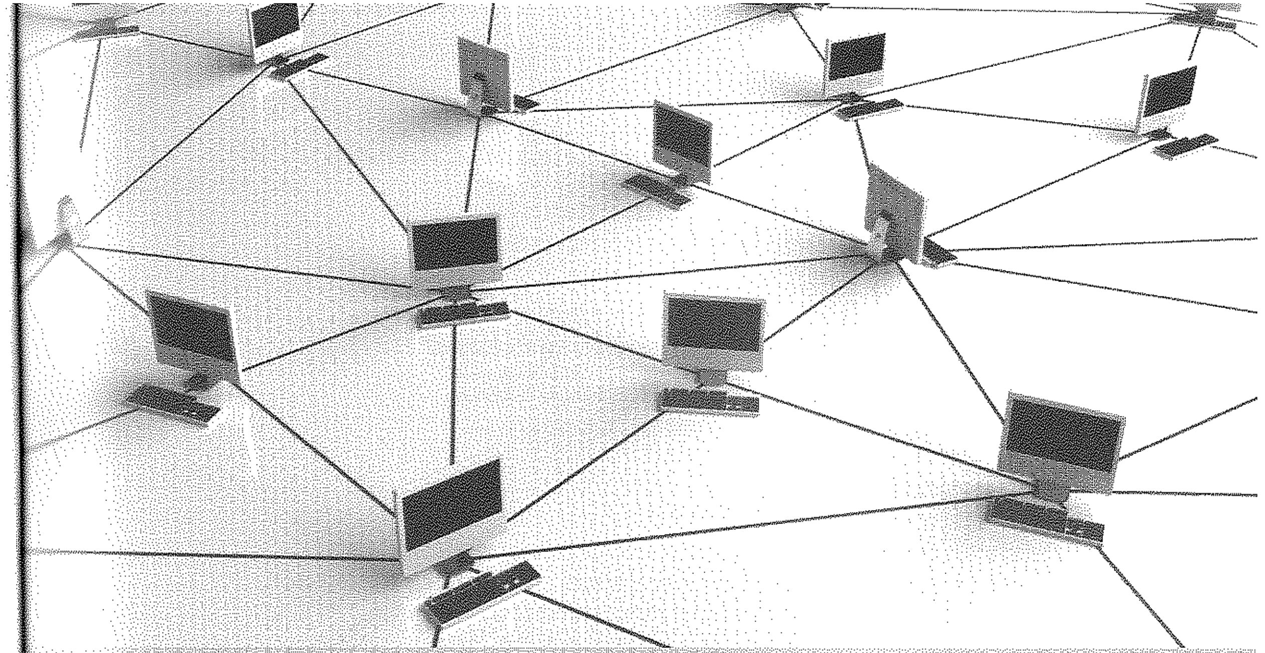
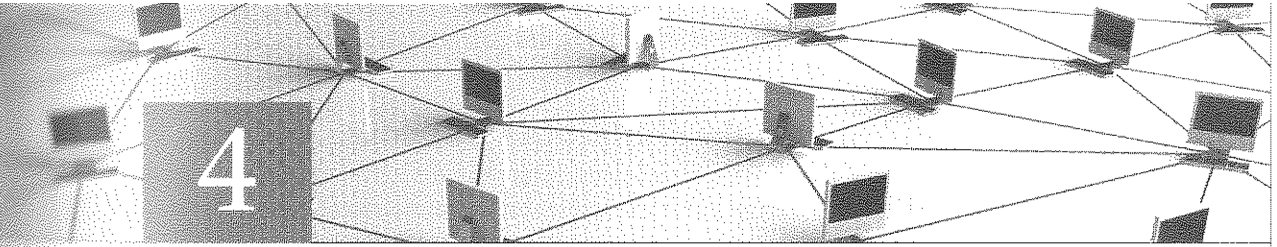


Information Technology Law

The law and society

Andrew Murray

OXFORD
UNIVERSITY PRESS



Regulating the digital environment

As discussed in Chapter 3, the process of digitisation is proving to be a logistical challenge for lawmakers. In the real world we design laws to protect physical goods and to control the actions of corporeal individuals. Thus, as was discussed in Chapter 1, s. 1 of the Theft Act 1968, expects that stolen goods are tangible. Similarly, and as discussed in Chapter 3, Copyright Law, although a law designed to deal with intangible goods, makes use of the physical environment to assist in the regulation of copyright infringement, while personal data privacy was, prior to digitisation, protected in part by the environmental factors which made storage of, access to, and cross-referencing of information held in physical files expensive and time consuming. The societal move from value in atoms to value in bits therefore offers a major challenge to lawmakers as it suggests traditional legal rules require to be re-evaluated when we consider extending them into the digital environment. For example, should the provisions of real world laws such as the Theft Act 1968 apply to virtual universes where virtual property is acquired and sometimes stolen?[1] Similarly should the legal provision designed to prevent abuse of children in the production of child abuse images, found in s. 1 of the Protection of Children Act 1978, be extended to prevent the production and possession of pseudo-images; images which appear to portray the abuse of a child but which have been computer generated?[2] These challenges of digitisation, allied to the ability of internet communications to cross borders without being subjected to border controls, led some lawyers and academics to suggest that traditional legal rules, predicated on the dual foundations of physicality of goods and persons and jurisdictional boundaries, could not be extended to Cyberspace. They believed that the incorporeal and borderless nature of the digital environment would render traditional lawmakers powerless, and would empower the community within Cyberspace to elect its own lawmakers and to design its own laws tailored to that environment. Others disagreed, and for a period of time the argument was not about which laws should be applied in the digital environment: it was more simply could we regulate the actions of individuals in the digital environment at all?

