London School of Economics and Political Science

From the SelectedWorks of Professor Andrew D Murray

Fall 2011

Nodes and Gravity in Virtual Space

Andrew D Murray, London School of Economics and Political Science

Available at: https://works.bepress.com/andrew_murray/10/
Nodes and Gravity in Virtual Space

Andrew D. Murray

Abstract

In 1996 John Perry Barlow made his now infamous Declaration of Independence for Cyberspace. In this the cyberlibertarian ethos was laid out: “We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.”

Since that date much has changed. The work of a number of US cyberpaternalist philosophers such as Jonathan Zittrain, Jack Goldsmith, Joel Reidenberg, Yochai Benkler and most famously Lawrence Lessig has illustrated the fundamental weaknesses in Barlow’s (and therefore cyberlibertarianism’s) basic premises. This does not mean though that because one can be controlled in cyberspace, one ought to be controlled or even one will be controlled. The distinction is between the ability to control and the effectiveness and legitimacy of control mechanisms. It is this distinction which is at the heart of network communitarianism and which is likely to come more to the fore as the network is replaced with the cloud, always on data, augmented reality and mobile data communications. The key issue for regulators now is the strength of the network and the ability of regulators to control within the network.

Building upon previous regulatory designs of the author and taking account of nodal governance theory as developed by Clifford Shearing and Julia Black, this paper aims to demonstrate that the key to building effective and legitimate regulation in the virtual space is to recognise and harness key nodal connections and key nodes themselves. It will demonstrate how the cybercommunity functions as both a community and a group of individual nodes and will seek to develop a theory of regulatory gravity in which the relative communicative power of various nodes may be modelled to take account of the effectiveness and legitimacy of a regulatory intervention.
Nodes and Gravity in Virtual Space

Andrew D. Murray*

A. Introduction: Space and Cyberspace

At first glance it appears the regulatory challenge of cyberspace is to be found in the geography of the place, or rather in its lack of geography. Continually journalists, lawyers and lawmakers examine individual case studies which seem to prove or disprove the thesis that direct regulatory action can be effective in cyberspace. Recent examples of such proof/disproof include the WikiLeaks Cablegate affair (Benkler, 2011), the related, but pre-existing, “Anonymous” campaign of online civil disobedience (Legal Piracy, 2011) and Operation Rescue (McVeigh, 2011). Whether you believe in the efficacy of direct regulation of online activity or not colours which examples you choose to establish your case.

Looking at individual case studies though obscures the wider view. The micro view and the macro view are very different. The success of Operation Rescue is due to the extensive resources made available by an international group of law enforcement bodies in an area where there is widespread international co-operation; the availability of agreed international standards, (Convention on Cybercrime, Art.9) and widespread public support for the activities of the law enforcement community. Similarly what is perceived as a failure to curb the WikiLeaks cables may not be in fact true, or if true is not a function of the structure of WikiLeaks. Although the US Federal Government has made extensive public attempts to appear to “close down” the flow of leaked US Embassy Cables, the documents themselves are relatively benign and mostly refer to activities of the previous Republican administration. Politically the strongest voices against WikiLeaks in the United States are of the Republican right, not the Democratic administration. In a BBC interview of 29 November 2010, Mark Stephens, a senior member of Julian Assange’s legal team made reference to the fact that the US Federal Government were offered the opportunity to specifically review the cables before release to indicate where US citizens or employees may be put at risk, a fact he reiterated at a British Institute of International and Comparative Law event on WikiLeaks.

* Professor of Law, London School of Economics and Political Science.
on 31 January 2011 in some greater detail where he explained that the US Federal Government were offered access to the full database of cables before their release to ensure no operation, citizen or employee were put at risk. According to Stephens two cables were removed from the dataset by WikiLeaks at the request of officials and a (very) few others were further redacted.\(^1\) Thus it may be said that the reaction of the US Federal Government to the Cablegate affair is a son et lumière performance of a Democratic administration designed to reply to and appease Republican commentators. In other words it is politics not a failure of regulation and governance. In the event that this interpretation is false and that the US Federal Government did in fact lose control of the data in a way which meant they feared genuine harm may be caused by WikiLeaks’ revelations, what does this mean for those of us interested in cyber-governance and regulation? Well nothing really. WikiLeaks is a drop box, nothing more. The failure to stem the flow of data from WikiLeaks, or to trace its source, is not due to the specific nature of the WikiLeaks structure. The disaffected employee (who may or may not be PFC Bradley Manning) could have downloaded the data to a dozen DVDs or data cards and then simply dropped them in the mail to any number of international media outlets including El País, Le Monde, Der Spiegel, The Guardian and The New York Times. Thus WikiLeaks is not a case study in the unregulability of cyberspace; rather it is a case study in globalisation of the media. These examples demonstrate that looking at the micro case study is unlikely to explain the macro position.

Cyber-governance theorists have therefore tended to focus on macro questions of geography and establishment. In this they follow a long established line of inquiry which places the design of the environment centre stage in regulatory/governance discourse. It has its foundations in Bentham’s Panopticon prison, (Bentham 1995: 29-95) and now is rooted in the works of Michel Foucault (Foucault 1977: 195-231) and Clifford Shearing who explains in great detail how town centres and theme parks are designed as tools of control of movement and activity (Shearing and Stenning 1985). Over the years, and developing these themes, cyber-governance theorists have developed a number of alternate models for cyber-governance and regulation each

\(^1\) The BBC interview may be streamed from [http://www.bbc.co.uk/news/world-us-canada-11866342](http://www.bbc.co.uk/news/world-us-canada-11866342). Unfortunately there is no recording of the BIICL event although the author was present and heard the detailed comments.
focussed upon a particular aspect of internet geography, and each following the predominant social theories of cyber-culture at the time.

1. Cyberlibertarianism

The first movement was the Cyberlibertarian School whose development mirrors the spirit of the open network era of the 1980s and early-mid 1990s, sometime called the “wild west” era of the internet. This school focussed upon the virtual geography of the internet. It suggested that the nature of the internet as a non-geographical space with no regard for traditional borders or boundaries and with its unique micro community structure was a place unsuitable to traditional forms of regulation (Johnson and Post 1996: 1370-8). It found powerful voices in social activists such as John Perry Barlow, (Barlow 1996) and legal commentators such as David Johnson and David Post. Cyberlibertarians believed that with no single Realspace government in a position to legitimately exert control over all the citizens of cyberspace; and with no possibility of Realspace governments targeting only their citizens in cyberspace due to the geography of the place as one which does not lie within physical borders, any form of external intervention by Realspace governments would be illegitimate. They further believed that Realspace governments had no de facto ability to control the actions of individuals within cyberspace due to the borderless nature of the environment.

