 2012 Web Server Survey" (2012) available at http://news.netcraft.com/archives/2012/04/04/april-2012-web-server-survey.html (accessed 20 July 2012).

[28] M Walton, "Web reaches new milestone: 100 million sites" (2006) http://edition.cnn.com/2006/TECH/internet/11/01/100millionwebsites/ (accessed 20 July 2012).

[29] See note 27 above.

[30] This area has greatly proliferated with work on content regulation including obscenity, defamation and copyright breach.

[31] For an overview of recent issues see D Fidler, "Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law" (2012) 6 *Insights* available at http://www.asil.org/insights120620.cfm (accessed 20 July 2012).

[32] A Alghamdi, *The Law of E-Commerce: E-Contracts, E-Business* (UK: AnchorHouseUK, 2011).

[33] Internet Engineering Task Force available at http://www.ietf.org/ (accessed 20 July 2012).

> developed its own emphasis and even own language, despite the fact that they are all simply different facets of the same problem.[34]

Thus, as we shall explore, despite the novelty of technological and sociological experiences being regulated, and the mapping of these new relationships by the theorists just discussed, those in the regulatory field seem to be recycling the same old conceptions and tropes but cloaking them in the language of regulatory models rather than as arguments about the "space" of cyberspace. (Even Reed and Murray whose work we will discuss below could be easily slotted into the cyber-libertarian framework.) In this section we examine some of the main modes of Internet governance and explain how they replicate the divisions and errors of the schools already described. This development although disappointing, is hardly surprising, after all one makes a restraint fit for an elephant, based on one's idea of the strengths and weaknesses of the elephant.

There are a number of different ways of viewing Internet regulation, both Guadamuz[35] and Mayer-Schonberger,[36] give convincing accounts of the nature of the existing regulatory framework, and of the need for a fundamental re-shaping of the discipline, if regulation is to be effective. Guadamuz bases his argument on network complexity, and Mayer-Schonberger on the need to blend traditional existing governance models together to deal with cyberspace. The reader should note that even in examining these two authors who try to give an overview of the area, the dichotomy between discourses which take technology (Guadamuz) and, discourses which take law (Mayer-Schonberger) as their point of origin is obvious. Yet, despite differences in labelling and forms of classification, both works reveal a trend with resonance for this work.

The conservationists and mappers are the impetus behind the regulatory impulse. Information about the social conditions prevalent in cyberspace has fuelled the conservationist desire to protect and conserve. In particular those interested in protecting users and guarding national interests have felt the need to regulate across a number of areas. However, instead of producing fresh and responsive regulatory frameworks, they are being trapped within the old discourses.

There is a clear thread of scepticism in regulatory discourse, Mayer-Schonberger refers to this as "state based traditionalist discourse",[37] Guadamuz makes it the crux of his work highlighting that the failure to recognise the self-organising capacity of the Internet will ultimately lead to the failure of regulatory efforts.[38]

The parallels also continue strongly when one looks at the cyber-libertarian paradigm.

---

[34] A Klimburg and P Mirtl, "Cyberspace and Governance a Primer" (2011) available at http://www.oiip.ac.at/publikationen/policy-paper/publikationen-detail/article/93/cyberspace-and-governance-a-primer.html (accessed 20 July 2012), at 9.

[35] A Guadamuz, *Networks, Complexity and Internet Regulation: Scale-free Law* (UK: Edward Elgar, 2011).

[36] V Mayer Schonberger, "The Shape of Governance: Analyzing the World of Internet Regulation" (2002-2003) 43 *Virginia Journal of International Law* 605-673.

[37] See note 36 above, at 612-618.

[38] See note 35 above, at 214-215.

They are directly discussed in Guadamuz work[39] and clearly can be seen in Mayer-Schonberger's "cyber-separatists".[40] Indeed, this type of thinking proliferates across many of the works proposing self-regulation. Some see self-regulation as the way of achieving the revived civil society[41] and that the correct way to resolve the issues is to engage more fully with the private sector stakeholders for economic as well as legal reasons. (Marsden's work is one exemplar of this model.[42])

Thus, the potential insights gained by the "mappers" have largely been squandered, in the battle between the libertarians and the sceptics. In the fight between these two great elephant paradigms the green shoots of effective and responsive regulation have been trampled.