[1] This question will be discussed in depth in Ch. 21.
[2] This question will be discussed in depth in Ch. 14.

4.1 Can we regulate the digital environment?

4.1.1 Cyberlibertarianism

On 8 February 1996 John Perry Barlow published his declaration that Cyberspace was a separate sovereign space where real world laws and real world governments were of little or no effect.[3] His *Declaration of Independence for Cyberspace* was a powerful challenge to lawmakers and law enforcement bodies.

Highlight Barlow's Declaration of Independence for Cyberspace

> Weary giants of flesh and steel you are not welcome among us and have no sovereignty where we gather.... You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

The final part of this sentence sets out one of the key supports utilised by the school of thought that was soon to become known as cyberlibertarianism. They believed that as traditional lawmakers may only enforce their laws within the confines of their legal jurisdiction, subject of course to a few specialised examples of extraterritorial effect,[4] when a citizen of a real world jurisdiction, such as England and Wales, enters Cyberspace they cross a virtual border to a new sovereign state where the laws of the old state they left are no longer legitimate or valid. Further because this person is in a virtual (digital) environment they have no corporeal body to imprison and any digital goods they own are in limitless supply meaning that the sequestration of goods is an impractical method of punishment. This led to the belief, as expressed by Barlow, that traditional lawmakers could not enforce their laws against citizens of Cyberspace.

There is an obvious weakness in this argument. When one visits Cyberspace one does not travel to that place. Unlike the imaginary worlds of childhood fantasy such as Narnia or Alice's Wonderland, Cyberspace is not somewhere to which we are physically transported. This means that if an individual were to engage in illegal or anti-social behaviour online their corporeal body (and all the assets owned by that individual) remains at all times subject to the direct regulation of the state in which they are resident at that time.[5] Thus a UK citizen who visits online paedophilic communities to engage in the trading and viewing of child abuse images remains at risk of apprehension and prosecution in the UK as their corporeal body is at all times subject to the actions of UK Law enforcement authorities.[6] This belies Barlow's claim that traditional lawmaking and enforcement bodies 'do not possess any methods of enforcement we have true reason to fear' and led to a number of responses indicating that there is nothing about the nature of the digital environment which naturally protects individuals from the controls of real world lawmakers and law enforcement authorities. Professor Chris Reed calls this cyberlibertarian environmental argument 'the Cyberspace fallacy'[7] pointing out that: '[this] 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 ... 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 ... It is inconceivable that a real-world jurisdiction would deny that its laws potentially applied to the transaction.'[8] As Reed goes on to demonstrate, wherever traditional law enforcement bodies have faced the challenge of cross-border trade or harm the ordinary rules of private international law, jurisdiction and choice of law, have proven effective in identifying the correct forum and legal rules to apply.

The lack of physicality found in the digital environment forms only part of the Cyberlibertarian school of thought. The other key support, alluded to in Professor Reed's response, is that real world law enforcement bodies lack legitimacy to interfere in the operations of 'Sovereign Cyberspace'. This is predicated upon the twin beliefs that there is a border between real space and Cyberspace, a border not dissimilar to that we find between jurisdictions in real space, and that once one crosses this border into Cyberspace, one may move freely about in 'Sovereign Cyberspace' without barrier or challenge. In other words the Cyberlibertarian School believed that Cyberspace was a separate state, although not physically.

This concept is most fully explored in the groundbreaking work of two US Law Professors, David Johnson and David Post who in May 1996 published their highly influential paper *Law and Borders—The Rise of Law in Cyberspace*.[9] In this paper they set out fully, and for the first time, a legal interpretation of the Cyberlibertarian contention that regulation founded upon traditional state sovereignty cannot function effectively in Cyberspace. They argued that as individuals in Cyberspace may move seamlessly between zones governed by differing regulatory regimes in accordance with their personal preferences it was impossible to effectively regulate the activities of these individuals.

[3] J.P. Barlow, *A Declaration of Independence for Cyberspace*: http://homes.eff.org/~barlow/Declaration-Final.html.

[4] For example Sch. II of the Sex Offenders Act 1997 gives courts in the UK jurisdiction to prosecute UK citizens and residents who commit sex offences against children abroad. This law applies to British citizens and residents and is applicable even where the person in question was not a British citizen or UK resident at the time of the offence but has subsequently become one.

[5] Or the state in which the assets are to be found.

[6] As has been demonstrated on many occasions: see, e.g. *R. v Fellows & Arnold* [1997] 2 All ER 548; *R. v Bowden (Jonathan)* [2001] QB 88; *Atkins v Director of Public Prosecutions* [2000] 1 WLR 1427 or *R. v Jayson* [2002] EWCA Crim 683.

[7] C. Reed, *Internet Law: Text and Materials* (2nd ed. 2004).

[8] *ibid*, 174–175.

[9] 48 *Stanford Law Review* 1367 (1996).

Example Obscenity

Leo is a UK resident who wishes to access and download pornographic images which are in breach of the Obscene Publications Acts. Although illegal in the UK these images may be legal in the US. Leo therefore may access material hosted in the US and view it on his computer in the UK.

Example Contempt of Court

In 2007 two men attempted to blackmail a member of the UK Royal Family. A s. 11 Order was granted under the Contempt of Court Act 1981 meaning it was illegal to publish the name of the person involved (it still is). Despite this it is extremely easy for a UK resident to find the name of the person involved with a quick Google search as the name has been published online by several overseas news organisations and gossip sites which are all accessible in the UK. It would even be possible for a UK resident to publish this person's name, in breach of the Contempt of Court Act overseas, but if identified they may face prosecution.