This assumption was at the heart of the Cyberlibertarian School. It was premised upon the thesis that territorial borders delineate the effective boundaries of legal enforcement procedures. Thus if a citizen of the United Kingdom carries out an illegal act, such as the offering for sale of obscene material within the UK he may expect enforcement through the UK criminal justice system: to be investigated by UK police officers and prosecuted before the UK courts before being fined or imprisoned in a UK prison. If that same citizen was to carry on his activity in France the UK criminal justice system would have no say over investigation and prosecution of his actions: it would be within the purview of the French criminal justice system. The Cyberlibertarian School believed that as cyberspace “floated above Realspace” and did not respect Realspace borders, laws passed by states-regulators, sovereign only within their own borders, must fail. For cyberlibertarians therefore only self-regulation which drew upon the will
of the governed could be effective because the geography of the place meant that individuals could *de facto* avoid the will of the regulatory body or state by relocating content and activity elsewhere and in any event the *de lege* right of the regulatory body or state was in question due to a lack of legitimacy to govern across borders. Thus the Cyberlibertarian School based their assumptions of freedom from external systems of governance and control upon their interpretation of the geography of cyberspace. However a movement quickly grew which took a radically different view of cyberspace geography.

2. Cyberpaternalism

This movement has many names but is most often referred to as cyberpaternalism as it grew from a belief that an unregulated cyberspace is inherently undesirable as left unchecked harmful activities will be allowed to flourish in pockets within cyberspace; activities such as unregulated access to indecent and obscene materials, identity theft, virus seeding, fraud, bullying, child abuse (via image trading) and potentially, terrorist activity. The Cyberpaternalist School has two distinct sub-schools, both of which are equally critical of the cyberlibertarian view that the geography of cyberspace protects the liberty of its citizens from external regulation.

The first of these schools is the Cyber-realism or “internet fallacy” School. This has a number of powerful proponents including most famously Jack Goldsmith, (Goldsmith 1998) but also Tim Wu (Wu 1999) and from the UK Chris Reed (Reed 2004). These realists noted that the internet was no more global than any number of other areas in which international co-operation ensures the rule of law. They cite successes in regulating international trade; in aviation law, the law of the sea and in environmental law. They also note the success of international criminal law in dealing with everything from wire fraud to international trafficking of drugs. As Goldsmith notes “changes in transportation, communication, and in the scope of corporate activity led to an unprecedented increase in multijurisdictional activity. These changes put pressure on the rigid territorialist conception, which purported to identify a single legitimate governing law for transborder activity based on discrete territorial contacts” (Goldsmith 1998: 1206-7). Despite those challenges we do not say that law cannot
regulate interstate trade or the multi-state activities of multinational companies. These are all questions of taking effective jurisdiction, not a challenge to either the de facto controls or de lege legitimacy of the states involved. As noted by Chris Reed the cyberlibertarians had made an error in assumption, the so called “cyberspace fallacy”:

The cyberspace fallacy states that the Internet is a new jurisdiction, in which none of the existing rules and regulations apply. This jurisdiction has no physical existence; it is a virtual space which expands and contracts as the different networks and computers, which collectively make up the Internet, connect to and disconnect from each other. The geographical locations where activities occur are often purely fortuitous, dictated by the then current configuration of the Internet. The worldwide accessibility of the Internet means that no one legal jurisdiction has de jure or de facto control of these activities. From all this, it is concluded that no jurisdiction has any control.

A moment’s thought reveals the fallacy. All the actors involved in an Internet transaction have a real-world existence, and are located in one or more legal jurisdictions. The computing and communications equipment through which the transaction takes place is also located in legal jurisdictions, even though it may be difficult to identify precisely which equipment was in fact used. It is inconceivable that a real-world jurisdiction would deny that its laws potentially applied to the transaction. In fact, because the Internet is accessible from almost everywhere in the world, transactions whose real-world analogues would have been restricted to only one or two jurisdictions may potentially be subject to every jurisdiction – this is particularly clear in the case of advertising via a Web site. It may be that the Internet, rather than being unregulated, is in fact the most heavily regulated ‘place’ in the world (Reed 2004: 1-2).

This movement quickly gained support. In essence it turned the freedom enhancing view of cyberspace geography, as preferred by cyberlibertarians, on its head. Now instead of seeing cyberspace as a place free from external interference and control it was a place of multiple overlapping jurisdictions. The question no longer was could an individual state
or regulator take effective regulatory control over an area or activity on cyberspace but ought it to do so? The legitimacy question remains on the table; the ability to control is no longer in doubt.

The second sub-school of the cyberpaternalist movement is the Techno-determinism, or Berkman School (Mayer-Schönberger 2008). This school is named for the Harvard research centre around which most of its proponents have developed networks. Its most famous proponent is Lawrence Lessig, but its origins are in a paper by Joel Reidenberg. In his 1998 paper *Lex Informatica: The Formulation of Information Policy Rules Through Technology* (Reidenberg 1998) Reidenberg provided the link between the earlier Cyberrealism School and the later Berkman School. Reidenberg realised that a functional example of international law without state may be found in the *Lex Mercatoria*. Here several hundred years ago international traders from a variety of states developed a common set of rules which came to govern interstate trade throughout Europe for hundreds of years. It worked because all parties agreed to be bound by it. Reidenberg noted that a similar body of soft law may be developed with regard to the internet. He called this new body of law *Lex Informatica* but vitally made a bridge between the Cyberrealism and Berkmanism. He realised that as *Lex Mercatoria* was the primary legal construct for medieval merchants so *Lex Informatica* not *Lex Fori* would be the effective primary legal framework for the online activities of individuals (Reidenberg 1998: 565-75). The question was how would *Lex Informatica* be enforced in an environment which, as the cyberlibertarians had already demonstrated, resisted the application of external control mechanisms? Here Reidenberg was influenced by Lawrence Lessig’s groundbreaking 1996 article *Reading the Constitution in Cyberspace* (Lessig 1996). In this Lessig had argued that software codes were a form of constraint on action, an idea he developed subsequently into his “code is law” thesis in his 1999 article *The Law of the Horse: What Cyberlaw Might Teach* (Lessig 1999). This thesis forms the heart of the Berkman School as now followed not only by Lawrence Lessig and Joel Reidenberg but by many others such as Jonathan Zittrain (Zittrain 2009) and Yochai Benkler (Benkler 2000a).