2.6 Summary

The analogies explored all suffer from some fundamental problem, they do not respond to the dynamic nature of cyberspace or the complexity of the human interactions it facilitates. Cyber-libertarians struggle to deal with competing rights, and they have no clear path to forming effective enforcement mechanisms. Cyber-sceptics find it difficult to move beyond the application of established legal ideas, regardless of their degree of "fit" with cyberspace. Despite their political diversity cyber-conservationists wish to stultify some aspects of the growing and dynamic cyberspace phenomenon, an approach which seems transparently weak. The social mappers, despite some excellent data gathering, can offer only descriptive rather than proscriptive analysis. Regulators try to build on this work but remain mired in the old paradigms.

Some key element is always missing. Theorists either focus on spatial considerations to the detriment of human interactions, or conversely offer a vision of interactions which is technologically or socially unsustainable.

3. Recommendations

Thus, we can see the existing analogies for cyberspace within the legal realm are inadequate. This paper does not seek to directly posit alternative paradigms since this would arguably require a large amount of empirical research beyond the present scope of this work. However, this paper will explore a theoretical framework wherein such ideation is possible. Previous models, as we have seen, have proven insufficient to adequately reflect cyberspace. This paper hopes to show how the best elements of some existing theories can be fused to resolve the problem. We shall, therefore, take the reader methodically through the development of this new "fusion" approach. The first step in developing this framework is to consider the nature of cyberspace, much

---

[39] See note 35 at 83-86.

[40] See note 36 above, at 618-626.

[41] See C Fuchs, *Internet and Society: Social Theory in the Information Age* (New York: Routledge, 2008).

[42] See C Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge: CUP, 2011).

as Svantesson suggested. However, in order to avoid becoming technologically deterministic, and also to focus on the aspect of cyberspace which is pertinent to regulation, the examination will consider online behaviour and the sociology of how users view and use the space.[43] The second, interconnected, step is to begin to try and view collective user creation of cyberspace through a different theoretical lens: a lens which allows us to view user behaviour as not simply a mechanistic product of legal or technological advances but as something more substantial and powerful in and of itself. This approach is an attempt to counter-balance the prevailing trend by seeking to fit regulation to the patterns of cyberspace not to pre-existing legal ideas. The theoretical framework posited here is autopoiesis which we shall now go on to discuss in detail.

3.1 The theory of autopoiesis

As a theory autopoiesis was first posited in the biological sciences to differentiate between the living and the non-living.[44] It is an explanatory theory of how entities develop and govern themselves. The influential scholar Luhmann accomplished an interesting "theory transfer" into the world of sociology; he posited the idea that self-organising and self-reproducing social systems (autopoietic systems) reproduce and maintain their structure not because of the characteristics of individuals, the demarcation of specific roles, or even through deliberate acts but via their process of communication.[45] This is particularly interesting when one is considering that this means that systems can be self-referential. In other words they can communicate about their communications and develop themselves reflectively in that way. Cyberspace by its very nature seems perfectly suited to this form of analysis as it presents itself as a discrete world of interconnected communications.

In relation to social systems, autopoiesis suggests that all that can ever accurately be observed is the system's communications. Through this observation, by learning to understand the system's language, or, to use Luhmann's preferred term, the "code" it employs, we can work out what a system's function is. This "code" can then develop into a "program" (a series of expressions in that language) which expands and solidifies code making it possible to do things with it. Finally, when we examine this program we can determine what effects it has in practice, what Luhmann calls its "efficiency". Ultimately, the largest and most successful social systems outgrow simple language expressions and develop their own sphere or "medium" of communication. This would seem to have particular resonance for cyberspace which in effect has become its own medium.

Social systems form part of society as we experience it and are both influential upon and influenced by their surrounding social systems. However, they can also be said to

---

[43] M Gillen, "Law 2.0, Web 2.0, Why Not Legal Sociology 2.0?" *Papers of the BILETA Conference 2008* available at http://www.bileta.ac.uk/Document%20Library/1/Law%202.0,%20Web%202.0,%20Why%20Not%20Legal%20Sociology%202.0%20%5BMartina%20Gillen%5D.pdf (accessed 20 July 2012).

[44] F Varela, H Maturana and R Uribe, "Autopoiesis: The Organization of Living Systems, Its Characterization and a Model" (1974) 5 *Biosystems* 187-196.