This meant that citizens of Cyberspace could engage in a practice known as regulatory arbitrage. This occurs when an individual or group may potentially be regulated by a number of alternate regulatory bodies and is offered the opportunity to choose which one to be regulated by. The individual then arbitrages (or plays off) these regulators against each other to seek the best regulatory settlement for the individual.[10] In our obscene publications example our UK resident in the real world is directly regulated by the UK border and police forces. There is no opportunity to arbitrage their regulation (in enforcing the Obscene Publications Acts) against anyone else without leaving the jurisdiction of the UK courts. But in Cyberspace he or she may seek the shelter of the US regulatory authorities by sourcing their pornographic content from US based web servers. Technically the UK resident remains in breach of s. 42 of the Customs Consolidation Act 1876 which makes it an offence to import indecent or obscene prints, paintings, photographs, books, cards, lithographic or other engravings, or any other indecent or obscene articles. But with surveys suggesting that 10 million UK adults visit pornographic websites,[11] it is clear the authorities simply do not have the resources to prosecute such a mass programme of disobedience. This is demonstrated by the fact that to date there have been no prosecutions in England and Wales under either the Customs Consolidation Act or the Obscene Publications Act 1959 for privately viewing obscene material using an internet connection. Thus the UK resident can safely arbitrage the UK regulatory framework of the Obscene Publications Acts and the Customs Consolidation Act for the US regulatory framework which has protection from the US First Amendment.[12] This allows, at least in cyberlibertarian theory, the citizen of Cyberspace to choose a different regulatory regime from that which regulates his or her activities in real space, undermining the effectiveness of traditional lawmaking processes and law enforcement institutions. Accordingly, the only effective 'Law of Cyberspace' would largely be determined by a free market in regulation in which network users would be able to choose those rule sets they found most congenial. Johnson and Post maintained that the various dimensions of inter-networking could be governed by 'decentralised, emergent law' wherein customary and privately produced laws, or rules, would be produced by decentralised collective action leading to the emergence of common standards for mutual coordination.[13] In other words, they believed that the decentralised and incorporeal nature of Cyberspace meant that the only possible regulatory system was one which developed organically with the consent of the majority of the citizens of Cyberspace.[14]

Cyberlibertarianism is clearly attractive for internet users. It suggests the development of new internet only laws designed to reflect the values of the community of internet users and separate from the old world values of state based lawmakers. Thus we could imagine copyright evolving to allow a private use copying right which would allow individuals to make multiple copies of files for use on several devices (Home PC, Laptop, Smartphone, MP3 player, etc.) or as appears to be the *de facto* position a relaxation of indecency laws to allow for far greater distribution of adult content. There are though clearly problems with such an approach. The first is who makes up the community of internet users, and who is authorised to speak for them?

The problem that the cyberlibertarians had to address was there is no homogenous community of internet users; instead in Cyberspace there are a series of heterogeneous communities with few shared values. This problem was highlighted by Professor Cass Sunstein in his book *Republic.com* where he suggested that the nature of the internet was to isolate individuals behind filters and screens rather than to provide for community building and democratic discourse.[15] Sunstein suggested that while a well functioning system of deliberative democracy requires a certain degree of information so that citizens can engage in monitoring and deliberative tasks,[16] the ability to filter information offered by digital technologies interferes with the flow of this information in two ways. The first is that the user may simply choose not to receive some of this information by using filters to ensure they only receive information of interest to them. As such there is no homogeneity of information across the macro community of users of

[10] See A. M. Froomkin, 'The Internet as a Source of Regulatory Arbitrage' in B. Kahin & C. Nesson (eds), *Borders in Cyberspace* (1997).

[11] Anthony Barnes & Sophie Goodchild, 'Porn UK', *The Independent on Sunday*, 28 May 2006: http://www.independent.co.uk/news/uk/this-britain/porn-uk-480084.html.

[12] *Reno v ACLU* 521 US 844 (1997).

[13] This notion parallels the concept of polycentric or non-statist law. See T. Bell, 'Polycentric Law' 7(1) *Humane Studies Review* 4 (1991/2); T Bell, 'Polycentric Law in the New Millennium.' Paper presented at The Mont Pelerin Society: 1998 Golden Anniversary Meeting, at Alexandria Virginia: http://www.tomwbell.com/writings/FAH.html.

[14] Johnson & Post, above n. 9. See also D. Johnson & D. Post, 'The New "Civic Virtue" of the Internet: A Complex Systems Model for the Governance of Cyberspace' in C.M. Firestone (ed.), *The Emerging Internet* (1998 Annual Review of the Institute for Information Studies).

[15] C. Sunstein, *Republic.com* (2001).

[16] *ibid*, 174.

the internet making truly deliberative democratic discourse impossible. Further Sunstein recognised that with the advent of internet communications it becomes easier to locate likeminded individuals whatever one's shared interests may be. This creates in Sunstein's words 'fringe communities that have a common ideology but are dispersed geographically'.[17] In turn this leads to community fragmentation. There are little in the way of common experiences and knowledge among the larger macro community of internet users. As Sunstein quickly demonstrated there can be no cyberlibertarian ideal of a 'decentralised, emergent law' as decentralised collective action is highly unlikely to lead to the emergence of common standards for mutual coordination in the highly decentred and filtered environment of Cyberspace.