Essentially the Berkman School sees control affected by changes made to the geography of the place. In a return to Bentham’s Panopticon, Lessig argues that changes made to
the underlying code of internet communications technologies control our every online act (Lessig 2006: 120-38). A simple question of regulation may be “do we want to allow people to view flash content or not?” This is a question at the heart of Apple policy in recent years and, as discussed by Jonathan Zittrain, as the hardware provider Apple gets to choose whether I can play flash games on my iPad by “tweaking” the code of the operating system (Zittrain 2009: 1-5). More complex questions though may be asked and answered through code. Do we allow people to post anonymously or pseudonymously? Do we allow people from foreign jurisdictions to access our content? Do we block access from “unsecure” sites? etc. As Lessig notes “Cyberspace demands a new understanding of how regulation works. It compels us to look beyond the traditional lawyer’s scope—beyond laws, or even norms. It requires a broader account of ‘regulation,’ and most importantly, the recognition of a newly salient regulator. That regulator is [ ] Code. In real space, we recognize how laws regulate—through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different ‘code’ regulates—how the software and hardware (i.e., the ‘code’ of cyberspace) that make cyberspace what it is also regulate cyberspace as it is” (Lessig 2006: 5). For Lessig the two key components of code-based regulation are: (1) it is always designed by a code designer or engineer (unlike the environment of the real world there is no pre-existing geography in cyberspace) (Lessig 2006: 6); and (2) the development of code can be captured by external bodies or groups, including vitally real world regulators such as states.²

3. Space and Cyberspace: Geography and Cyber-governance

The commonality in all these approaches is in the assumption that the geography of the cyberspace environment is analogous with the physical geography of Realspace. The power of Lessig’s “code is law” argument is in the parallels that may be drawn with design-based regulation in Realspace. How much more effective is it to bar access to a property rather than putting up a sign saying access is prohibited under law? Design based control mechanisms are extremely powerful as they act ex ante rather than ex post and they are self executing rather than demanding the attention and interaction of others (Murray and Scott 2002). To give but one example: imagine a book reseller wants

² See Lessig’s discussion of the “Regulatory Two Step” at (Lessig 2006, 62-80). See also (Brownsword 2005).
to sell digital copies of their book via an eReader device and they want to ensure the book cannot be traded on to other users of similar devices to prevent market erosion. They may either use law: to make a copy of the work will infringe copyright, so a license condition which says the end user may not copy, forward or transmit their copy of the book to another will be effective. But if the end user chooses to ignore the license the economic harm occurs before the effect of the law is felt. The license holder will have to spend considerable sums and time tracking down the offender, identifying the correct legal forum for the case and then presenting a case in damages before anything can be recovered. During this time they remain economically disadvantaged and open to further harm should the infringing copy continue to circulate. Now imagine instead the licensor electronically locks their copy with a hardware lock which says that only the eReader which is licensed to open this file may open it. If the licensee transfers the file it will not function and no economic harm will be done. The control is now *ex ante* and completely automatic. Why you may be asking is this not everyday then? Why is the does the music industry still fear economic ruin due to file sharing? (Sweney 2011) Why is the TV and Movie industry now claiming similar harm? (THR Staff 2011) Surely if the Berkman School is right design controls can be effected which would prevent this? Some, such as Zittrain (Zittrain 2009: 101-27), may point to the effectiveness of the Apple environment which does have such levels of control to show this may be effective. But why is the internet at large not so controlled? It is because the Berkman School, like the Cyberlibertarian School before it, has a major weakness. The cyberspace environment is not analogous with the physical environment of real space. It is a place not only of geography and structure; it is also a place of communication and discourse.

B. Communities and Discourse

In his original “code is law” model Lessig imagined a discursive dialogue between the regulator and the regulatee. This is the common model found in much regulatory theory including regulatory cybernetics (Hood et al 2001: 23). The dialogue usually goes something like this: (1) What is the behaviour we wish to control, encourage or discourage (standard setting); (2) How can we ensure the regulatee respects our position on this (detecting variation) and (3) How can we communicate to the regulatee that they need to modify behaviour (effecting a return to the norm). We can see in
examples of such dialogues from criminal law: (1) we wish to prevent excess speed as it may cause harm to pedestrians and other road users so we make speed limits; (2) we will install clear signage, use police patrols and speed cameras; (3) those caught speeding will be fined or banned from driving; and from tax law (1) we wish to ensure that citizens pay their income tax so we will set laws outlining the levels of taxation payable; (2) we will periodically audit citizens to ensure they are paying the correct tax; (3) those not paying the correct tax will be fined or surcharged.

Dialogue is at the root of regulatory cybernetics: “any control system in art or nature must by definition contain a minimum of the three components ... There must be some capacity for standard-setting, to allow a distinction to be made between more or less preferred states of the system. There must also be some capacity for information-gathering or monitoring to produce knowledge about current or changing states of the system. On top of that must be some capacity for behaviour-modification to change the state of the system” (Hood et al 2001: 23). This is a bipartite or dialogue model between the regulator and the regulatee. In Lessig’s model it becomes apparent when he talks of a pathetic dot: “That someone regulated is represented by this (pathetic) dot—a creature (you or me) subject to different regulations that might have the effect of constraining (or as we’ll see, enabling) the dot’s behavior” (Lessig 2006: 122). For Lessig the singular dot represents the regulatee, the regulator(s) are represented by his four constraints on action – Law, Norms, Markets and Architecture. This though is a simple restatement of the now outdated cybernetic model. A much newer and dynamic regulatory model is seen in the Nodal Governance models used by, among others Clifford Shearing (Shearing and Wood 2003; Burris et al 2005) and Julia Black (Black 2001). This model does not imagine that the individual is isolated within a fixed environment. Instead it accounts for the dynamics of communication within the community which inhabits the environment; it draws upon a number of models including Habermas’s model of communicative power (Habermas 1998), or Luhmann’s social systems (Luhmann 2004) depending upon the subject matter being modelled.