[45] N Luhmann "The Autopoiesis of Social Systems" in: F Geyer and J van der Zouwen (eds), *Sociocybernetic Paradoxes* (London & Beverly Hills, CA: Sage, 1986) 172-192.

be independent from the latter since they depend upon their own code and media for interpreting (or perhaps more correctly creating) their own environments and their own organs. Thus, what we commonly call society is made up of open yet also discrete social systems. This discreteness is often described as meaning that the system is operationally closed; in other words: that the "realness" of anything within the system depends on its absorption or adherence to the code of that system. This is a very important distinction. Luhmann himself highlights it:

> I think that the theory of autopoiesis and the theory of autopoietic systems...are underestimated in the radicalism of this approach. This radicalism goes back to the hypothesis of operational closure. This hypothesis implies a radical shift in epistemology, and also the ontology it supposes. If one accepts it and also relates it to the concept of autopoiesis and treats the latter as a further formulation of operational closure, then it is clear that it also breaks with the epistemology of the ontological tradition that assumed that something of the environment enters the understanding and that the environment is represented, mirrored and imitated or simulated within a cognizing system. In this respect the radicalism of the new approach can hardly be underestimated.[46]

3.2 Autopoiesis and law/cyberspace

Andrew Murray's work is outstanding in the field of autopoiesis and cyberspace. In "The Regulation of Cyberspace: Control in the Online Environment"[47] Murray espouses a process he dubs symbiotic regulation. Symbiotic regulation works by utilising feedback. At the heart of the concept is the observation that there are stable patterns of communication in the systems that can be mapped. Note it is the pattern or dynamic trend of communications that is to be analysed, not every individual communication. A simple analogy would be that the process is like modelling the dynamics of a school of fish rather than studying the biology and psychology of individual fish.

Once the communications patterns between the nodes (i.e. users on the network) are identified then we can create a regulatory matrix, a multidimensional map of the intersections between the law and cyberspace closed systems. Murray identifies these intersections as one of the key features of networked communications. This feature gives rise to his vision of cyber-regulation. He proposes regulation designed to take advantage of those intersections to perform regulatory interventions, which will ripple through into the otherwise closed system. The idea is that because the communications trends within each system are already known then the regulator can design the intervention to have the desired output building upon the system's own internal structures. Of course these are highly complex systems and so sometimes unpredicted or even unpredictable outcomes may occur. However, the feedback process of observing the effects and tweaking the interventions should ultimately lead

---

[46] *Ibid,* 114.

[47] A Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Oxford: Routledge-Cavendish 2007).

to a system where the regulation and the system (in our case cyberspace) are so in tune with each other, and the understanding of the communications patterns so well mapped and understood, that the interventions cease to be trial and error but become truly symbiotic. Symbiotic in this case means that the regulations will be perfectly tailored to the regulatory environment and vice versa. Murray is confident that computer mapping of system dynamics would enable this to occur:

> The three-dimensional regulatory matrix...allows us to imagine the structure of nodal or decentralised regulation in the complex, multi-layered, new media environment…When this model is paired with Mingers' representation of autopoietic communication...it allows regulators to chart the communications flow within the regulatory matrix, enabling the construction of a 'first order model' of communication within the regulatory matrix. This first order model forms the foundation for an initial intervention and a series of dynamic feedback loops, where the results of every intervention are measured against the responses from each regulatory node, allowing for the fine-tuning of the intervention and creating ultimately robust, symbiotic regulation...[48]

Of course, the degree of uncertainty inherent in the initial stages of this tweaking process is challenging to regulators. Murray views this as the major stumbling block to the adoption of such a regulatory model. Nevertheless, he also urges regulators to embrace the uncertainty and recognise that acknowledging the limits of their own current knowledge is the only way to advance. The current author agrees with Murray's analysis, but would like to suggest that perhaps he underplays, or is too timid in asserting the full effects of this feedback process. Part of the reason for this may be that, as Svantesson noted (see quotation above) too much attention is being paid to the idea that using legal norms is a given, and their goals and objectives should be applied to the regulatory system. To give an example from Murray's work let us consider the following:

> Thus Action 1, causes a set of results and resultant feedback, for example adding DRMs to digital media files causes consumer disquiet and a rise in the activity of crackers. As a result the regulator considers this and makes a second intervention, Action 2. This may be attempts to legally control the activity of crackers though legislation such as the Digital Millennium Copyright Act or the Directive on Copyright and Related rights in the Information Society. The effect of this may be to cause a shift in focus from cracking to sharing through file sharing technologies, leading to a third order intervention in file sharing communities and so on.... It, like the regulatory environment, should be dynamically modelled over a period of months, or even years, with each new intervention being designed specifically with regard to the feedback received at

[48] *Ibid,* 257.

each point of intervention.[49]

Murray clearly sees that the regulations might have to be tweaked, or varied, to achieve consensus, and the required goals. However, surely to achieve a true symbiotic relationship laws (and lawyers) must be open to having their goals challenged by the feedback process as well?