If Sunstein was correct this meant that Cyberspace lacked the necessary homogeneity to achieve the necessary levels of internal democratic discourse needed for the creation of Cyberspace Law and as a result the internet could not be effectively regulated from within. But, as Post and Johnson had demonstrated, attempts to impose external regulatory settlements in Cyberspace would be equally ineffectual due to the effects of regulatory arbitrage and a lack of physical borders. This suggested an impasse. There had to be a legal framework which could be utilised in the online environment for it to flourish as a place to do business, further there had to be a way to regulate and eliminate antisocial and anti-market activities such as the trade in pornography and copyright infringing digital media files.[18] Fortunately Professor Sunstein was not the only theorist who had taken issue with the cyberlibertarian approach.

4.1.2 Cyberpaternalism

A new school of thought was developing, one which did not believe Cyberspace was immune from regulatory intervention by real world regulators. One of the strongest early critics of the cyberlibertarian position was Joel Reidenberg of Fordham Law School. Despite sympathising with the cyberlibertarian view that the internet leads to the disintegration of territorial borders as the foundation for regulatory governance, Reidenberg argued that new models and sources of rules were being created in their place. He identified two new regulatory borders arising from new rule-making processes involving States, the private sector, technical interests, and citizens. He believed the first set of these were made up of the contractual agreements among various Internet Service Providers. The second was to be found in the network architecture. The key to Reidenberg's analysis was this second border, the new geography of the internet which unlike the geography of the natural world was man-made and in our control.

[17] *ibid*, 58.

[18] Note: I have not forgotten Professor Reed's point that the corpus of the individual user of online services remains subject to the direct control of the state where the individual is resident. Directly harmful activities such as the trade in child pornography will be directly regulated in this fashion. What is in issue here is more generally harmful or antisocial behaviour which is being engaged upon by a large number of users of online services and for whom direct legal regulation through the courts would be impracticable due to the large numbers of persons involved.

Reidenberg claimed that technical standards could function like geographical borders as they establish default boundary rules that impose order in network environments. Using the network architecture as a proxy for regulatory architecture Reidenberg suggested a new way of looking at control and regulation in the online environment a conceptualisation he called *'Lex Informatica'*.[19] This draws upon the principle of *Lex Mercatoria* and refers to the 'laws' imposed on network users by technological capabilities and system design choices. Reidenberg asserted that, whereas political governance processes usually establish the substantive laws of nation states, in *Lex Informatica* the primary sources of default rule making are the technology developer(s) and the social processes through which customary uses of the technology evolve.[20] To this end, he argued that, rather than being inherently unregulable due to its design or architecture, the internet is in fact closely regulated by its architecture.

Reidenberg contended that in the light of *Lex Informatica's* dependence on design choices, the attributes of public oversight associated with regulatory regimes, could be maintained by shifting the focus of government actions away from direct regulation of Cyberspace, toward influencing changes to its architecture. Reidenberg's concept of regulatory control being implemented through the control mechanisms already in place in the network architecture led to development of the new cyberpaternalist school. This new school viewed legal controls as merely part of the network of effective regulatory controls in the online environment and suggested that lawmakers seeking to control the online activities of their citizens would seek to indirectly control these activities by mandating changes to the network architecture, or by supporting self-regulatory activities of network designers. This idea was most fully developed and explained by Professor Lawrence Lessig in his classic essay *Code and Other Laws of Cyberspace*.[21] Lessig contends that there are four 'Modalities of Regulation' which may be used individually or collectively either directly or indirectly by regulators to control the actions of individuals offline or online.[22] Further, Lessig suggests that Johnson and Post were wrong to suggest that regulatory arbitrage must undermine any attempt to regulate the activities of individuals online as regulators draw their legitimacy from the community they represent (and regulate) and as individuals we are therefore tied to the regulator in a way which Johnson and Post fail to recognise. As Lessig says: 'Even if we could construct cyberspace on the model of the market there are strong reasons not to. As life moves online, and more and more citizens from states X, Y, and Z come to interact in cyberspaces A, B, and C, these cyberspaces may well need to develop the kind of responsibility and attention that develops (ideally) within a democracy. Or, put differently, if cyberspace wants to be considered its own legitimate sovereign, and thus deserving of some measure of independence and respect, it must become more clearly a citizen sovereignty'.[23]

[19] J. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 *Emory Law Journal* 911; J. Reidenberg, 'Lex Informatica: The Formation of Information Policy Rules Through Technology' 76 *Texas Law Review* (1998), 553.

[20] On the role of software designers in default rule making see P. Quintas, 'Software by Design' in R. Mansell and R. Silverstone (eds), *Communication by Design: The Politics of Information and Communication Technologies* (1998).

[21] Basic Books (1999).

[22] *ibid*, 88ff.

[23] L. Lessig, *Code Version 2.0*, (2006), 290.

Thus Johnson and Post's position that regulatory arbitrage, coupled with a physical border between real space and Cyberspace must lead to the development of a distinct and separate body of law for Cyberspace is in Lessig's view tautologous. By attempting to reject real world regulation citizens within Cyberspace undermine the possibility of competing real world regulators recognising the independence of Cyberspace as a sovereign space meaning that attempts to develop a separate set of principles for Cyberspace will fail. For Lessig the key to regulating all activity, whether it happens to be in the online or the offline environment is to be found in his four modalities of regulation: (1) laws (2) markets (3) architecture and (4) norms. Lessig believes that regulators may by using carefully selected hybrids of the four to achieve whatever regulatory outcome they desire. If Lessig is correct there is no doubt that we can regulate the digital environment and the cyberlibertarians were mistaken in their claims to the contrary.