1. Network Communitarianism
This movement from fixed geographical considerations to communicative theories gave rise to a newer, more dynamic model of cyber-governance. This model has become known as network communitarianism. It answers those difficult questions that cyberpaternalism in general and the Berkman School in particular has found difficult to answer, such as if network engineers can design code controls which permit or restrict freedoms in the digital environment, why is the music industry still claiming the potential for economic ruin due to file sharing? The answer from network communitarianism is that it is because the individual is not isolated: he is not Lessig’s pathetic dot rather he is a Habermasian opinion former, a member of a community of dots who give (or remove) legitimacy from external regulatory actions. If the external imposition of a control system is seen to be over-regulatory the “dots” will communicate this and when a critical mass of dots (negative responses) is achieved civil disobedience follows. The regulatory controls are removed (often illegally) and materials are distributed in breach of legal principles. The law then faces a challenge: does it seek to enforce the rule of law against what may actually be a majority of the community?3 And if it does so is that law still actually legitimate?

I have put forward one model of network communitarianism (Murray 2007). I label this “active matrix theory” and it is designed to assist regulators in mapping when external regulatory interventions are likely to be effective, though unfortunately not when they are likely to be legitimate: for that one must refer to traditional models of jurisprudential thought. The active matrix model may be found in The Regulation of Cyberspace (Murray 2007: 22-54; 233-51). There I re-examine the Berkman School’s “code is law” model and find that in applying the principles of actor-network theory (ANT) and social science theory (SST) we can consider the dot rather differently. The dot is in ANT terms a material node in the network, while in SST terms it is part of a system. In either term the dot is not isolated: it forms part of a matrix of dots. To put it another way the dot, which is designed to represent the individual, must always be considered to be part of the wider community and it is here that traditional cybernetic/code theory runs into difficulty, for when one examines the modalities of regulation proposed by

---

3 In 2010 the British Phonographic Institute estimated that 1.2 billion tracks were illegally downloaded in the UK. This suggests three-quarters of all music downloaded in the UK was illegally obtained in 2010 (Cheng 2010).
Lessig we find that of the four, three of them, Laws, Norms and Markets are in fact a proxy for community-based control. Laws are passed by lawmakers elected by the community; markets are merely a reflection of value, demand, supply and scarcity as reflected by the community in monetary terms and norms are merely the codification of community values. I therefore term these “socially mediated modalities”, reflecting an active role for the dot in the regulatory process. Far from being a “pathetic dot” which is the subject of external regulatory forces the dot is in fact an “active dot” taking part in the regulatory process (Murray 2007: 233-51).

There are two key distinctions between the classic cybernetic/code model and the new active matrix model. The first is to replace the isolated pathetic dot with a networked community (or matrix) of dots which share ideas, beliefs, ideals and opinions (Figure 1). The second is to recognize that the socially mediated modalities of law, norms and markets draw their legitimacy from the community (or matrix of dots) meaning the regulatory process is in nature a dialogue not an externally imposed set of constraints (Figure 2).

Figure 1 - From the Pathetic Dot to the Active Matrix
What does this mean for our understanding of internet regulation? Firstly it suggests that regulation in the online environment is little different to regulation in the real world, and is based on finding threads of communicative power rather than based on geography and environment. Regulation is a process of discourse and dialogue between the individual and society. Sometimes society, either directly through the application of norms, or indirectly by distilling its opinions, norms, or standards down to laws wishes to force a change in behaviour of the individual. But, sometimes it is the regulatory settlement itself which is challenged by society when there is no longer any support for it. This is most clearly illustrated by the fact that the UK enforcement authorities have declined to prosecute individuals under either the Customs Consolidation Act 1876 or the Obscene Publications Act 1959 for privately viewing obscene material using an internet connection. We, the community of dots, have collectively decided that the viewing of pornography by internet connection is no longer to be viewed as morally objectionable and have communicated this decision by both driving the market for

Figure 2: The Network Communitarian Regulatory Discourse
material of this type and by communicating to our lawmakers where a line is to be drawn. We wish to sanction and criminalise those who possess or trade in images of child pornography (including pseudo images) and those who possess or trade in images of sexual violence, harm, bestiality, and necrophilia. Thus the regulatory settlement is not imposed upon us, if it were we would all avoid the viewing of obscene material for fear of prosecution under the Obscene Publications Acts, but is rather part of a dialogue in which the regulatory settlement evolves to reflect changes in society.4

2. Communitarianism and Legitimacy
It surely cannot be true that the general will of the people, lacking the imprimatur of legitimacy that is to be found in legislative assembly, can simply decide which laws are “valid” and which are not. The danger of the active matrix theory is that it comes perilously close to suggesting mob rule for cyberspace. In my defence it should be said that, as previously noted, it is not the aim of the active matrix model to decide the legitimacy or otherwise of the outcome of a regulatory discourse, it is merely a model of regulatory discourse intended to improve the efficacy of regulatory interventions. Equally it never was my intent to suggest, in the style of cyberlibertarianism, that the will of the community overcomes the will of the legitimate external regulator. Rather it was about modelling responses to regulatory interventions in an attempt to model the high rate of regulatory failure in cyberspace. Yet it is conceded that it could be seen as a model which suggests the community possesses regulatory power equal to or greater than that of traditional and clearly legitimate regulators. In the second half of this paper I will attempt to remove some of these weaknesses in the original model by examining changes in the tools used by external regulators to attempt to control online behaviour in the intervening years and introducing a newer, more refined model of network communitarianism: regulatory gravity theory.