Of course, if taken at face value this seems to be paradoxical. How can an operationally closed system like law, respond to the needs and goals of the systems it seeks to regulate without losing its own internal cohesion, and therefore ceasing to be autopoietic? Thus, law would not seem to be amenable to autopoietic explanation. At the very least, one would be limited to the regulatory interventions approach, adopted by Murray, where only a portion of the code of the system could be influenced not its program nor its efficiency. This however, fails to fully take into account the true impact of autopoietic theory on cyberspace and law.

Two major solutions may be drawn out from existing work and applied to this problem. The first is to identify multiple autopoietic legal systems: rather than profess the unity of law (or the monolithic nature of cyberspace), it is seen as part of the autopoietic process that the systems reproduce in a plural fashion within the context of the "local logic" for the legal doctrine.[50] This approach allows for cultural diversity, and a proliferation of legal regimes, to be seen as manifestations rather then refutations of the autopoietic thesis. The second solution (primarily espoused by Gunther Teubner)[51] is to take this pluralism, and add it to Habermasian ideas of recursive discourse (where the citizen and the state interact in a reinvigorated public sphere to shape the role of the state, the role of the citizen and the boundaries of the public sphere itself).[52] The immediate consequence of this is that it becomes plain that systems are closed (and in that sense autopoietic) to varying degrees; this would seem to once again, severely challenge the concept of law as an autopoietic system.

However, Teubner has a further enhancement of the autopoietic thesis which resolves this issue. That is, the idea of inter-systemic collision law i.e. that the autopoietic systems set their own rules for how they interact with the less autopoietic systems (the partially autonomous and socially diffuse systems) and, also, how those other systems interact with each other inside law's domain. For example law dictates how citizens and state interact together in the public sphere and thus even how that sphere is defined. These rules can be seen to operate between and among various social sub-systems, between state law and other quasi-legal orders and finally in conflicts within law.[53] In relation to cyberspace this would again account for observable trends, like

---

[49] A Murray, "Regulating the Post-Regulatory Cyber-State" available online at http://works.bepress.com/andrew_murray/7/, at 23-24.

[50] K Ladeur, "Perspektiven einer post-modernen Rechtstheorie: Zur Auseinandersetzung mit N. Luhmanns Konzept der 'Einheit des Rechtssystems" (1985) 16 *Rechtstheorie* 383-427, at 426.

[51] G Teubner *Law as an Autopoietic System* (Oxford: Blackwell, 1993).

[52] J Habermas, *The Structural Transformation of the Public Sphere* (Cambridge, MA: MIT Press, 1989).

[53] See Note 50 above, at 100-122.

local responses to specific laws for example, without destroying the possibility of viewing cyberspace as an autopoietic system. Response to the law could be viewed as openness at a secondary level whilst the core activities of interaction would still otherwise be closed and controlled.

Thus, autopoiesis offers a theory of law which recognises that there can be a range of legal systems and quasi-systems interacting (communicating) together and that law can and should be responsive to these without losing its internal consistency and autonomy. The corollary of this is that the observation of these interactions can outline the nature of the law. If autopoiesis can be applied to something as diverse and complex as law which has these parallels with cyberspace then it can be applied to cyberspace itself. Such an application of theory may ultimately serve to close the gap between law and cyberspace. Murray's regulatory methods could be saved and indeed enhanced by being truly open to the feedback process which would allow them to be applied toward well designed goals suitable for the cyberspace medium.

4. Conclusion

This article has focused on the mismatch between law and cyberspace and suggested that close observation of user behaviour within an autopoietic theoretical framework may offer a solution to our current theoretical impasse. The reasons for this are compelling. Autopoiesis is a theory which focuses on communication and language media which makes it ideal for exploring cyberspace, a space created not by geological phenomena but the exchange of data. Furthermore, autopoiesis permits cyberspace to be viewed as an entity in its own right (rather than as a mere subject of any other social phenomenon, in particular law) yet, allows us to account for the localised social reality, that other factors, including law, and technology, can affect its development. Finally, Murray's methods offer a concrete path to the application of law to cyberspace, in the form of effective regulation. However, we must build on them to consider the nature of our regulatory goals as well as our regulatory methods, if this potential is to be fulfilled.

Of course, this is only a beginning. The work identifying the language and medium of cyberspace must take place in order for this model to become a functional regulatory tool. This theory offers the chance for us to view and analyse the debate in a different way, a way which eschews methods and viewpoints we already know to be flawed. Thus, perhaps the gap between law and cyberspace will cease to be infinite and unbridgeable. Users and regulators might once again build and explore cyberspace with the joy and hope of a child seeing their first circus elephant.