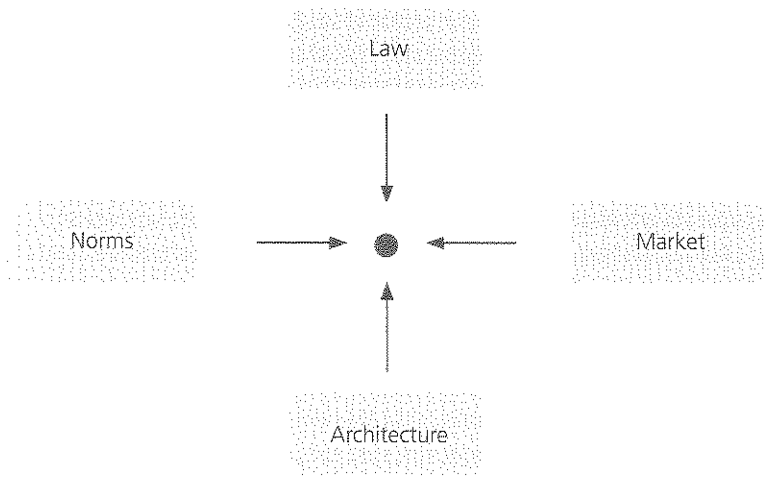
4.2 Lawrence Lessig's modalities of regulation

Lawrence Lessig asked us to reconsider how one is regulated on a day-to-day basis. Although the law may say it is illegal to steal it is not usually the legal imperative that prevents most of us from stealing, rather the majority of people do not steal because they do not want to steal in the first place. We do not steal, not because we fear imprisonment but because we have been morally conditioned to accept that theft is a morally reprehensible act. Lessig concluded that four factors, or modalities, control the activities of individuals and each of these modalities functions by acting as a constraint on the choices of actions that individuals have. Thus law constrains through the threat of punishment, social norms constrain through the application of societal sanctions such as criticism or ostracism, the market constrains through price and price-related signals, and architecture physically constrains (examples include the locked door and the concrete parking bollard). To demonstrate how these four modalities function collectively on the choice of actions an individual Lessig had us imagine a 'pathetic dot' which represents the individual and then graphically represented the four modalities as external forces which act upon that dot in control of its actions. This is seen in Figure 4.1.

Lessig demonstrated how these modalities function by using examples such as the regulation of smoking[24] or in the supply of illegal drugs[25] or the right of a woman to choose to have an abortion.[26] A further contemporary example, perfect for a discussion of digital property rights, may be found in regulating the illegal secondary market for copyright infringing MP3 music files. It is clear that in the UK anyone who makes a copy of a copyright protected MP3 music file without the consent of the copyright holder commits a infringement of that copyright.[27] Further anyone who makes a copy of an MP3 file with the intent to sell or hire that copy or distribute it in the course of business commits a criminal offence.[28] Thus the legal controls on copyright infringement are clear. The law states that one cannot make and/or distribute a copy of a protected work in the UK without facing civil, or possibly even criminal, sanctions. To use the language of Lawrence Lessig the modality of law has been employed to prevent this activity.

[24] *ibid* 122–123.
[25] *ibid*, 131.
[26] *ibid*, 132.
[27] CDPA 1998, s. 17.
[28] *ibid*, s. 107.

Figure 4.1 Lessig's modalities in action



Source: Lawrence Lessig CC: BY: SA

Yet it appears that the application of the law in this area is of little impact as individuals continue to download and share music using illegal sources. This failure of the law to control individuals is the failure that was predicted by the cyberlibertarian movement. Individuals use the network to evade legal controls and do so by using tools such as BitTorrent.[29] But this does not mean that the MP3 market is not subject to control. For while the direct effects of the law may be failing the other modalities provide an alternative means of regulation.

The second of Lessig's modalities is markets and here the first successful regulatory intervention may be seen. With the success of technologies such as the iPod and its sister product iTunes Apple pioneered the technology for online MP3 sales. This market has now massively expanded with a variety of services offering the opportunity to legally buy an MP3 track or album, or offering subscription services which lease to you music on a monthly basis for payment of a fee.[30] As the costs of these services have fallen,[31] we saw for the first time in 2008 clear evidence that legal music downloads are

[29] While historically the copyright industries have had some success in litigating against file sharing technologies such as Napster (*A&M Records Inc. v Napster* 239 F.3d 1004 (9th Cir. 2001)) and Grokster/Kazaa (*MGM Studios, Inc. v Grokster, Ltd* 545 U.S. 913 (2005)), the completely decentralised nature of BitTorrent has proved a challenging proposition for real world laws. Despite the recent success of the copyright industry in the case of *Sweden v The Pirate Bay*, the Pirate Bay site remains in operation pending an appeal while other Torrent tracking sites remain in place should The Pirate Bay be closed down.

[30] For example, Napster's Hits Unlimited service costs £9.95 per month for unlimited access to the entire Napster catalogue.

[31] The price of Napster's unlimited service dropped from £14.95 to £9.95 in 2008, while the arrival of Amazon in the MP3 download market has seen a major provider offer single tracks for 59p and albums for £3 compared to Apple's 79p and £7.99.

growing faster than illegal file sharing in the UK.[32] Where the legal control failed to have impact we find that a market solution seems to be having effect. This is exactly as Lessig predicted. In the digital environment while the effect of direct legal controls is often diluted by a remoteness from the law enforcement authority and by a lack of border controls other modalities are strengthened including market modalities which benefit from greater transparency and speed of information.