C. Gatekeepers and Control
The model of control used by external regulators has changed in recent years. Around the time I wrote The Regulation of Cyberspace the dominant model reflected the theories of the Berkman School. Code based controls were primarily used. Primary among these

4 In this final analysis network communitarianism in the internet regulation context shares core values with decentred regulation in mainstream regulatory theory. See (Black 2001) and (Scott 2004).
were blocking and filtering tools designed to ensure certain content was unavailable to end users (Diebert et al 2008). A prime example of such a technique is the activity of the Internet Watch Foundation (IWF). The IWF is an industry body based in the United Kingdom. Nearly all UK ISPs are members of the IWF and it is supported by a number of industry partners such as Yahoo! and Microsoft. It is also financially supported by the UK Government and the European Union. In 2006 the UK Government made a veiled threat to ISPs who did not apply IWF filtering tools, designed to block access to sites containing child abuse images or content in breach of the UK Public Order Act (material inciting racial, religious of gender hate). In a Parliamentary Written Answer in May 2006 Home Office Minister Vernon Croaker noted:

Recently, it has become technically feasible for ISPs to block home users’ access to websites irrespective of where in the world they are hosted. It is clear from the various meetings that Ministers have had with the ISPs, that the industry has the will to implement solutions to block these websites. Currently, all the 3G mobile network operators block their mobile customers from accessing these sites and the biggest ISPs (who between them provide over 90 per cent. of domestic broadband connections) are either currently blocking or have plans to by the end of 2006.

We recognise the progress that has been made as a result of the industry’s commitment and investment so far. However, 90 per cent of connections is not enough and we are setting a target that by the end of 2007, all ISPs offering broadband internet connectivity to the UK general public put in place technical measures that prevent their customers accessing websites containing illegal images of child abuse identified by the IWF. For new ISPs or services, we would expect them to put in place measures within nine months of offering the service to the public (Home Office 2006).

The technique he is referring to is a blocking and filtering system called Cleanfeed. A blacklist of sites is made available to ISPs from the IWF. Sites are updated regularly based upon reports from members of the public, investigations of law enforcement bodies and reports from ISPs themselves. All ISPs who use the system agree to block
access to the sites on the register. It is fair to say that the activities of the IWF have been highly controversial; (Laidlaw 2010a) not least because there is no independent oversight of their actions. The IWF is though only one example of the type of code-based control favoured by regulators in the 1990s and 2000s as proxy for direct control. In fact during the period 1998-2008 it seemed that the Berkman School provided the solution for nearly all problems of unregulated cyber-activity. Technical standards were used, among other areas, to set rules on electronic signatures,\(^5\) to protect content from copyright infringement\(^6\) and for the issuance and redemption of e-money.\(^7\) Filtering and blocking in particular was favoured by states globally to block access to any number of content types from criminally obscene content, as found in the UK, to political content, religiously unobservant content and violent content (Diebert et al 2008). But slowly the wheels turned. From around 2008 onwards observance of technical controls has waned. Critiques of the effectiveness of such controls have become more vocal. Recently one of the founders of the IWF, Trefor Davies, Chief Technology Officer and Co-Founder of Timico UK, has questioned its effectiveness:

The Internet Watch Foundation is always cited as a perfect example of how internet blocking can work. The IWF provides ISPs with a list of websites containing illegal child abuse material. These sites are reported to the IWF by general internet users and by ISPs themselves. ISPs then implement blocking techniques (there are various) to prevent their customers from being able to access these sites.

Unfortunately although this sounds great in practice it doesn’t really work. Sure Joe Public is prevented from accidentally accessing such sites but the dedicated sicko can easily find was around the blocking [ED: DNS change, proxy servers, VPN etc]. Just like it will be impossible to block the millions of web pages out there relating to how to use Bit Torrent and other file sharing

---


technologies to download copyrighted material. It is too big a job (Mark 2010).

What Davies is picking up here is the network effect. As predicted by the active matrix model the problem of code-based regulation is that it assumes a static dialogue with a single regulatee whereas in truth there is a discourse between the regulator and a community of multiple regulatees. Code-based controls such as filtering or standards work better when you directly address an isolated individual with few available resources. In fact the situation is rather more fluid than this. Anything built by man may be redesigned or destroyed by man; it only needs the investment of time and resources necessary to do so. Thus any code-based control can be de-tasked through investment by the regulated community in tools designed to overcome the problem. We saw this clearly in relation to DRM technologies. The efforts of DRM designers were overcome by crackers almost as quickly as they could be implemented. More importantly though the community supported the crackers in their efforts by using and distributing their products even though this activity was clearly illegal. This demonstrates that you cannot implement controls in a networked communications-based community without at least the acquiescence of the majority of that community (Murray 2007: 233-51). The problem though is that there is no singular online community. Cyberspace is a collection of millions of micro communities each with their own independent aims, standards and objectives (Murray 2007: 126-64). Among these are communities ordered around anti-social or even illegal activities. These communities feel little or no fealty to the larger more mainstream internet community. This was characterised by Sunstein as the process of internet balkanisation (Sunstein 2007, 138-46), but in fact it is not really about balkanisation more simply that people never felt part of a larger internet community in the first place.

To bring about effective control in such a fragmented collection of communities is extremely challenging. The original active matrix model requires to be amended to take account of the fact that the community is actually multiple overlapping matrices where individual members or nodes have membership of a number of groups. The true (complex) model is therefore as seen in Figure 3 (simplified to 2 dimensions for ease of reproduction).
The key control points in these overlapping networks are the points of commonality (highlighted as the larger macro-nodes). These are connections between communities: the pinch-points of information flow. These macro-nodes may therefore function as gatekeepers of information flow from one area to another. Firstly then who are these gatekeepers? Lately much work on this has been undertaken but some of the best work in identifying and classifying gatekeepers has been undertaken by Emily Laidlaw. In her paper *A Framework for Identifying Internet Information Gatekeepers* she notes that “Internet gatekeepers are those gatekeepers that control the flow of information” (Laidlaw 2010: 266). This though could mean just about anyone, how do we recognise those who fulfil a gatekeeper function and those who do not? Laidlaw goes on to employ Barzilai-Nahon’s Network Gatekeeper Theory (NGT), whose theory as she notes, “helps bring the gatekeeping concept into the networked world” (Laidlaw 2010: 266). This leads Laidlaw to conclude that “pursuant to NGT [] online gatekeeping is the process of controlling information as it moves through a gate, and the gatekeepers are the institutions or individuals that control this process” (Laidlaw 2010: 266). At first glance this may seem to get us no further as it seems to be a closed definition which delimits the group by reference to the activity and *vice versa*. But upon closer inspection we see this is not the case. The activity is clearly definable as separate to the group. The group is therefore definable by reference to the activity. What is clear though is that not all
gatekeepers have the same impact. Some gatekeepers will have little impact on the
general flow of information between communities and networks. Thus what we may call
micro-gatekeepers only impact information flows within communities: these would
include owners of blogs or sites which allow comments, operators of closed intranets
etc. Secondly we have authority gatekeepers; these may affect the flow of information
between networks but may be quite easily avoided by re-routing the information flow.
These would include media outlets such as the BBC or CNN which operate discussion
fora or boards, key informational portals such as Wikipedia and social network sites
such as Facebook. Then there are the macro gatekeepers, these are major controllers of
the flow of information and includes ISPs, search engine providers and governments
(Laidlaw 2010: 269-74).