The MP3 music market also demonstrates something else about the way Lessig's modalities function in the digital environment. It might be assumed that the most effective way to prevent illegal file sharing is to adjust the architecture of the digital files which carry the music to make illegal sharing of them impossible. This is the industry solution predicted by Lessig. Like Reidenberg he saw our ability to manipulate the network architecture as the most obvious development in Cyber-regulation. Where laws failed to have effect he believed industry would turn more to architectural or design-based modalities: 'We can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of building'.[33]

In the case of MP3s the music industry did just as Lessig predicted. They began to design a suite of Digital Rights Management software (DRM) and began to place it on their digital music released on CD. Some of the more famous include Cactus Data Shield used by BMG and Universal Music, Sony Extended Copy Protection, and most famous of all Apple's FairPlay used on iTunes products. These systems were reinforced by strong legal provisions promulgated by the World Intellectual Property Organisation[34] and which once implemented in leading markets made it illegal to remove or reverse engineer the DRM protection in the US[35] and in the European Union.[36] What has happened to all these DRM systems? Well, Cactus Data Shield became embroiled in controversy as discs containing the CDS software would not play on non Windows operating systems, nor on game systems such as the Xbox or the Playstation 2 or on older CD players which played protected discs with audible errors. As a result discs released with CDS often had to be reissued in a non-protected format rendering the DRM protection valueless. At the time of writing the author is unaware of any music releases still protected by CDS. The story of Sony's Extended Copy Protection (XCP) system is even more telling. In 2005 Sony released fifty-two titles with XCP protection. It quickly became apparent that the XCP system installed a rootkit, that is a piece of software installed without permission on the user's computer which can take control of hardware settings, and that due to a design flaw in this the software created security holes which could be exploited by malicious software such as worms or viruses. Within fifteen days of the flaw being discovered Sony BMG announced that it was backing out of its copy-protection software, recalling unsold CDs from all stores, and offering consumers to exchange their CDs with versions lacking the software.[37] Finally Apple FairPlay. It is by far the most enduring and successful DRM. It is designed to ensure people do not swap purchased music across Apple music devices. FairPlay encrypted audio tracks may be copied to any number of Apple portable music players, however, each player can only have tracks from a maximum of five different iTunes accounts, and in addition the track may only be played on up to five authorised computers simultaneously. Although it seems at first glance that the main beneficiary of FairPlay is Apple itself (it protects the iTunes market and makes the iPod/iTunes partnership irresistible) it appears Apple were forced into FairPlay by the music industry. Following a plea from Steve Jobs, CEO of Apple Inc., to the music industry,[38] it was announced on 6 April 2007 that Apple had reached agreement with EMI to make its music available DRM free, while on 6 January 2009 a further announcement made at the Macworld Conference and Expo revealed that from that date all music on iTunes would be DRM free.

All attempts to use design modalities to engineer music files which could not be copied have failed. Nearly all music available today, whether it be in MP3 format or encoded onto a CD comes free of DRM technology. The provisions of the WIPO treaties, the Digital Millennium Copyright Act and the Copyright and Related Rights in the Information Society Directive, look dated and irrelevant in the modern digital age, but why? Why if DRMs are the most effective and efficient way to protect against illegal file sharing have they failed to take effect? Surely if Lessig is right and we have to choose to either 'build, or architect, or code cyberspace to protect values that we believe are

[32] See IFPI, *Digital Music Report 2008*: http://www.ifpi.org/content/library/DMR2008.pdf.

[33] Lessig, above n. 23, 6.

[34] Article 11 of the WIPO Copyright Treaty of 1996 requires that: '[States] shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law'. In addition Article 18 of the WIPO Performances and Phonograms Treaty of 1996 requires that: '[States] shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.'

[35] Section 103 of the Digital Millennium Copyright Act 1998 (17 U.S.C Sec. 1201(a)(1)) states that 'No person shall circumvent a technological measure that effectively controls access to a work protected under this title'. The penalty for so doing being the possibility for statutory damages of up to $2,500 for *each* violation in addition to actual damages should a civil case is brought. In criminal cases (where the accused is deemed to have acted wilfully and for purposes of commercial advantage or private financial gain (note this includes file sharing)) for a first offence you may be imprisoned for up to five years and fined up to $500,000. For subsequent offences you may be imprisoned for up to ten years and fined up to $1,000,000.

[36] Article 6 of the Directive on Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (Dir. 2001/29/EC) requires states to 'provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective'. In the UK this has been given effect in the Copyright and Related Rights Regulations 2003 (SI 2003/2498).

[37] VNUnet.com, *Sony backs out of rootkit anti-piracy scheme*, 15 November 2005: http://www.vnunet.com/vnunet/news/2146053/sony-backs-root-kit-anti-piracy.

[38] On 6 February 2007, Steve Jobs, published an open letter entitled *Thoughts on Music* calling on the big four music companies to sell their music without DRM. According to Jobs, Apple does not want to use DRM but is forced by the four major musical labels with whom Apple negotiates contracts for iTunes. Jobs's main points were: (1) DRM has never and will never be perfect. Hackers will always find a method to break DRM. (2) DRM restrictions only hurt people using music legally. Illegal users aren't affected by DRM. (3) The restrictions of DRM encourage users to obtain unrestricted music which is usually only possible via illegal methods.

The vast majority of music is sold without DRM via CDs which has proven successful (see Steve Jobs, *Thoughts on Music*, 6 February 2007, http://www.apple.com/hotnews/thoughtsonmusic/).

fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear' we cannot end up with the scenario where all the built or architected changes are removed (or to stick to the building metaphor are demolished and the environment returned to open plain). Surely if we are all just pathetic dots the industry would have forced its DRM technology on us, after all as Lessig says 'Thus, four constraints regulate this pathetic dot-the law, social norms, the market, and architecture-and the "regulation" of this dot is the sum of these four constraints'.[39]

4.3 Network communitarianism

The reason for the failure of DRM systems in commercial music releases is explained by a new school of thought which has developed in the last few years. While cyberlibertarians believed the architecture of the network protected individuals from the attentions of real world regulators and cyberpaternalists believed rather the opposite, this new school of thought sees the relationship between the digital environment and the real world as a rather more fluid affair. This new school of thought is the network communitarian school.

Unlike cyberlibertarianism and cyberpaternalism this developed in Europe with much of the early work taking place in the UK. The main proponent of network communitarianism is Andrew Murray who in his book *The Regulation of Cyberspace* set out a model of network communitarian thought.[40] Murray believes that the cyberpaternalist model fails to account for the complexities of information flows found in a modern telecommunications/media system such as the internet. The main influences on network communitarianism are two European schools of thought which have yet to fully translate to the US, and which have therefore not influenced either cyberlibertarianism or cyberpaternalism. These are Actor Network Theory (ANT) developed in Paris in the 1980s by Michel Callon and Bruno Latour and Social Systems Theory (SST) developed in Germany by Niklaus Luhmann and Gunther Teubner.

ANT is a theory of social transactions which accepts a role for nonhuman actors in any social situation. Thus in a transaction between two individuals in a restaurant their transaction is also affected by the restaurant itself: one would expect a different transaction in a luxury Michelin starred restaurant than in a local café bar. The difference is not so much the surroundings themselves but the semiotic, or concepts, which the human actors have communicated to them through memory, experience, and surroundings.[41] A key concept of ANT is that social communications are made up of parallel transactions between the material (things) and semiotic (concepts) which together form a single network. This has the potential to be particularly powerful when applied to the internet. The internet is the largest person to person communication network yet designed. It allows individuals to move social transactions in space and time and it allows transactions between people with shared experiences who are geographically remote and between people with no common history who are geographically close.[42] The potential for new networks to form, dissolve, and reform on the internet is massive, leading one to reconceptualise the internet not merely as a communications/media tool but as a cultural/social tool.[43]

SST shares some roots with ANT but is quite distinct. SST attempts to explain and study the flow of information within increasingly complex systems of social communication. Luhmann attempts to explain how communications affect social transactions by defining social systems as systems of communication, and society as the most encompassing social system. A system is defined by a boundary between itself and its surrounding environment, dividing it from the infinitely complex, or chaotic, exterior.[44] The interior of the system is thus a zone of reduced complexity: Communication within a system operates by selecting only a limited amount of all information available outside. This process is also called reduction of complexity. The criterion according to which information is selected and processed is meaning.[45] Like ANT SST is an attempt to map and study the complex process of social interactions in the increasingly complex and connected environment of modern society. Whereas ANT is about the evolution and formation of networks, SST is about the filtering of information flows in the decision making process and the communication of ideas and concepts between systems.

Although these theories are quite distinct when taken together they can illuminate much of our understanding of communications and social interaction in a networked environment such as the internet with a variety of actors, both human and non-human.[46] This is what Murray attempts in *The Regulation of Cyberspace*. He re-examines the classical cyberpaternalist model discussed earlier in which a pathetic dot is found to reside among four regulatory modalities which act as a constraint on the choice of actions of that 'dot' and finds that in applying the principles of ANT and SST we can consider the 'dot' rather differently. The dot is in ANT terms a material node in the network, while in SST terms is part of a system. In either term the dot is not isolated, it forms part of a matrix of dots, or to put it another way the dot, which is designed to

[39] Lessig, above n. 23, 123.

[40] A. Murray, *The Regulation of Cyberspace: Control in the Online Environment*, (2007).

[41] This is a woefully inadequate description of ANT which is extremely complex, rich, and valuable. Students interested in embarking on a study of ANT should start with B. Latour, *Reassembling the Social: An Introduction to Actor-network-theory* (2007).

[42] And obviously between people geographically remote and with no common history also.

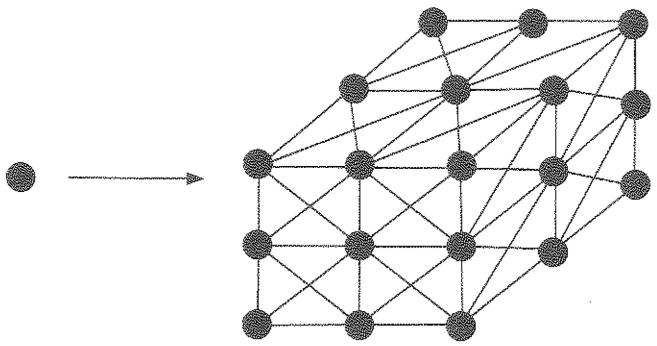
[43] This is actually well worn ground in the field of communications and media studies although it seems quite alien to many lawyers and regulators. See, e.g. M. Castells, *The Internet Galaxy* (2001) or R. Mansell (ed.), *Inside the Communication Revolution: Evolving Patterns of Social and Technical Interaction* (2002).

[44] Thus a system may be the legal system where lawyers practice their trade and give advice against the background of the corpus of law. Lawyers may be asked 'is it legal to use offshore tax systems to process the profits of a particular transaction?' they will not be asked 'is it moral?' or is it 'socially harmful?' these are questions for respectively theologians (or philosophers) and politicians. Thus in the internal language of the legal profession the question is binary legal or illegal, rather than multifaceted in the wider system of society at large.