In recent years governments have come to recognise the immense power of gatekeeper
control in the online environment. You can use it to isolate communities or to block
access altogether. This is most clearly seen in relation to online illegal filesharing
communities. A number of techniques have been tried including the isolation of a
particular community through legal action as has been attempted in relation to The
Pirate Bay in (among other places) Denmark, Germany, Greece and Italy. In each case
local action was taken to attempt to force local ISPs to block access to a single website,
The Pirate Bay. Similarly major search engines have been the subject of external
controls. In early 2010 a dispute between Google and the Chinese government saw
Google very publicly end filtering protocols required by the Chinese State eventually
leading Google to withdraw from the lucrative Chinese market. This story is though only
the tip of the iceberg. In 2008 it was reported that major search engine providers
including Yahoo! and Google were banned in Argentina by a series of court orders from
linking to stories naming up to one hundred famous people including football legend
Diego Maradona (Out Law 2008) more recently it has been reported that access to anti-
Islamic websites has been blocked by the Government of Pakistan (Joshua 2011). More
publicly EU governments are using the gatekeeper proxy power of ISPs to raise a final
attempt to gain control of rampant of online illegal file sharing. In France the Creation
and Internet Law (Loi favorisant la diffusion et la protection de la création sur Internet)
has created a three strikes procedure which may ultimately lead to users having their
account with their ISP suspended for a specified period of between two months to one
year. During the suspension the subscriber is blacklisted and other ISPs are prohibited from providing an internet connection. The service suspension does not, however, interrupt billing, and the offending subscriber is liable to meet any charges or costs resulting from the service termination. The UK has adopted its own three strikes framework in the Digital Economy Act 2010. Although not yet in force, partially due to a Judicial Review challenge of the Act, the Ofcom code once implemented will allow for “technical measures” to be taken against repeat infringers. The framework provision, in the new s.124H of the Communications Act 2003, does not contain the full detail of what technical measures may be employed (we await an order from the Secretary of State) but it is envisaged they may include speed throttling, port blocking and even disconnection in a manner similar to the French Law.

As regulators are likely to rely ever more on gatekeepers as proxies in their attempts to control online activities it means that our old models for cyber-governance and regulation have become outdated. Both branches of cyberpaternalism now look out of date as neither focussed on the information gatekeeper, assuming as they did that geography was the key. Equally the active matrix model which modelled all nodes as equal looks naïve in an environment where certain key players control the information flow. In the final section I propose a development of the active matrix theory which has application to regulatory relationships of communicative power in all areas of life, not just online activities. Due to the key role internet gatekeepers play though it is particularly powerful in that sphere of our activities.

D. Gatekeepers and Gravity

The starting point for this is to return to the root of the subject and ask the question “what is regulation?” This question is not as simple and clear-cut as it seems. Rob Baldwin and Martin Cave explain that although “Regulation is spoken of as if an identifiable and discrete mode of governmental activity, the term regulation has been defined in a number of ways” (Baldwin and Cave 1999: 1-2). Bronwyn Morgan and Karen Yeung note that “regulation is a phenomenon that is notoriously difficult to define with clarity and precision, as its meaning and the scope of its inquiry are unsettled and

---

contested” (Morgan and Yeung 2007: 3). These may seem to suggest that the term “regulation” is an amorphous and variable term applied to any widely derived source of control or direction. In traditional regulatory theory this tends not to be the case. Baldwin and Cave take a narrow approach, suggesting that there are two models of regulatory theory: (1) Philip Selznick’s notion of regulation “as control by a public agency” and (2) the “administrative law” model developed by a body of UK public lawyers in the 1980s and 1990s. Despite being set against each other by Baldwin and Cave both these models share common themes and vitally both define regulation as part of the menu of public law.9 Others such as Hood et al. apply a cybernetics approach (Hood et al 2001: 23). Both traditionally describe a public law centred theory of regulation. In the narrow Baldwin/Cave approach the legitimacy to regulate is rooted in public law theory, in the cybernetics approach the ability to regulate is rooted in capacity: capacity to standard set, capacity to information gather and capacity to modify. These suggest public authority power especially at the primary capacity to standard set. Cyber-regulatory theory has though opened up a new approach to defining the capacity and legitimacy of private regulatory bodies such as internet gatekeepers. Outwith the narrow confines of cyber-regulatory theory a similar development was seen in the twin theories of the post-regulatory state and nodal governance.

The post-regulatory state is a synonym for the transition from direct (or public sphere) regulation (the regulatory state) to indirect regulation (post-regulatory state). Post-regulatory theory is a developing school within mainstream regulatory theory. It was first conceptualised by Julia Black (Black 2001) and grown by others including Colin Scott (Scott 2004) and Adam Crawford (Crawford 2006). The post-regulatory state perspective takes a wider view than that of traditional public law regulatory theory. It recognises that the behaviour of a wider range of actors is relevant to the outcomes of ordering of social and economic life, including government itself and individual actors. The key to this is Colin Scott’s third and fourth characteristic of the post-regulatory state. (3) variety in controllers: within the regulatory state literature state regulatory

---

9 Selznick defines regulation as the “control exercise[d] by a public agency”, while administrative law theory ties regulation to the development of the regulatory state. In a very real sense the term ‘regulation’ is being used as shorthand for public regulatory activity. Thus both see regulation as a narrow, static and closed field of study, valuable for the interpretation of the actions of public bodies and the activities of Governments, but less valuable for those of us taking a wider view.
bodies are accorded a special place. In contrast no special legitimacy or value is placed on attributing control functions to state bodies – government departments, agencies and courts – within post-regulatory state thinking. Standard setting is observed at supranational level through a wide range of general and specific governance institutions such as trade associations trade unions and NGOs, and (4) variety in controleses: the regulatory state literature has traditionally viewed businesses as the key regulatees (Scott 2004).

Black’s concept of the decentred post-regulatory state has been developed in particular by Scott Burris (Burris et al 2007), Clifford Shearing (Shearing and Wood 2003) and Peter Drahos (Drahos 2004). In their excellent and often overlooked joint paper Nodal Governance they attempted to map the complexities of regulatory control systems (and legitimacy of regulatory bodies) by utilising the fast growing meme of nodes of control. Firstly they explain how nodes may organically and quite spontaneously develop outcomes or needs which require regulatory control or intervention.

Take any group of people living in the same place or on some other basis identifying themselves as a group for at least some important purposes. We will refer to this as a ‘collectivity’. The things these people do create outcomes over space and time. These outcomes are not necessarily the result of their intentional activities or of their activities alone. Outcomes are produced by the complex interaction of what people do, how they relate to one another, the institutions, technologies and mentalities they deploy, their biological equipment and the conditions and stimuli from the larger physical and social environment in which they operate. Any given collectivity can be understood to be an ‘outcome generating system’ (OGS). By this we mean that the products of the operation of the collectivity across space and time are not exogenous but organic to the collectivity, reflect the conditions of the OGS, and in turn influence the further development of the system over time. Individual collectivities constitute larger and even more complex systems. A system of collectivities is simply a larger OGS (Burris et al 2005: 37).
The effect of this system is that it produces outcomes: some positive (called goods by the authors), some bad (labelled problems). The system if left unregulated will continue to develop both goods and problems and is also likely to affect other systems with externalities many of which will be undesirable problems. Therefore as the authors note:

Every collectivity faces the task of regulating its outcome generating capacities to produce more goods than problems, and coping with outcomes relevant to it produced by external OGSs. All the people living in a collectivity wish to be satisfied — rich, happy, powerful, virtuous. They work within the boundaries of their understanding and social position to achieve that satisfaction. Their success depends, as Hayek argues, upon the degree to which people making up the OGS have made adaptations individually and in how they collectively manage the OGS that maximizes their ability to tap and coordinate knowledge and capacity disseminated throughout the collectivity. These adaptations take a variety of forms, including institutions, rules, principles, habits, customs, traditions and values. Many of these adaptations can be understood to be within the boundaries of what Bourdieu calls the ‘habitus’, the sense of the ‘rules of the game’ in a social field that both allows individuals to improvise to their advantage within a field and reproduces the rules of the field as they are understood by its inhabitants (Burris et al 2005: 39-40).

These adaptations are regulation. They may take the form of internal self-regulation or externally mediated regulatory settlements where nodes negotiate a regulatory form most acceptable. As the authors note: ‘networks have become important’ (Burris et al 2005: 40).

There are clearly similarities in nodal governance theory, the theory of the post-regulatory state and decentred regulation and both cyberpaternalism and network communitarianism. What each hints at but does not fully address is where the divergent centres of power are to be found. How does a regulatory mass develop which is sufficiently powerful to impose a regulatory solution? And how does a regulator draw
capacity and legitimacy when we are dealing with an almost organic form of regulatory development? It appears therefore that internet gatekeepers are being used to regulate in accordance with the traditional nodal governance model: the harnessing of communicative power by external regulators to achieve a regulatory settlement through the capture of a key gatekeeper as a regulatory proxy. This rather simplistic model though fails to answer the two key questions of authority and legitimacy. Although it may be the case that legitimacy is sometimes devolved from a legitimate public body as occurs under ss.3-14 of the Digital Economy Act 2010 or under Regs.4-8 of the Data Retention (EC Directive) Regulations 2009, often there is no devolved power in effect. The Internet Watch Foundation draws no legitimacy from a public authority or public body; similarly the regulatory actions of Google in filtering search returns are not drawn from a public authority or public good. Why then do these gatekeepers function as (mostly) unchallenged regulators of our online activity?

It may be that they draw capacity and legitimacy from another source. To return to Burris et al’s paper Nodal Governance we see a different form of legitimacy and authority outlined, one closer to cyberlibertarian theory. They suggest legitimacy drawn from within the node or regulated community; this is similar to Johnson & Post’s ‘legitimate, self-regulatory processes’ (Johnson and Post 1996: 1400-1). This form of organic internally formed regulatory settlement is similar to the more recent network communitarian theory of cyber-regulatory theory seen in my own work (Murray 2007) and in the work of Bert-Jaap Koops (Koops 2008) and Serge Gutwirth and Paul De Hert (Gutwirth et al 2008). This imagines a harnessing of network power to arrive at a legitimate and proportionate regulatory settlement. In The Regulation of Cyberspace I suggest that the power of network communication meant that only those regulatory settlements acceptable to a sufficiently large proportion of the online community would be effective for otherwise the ability of the community to influence all three socially mediated modalities: Law, Norms and Markets and to ‘engineer around’ the fourth: Architecture meant that the community was effectively its own regulator. Only regulatory settlements acceptable to the community would bind the community (Murray 2007: 233-51). If I am correct then the power of an illegitimate or abusive gatekeeper would be nullified by the response of the wider community. Legitimacy is drawn from the acquiescence of the community (passive regulation). ISPs which unreasonably filter
content or block access would be bypassed in favour of alternatives. Tied technology providers such as Apple with their iPhone/iPad/iPod holy trinity would be rejected in favour of open source platforms (Zittrain 2009: 101-27), and search engine providers who filter access to content would lose out to open competitors.

In fact though the model again does not seem to fit the reality of what occurs in practice. It is clear the gatekeeper holds a particular position within the regulatory matrix: they are something more than a mere node of equal value with all other nodes. Their position as gatekeeper gives them regulatory capacity (although not legitimacy). Arguably this is the missing link in network communitarian theory: the distinction between capacity and legitimacy. As I have said previously network communitarian theory is a model of capacity, not legitimacy. It models why regulatory interventions succeed or fail, not whether the intervention is legitimate. The final part of the model may be found in Burris et al’s paper. There they note:

All nodes are not created equal. Nodes vary in their accessibility, their efficacy, the other nodes they can influence and how that influence is exerted... The capacity of a node to influence or regulate depends in large part upon its resources — broadly defined to include a wide range of forms of capital in the Bourdieuan sense. A small local NGO, for example, can spend a small amount of money, can use social capital to persuade others to use a technology of problem solving, can give voice to local needs and mobilize local political pressure. By contrast, an industry trade association can mobilize a large number of firms and related trade groups, spend large amounts of money and use threats of economic coercion to achieve its regulatory goals. Likewise, mentalities and technologies may vary in their generative potency (Burris et al 2005: 39).

This connects both network communitarian theory and gatekeeper theory. If not all nodes are of equal size then they will exert differing gravitation force on the surrounding regulatory environment. Nodes within a plane exert forces upon each other and these forces are relative to what one may term the regulatory weight of each node. Major nodes such as states and public authorities are of considerable weight and exert a
considerable gravitational pull on any regulatory discourse and its settlement. Other players such as multinational corporations, civil society organisations or regional governments exert considerable but smaller force. Eventually in any regulatory discourse one arrives at the individual. The individual is of almost no weight or force but is extensive in numbers. To determine whether a regulatory settlement is effective or fails does not, as suggested by the unmodified network communitarian theory, turn upon the numbers of individual nodes who accept or reject that settlement but rather on a more complicated calculation of which camp carries the most regulatory gravity. Therefore a large and vocal campaign against the Digital Economy Bill failed as the combined weight and force of those ranged against the Bill was less than those combined in support including major multinational corporations, international NGOs and most importantly the Government. In the DRM example used by myself a lack of popular support for DRMs by governments and a strong community movement against their use was enough to swing the weight in favour of the campaigners. Thus to return to my model: network communitarianism does function as a model for regulatory discourse but the dots of equal size and weight must be replaced with a modified model to reflect the gravitational force exuded by the more powerful dots. This is seen in figure 4.

Figure 4 shows merely in relief the relative weight of the nodes which I originally mapped as being of equal weight. It is not intended to capture the complexity of the communication taking place in the regulatory matrix.\(^\text{10}\) Node A represents a node of extreme gravitational force for example a statutory regulator such as Ofcom. Nodes B

\(^{10}\) For which see (Murray 2007: 233-57).
represent major industry or NGO organisations such as the IWF, the ISPA or major ISPs such as BT or TalkTalk. Nodes C represent smaller pressure groups or local associations such as Article 19, Privacy International or regional government such as local authorities. The smallest, node D nodes, represent individuals (note this is not to scale). The question of regulatory success or failure is then measured by the relative gravity of the nodes on either side of the regulatory divide. Major regulatory players such as national governments or international NGOs will carry substantial weight and to overcome their regulatory settlements will be extremely onerous, bordering on the impossible for the individual without the support of more weighty allies such as NGOs civil society groups or other associative groupings. In a variation of the scales of justice the arguments of both sides are weighed not by a jury but by the community as a whole and found to be settled or failed.11

This finally explains the particular role of gatekeepers. As the sole guardians of access to certain spaces, communities or content they are extremely powerful and carry a significant amount of regulatory gravity. In fact they carry a regulatory weight probably not dissimilar to other state based regulators such as statutory regulators due to their unique ability to control the part of the community or network over which they control access. In particular internet gatekeepers are uniquely powerful regulators of all online activity. Arguably they are more powerful than any single state or state-based regulator as they uniquely have full regulatory control over that part of the network which they manage. As the cyberlibertarians pointed out fourteen years ago no government can claim such control. Internet gatekeepers are therefore uniquely powerful within cyberspace due to their positions at the nexus points between communications networks; this gives them considerable ability to control and therefore considerable gravity. This explains why they are such effective regulators; it does not though automatically imbue them with legitimacy.

E. Conclusion: Regulatory Gravity and Its Impact

11 Note it is not the aim of this paper to map the relative gravitational weights of each of the nodes, merely to postulate the theory of regulatory gravity. The mapping of relative gravitation weights will require considerable further analysis of a number of case studies.
This leaves a final, but vital issue. When is an external regulatory intervention legitimate? I do not aim to address all theories of legitimacy in such a short space as is offered by the conclusion of a paper looking at cyber-governance and regulatory theory. The main aim here is to model how regulatory effects move and flow in an open communications network with multiple overlapping communities. It may be argued though that regulatory gravity goes some way to also mapping the flow of legitimising authority as well as the flow of discourse. What regulatory gravity maps is the relative ability of nodes to influence the outcome of a regulatory intervention. Governments are of great gravitation pull as they have a number of regulatory levers, and the authority to use them. They may use direct regulation, including the power to make law, they may use economic incentives or penalties, they may intervene in the market, they may influence public opinion and they may delegate some of this authority to others. Of lesser gravity, but of clear influence, are gatekeepers and other private citizens in positions of power. This includes major multinational companies, local authorities, lobbying groups and organisations. It is clear these bodies carry substantial gravity – the Digital Economy Bill was passed after extensive lobbying of IFPI and the BPI, against the wishes of most individual citizens. These second tier nodes carry gravity due to a number of tools. They may have communicative access to tier one nodes, they may have considerable market power (or represent those who do), or they may simply be a gatekeeper. Further down smaller nodes swarm; smaller companies, website operators, and eventually individuals. These may carry little gravity but they are many. When combined they may represent a mass equal to that of a state regulator, as demonstrated by the recent uprisings in Egypt, Yemen, Bahrain and Libya. Although individuals in developed Western nations very rarely rise up and successfully challenge governments today the potential remains. The key to legitimacy, it seems, is not what mass you carry but how you carry it. The reason citizens of Western nations do not overthrow governments is because they are legitimate. They are legitimised through the democratic process. The key question is how that legitimacy may either be transferred to, or earned by, tier two and tier three actors. I would suggest there are two ways this may occur. Either power is legitimately transferred from an already legitimate regulator or legitimacy is recognised by the regulated community. If the latter is to occur there must be a free and unhindered flow of information to allow for deliberative discourse.

12 It is not the intent of the author to undertake an analysis of the legitimacy of public bodies at this late stage.
This suggests the use of gatekeepers, who affect the flow of vital information, as proxy regulators, is always illegitimate unless there has been a transfer of legitimate authority. The use of other proxy regulators though may be legitimised if the community supports that action after consideration and discourse (Habermas 1998).
Bibliography


Convention on Cybercrime, ETS No.185.


Zittrain, J 2009 The Future of the Internet: And How to Stop It: Penguin.