[45] As with ANT this is a woefully inadequate description of SST which is extremely complex, rich and valuable. Students interested in embarking on a study of SST should start with H. Moeller, *Luhmann Explained*, (2006). Law students may then be interested in N. Luhmann, *Law as a Social System* (2008).

[46] For a fascinating attempt to fuse the two together read G. Teubner, 'Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law' (2006) 33 *Journal of Law and Society* 497.

Figure 4.2 From the pathetic dot to the active dot matrix



represent the individual, must always be considered to be part of the wider community and it is here that traditional cyberpaternalism runs into difficulty, for when one examines the modalities of regulation proposed by 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,[47] 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. Murray recognised that these 'socially mediated modalities',[48] reflected an active role for the 'dot' in the regulatory process; far from being a 'pathetic dot' which was the subject of external regulatory forces the dot was in fact an 'active dot' taking part in the regulatory process.[49] For Murray there are two key distinctions between the classic cyberpaternalist model and the new network communitarian 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 (see Figure 4.2). The second is to recognise 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, as illustrated in Figure 4.3.

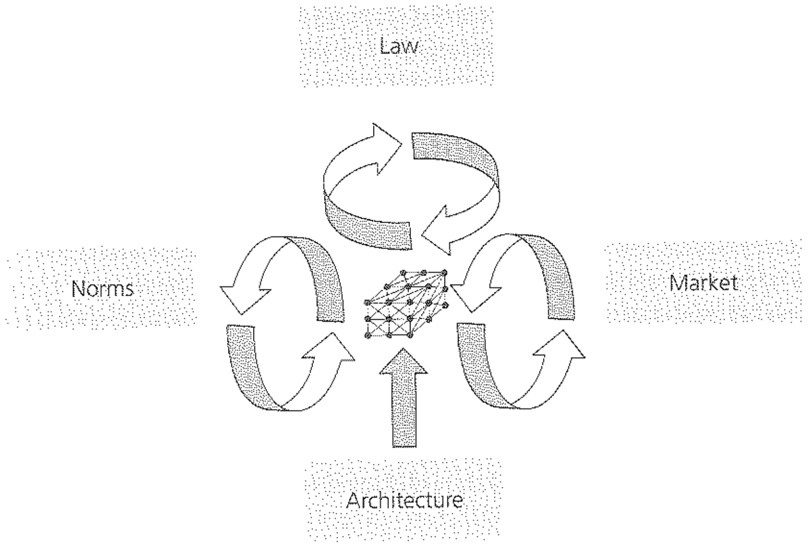
What does this mean for our understanding of internet regulation? Firstly it suggests that regulation in the online environment is little different to regulation in the real world. Regulation is a process of discourse and dialogue between the individual and society. Sometimes society, either directly through the application of norms, or indirectly by distilling its opinions, norms, or standards down to laws wishes to force

[47] At least in democratic representative politics as found in the UK. In the UK we may view the rights of MPs (our representatives) to make laws as being power drawn from the community at large as part of our social contract between the state and citizen. See J. Rousseau, The *Social Contract* (1762, trans M. Cranston, 2004).

[48] Murray, above n. 40, 37.

[49] *ibid*, Ch. 8.

Figure 4.3 The regulatory discourse



a change in behaviour of the individual.[50] 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 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 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 abuse (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. This also explains why Digital Rights Management systems failed to have the desired effect. DRMs were viewed by the majority of music consumers to be an unreasonable, and sometimes damaging, restriction on their freedom to enjoy something they viewed,

[50] A good current example of such a change is s. 63 of the Criminal Justice and Immigration Act 2008 which makes it an offence to possess 'extreme pornographic images'. These are images of sexual violence, bestiality and necrophilia. This is society in the UK setting a limit on the free availability of pornographic images in the online environment. We cannot prevent pornography from entering the UK but we can criminalise the most offensive varieties of pornography to stifle demand, thus also allowing the market to make the production of such material less commercially attractive.

having paid to purchase it, as their property. When Cactus Data Shield prevented them from playing their new CD on their old CD player, or when Apple FairPlay restricted them to having five authorised computers (a problem in an extended family) or worst of all when Sony Extended Copy Protection was shown to leave their PCs vulnerable to attack, consumers reacted in the way one would expect: They collectively used their market power to respond. The industry could not force its DRM technology on us because we can withhold our market support for them. In network communitarian theory the power to determine the regulatory environment does not rest with the regulator alone.[51]

Whichever of the current schools of cyber-regulatory theory you subscribe to: cyberpaternalism or network communitarianism, one thing is clear. There is one key issue that both agree upon: that in the man-made environment of the digital sphere our ability to change the design of that place with a few well placed keystrokes means that the use of architecture as a modality of control (that is employed by one of the other modalities as a means of enforcing their values) is increasingly in evidence and is increasingly effective. For this reason the remainder of this chapter will look at who some of the key regulators in this environment are. Who are the people with the opportunity to amend the software code of the digital environment and on which basis do they exercise their power?

4.4 **Regulators in cyberspace: private regulators**

There are a number of private regulators at work in the digital environment with the ability to regulate certain activities directly by making design changes to the environment. The first line of private regulation most internet users encounter in the UK is their internet service provider (ISP). As it is impossible for individuals to gain access to the internet without employing the services of an ISP, ISPs can act as gatekeepers. The position of gatekeeper is a powerful one in regulatory theory as gatekeepers control access to and egress from a particular place or community. As a result of their role as internet gatekeeper ISPs have been tasked with ever increasing regulatory roles in the UK. The most high profile role for ISPs is their collective role in preventing access to child abuse images and other illegal content.

In an attempt to control the trade in illegal content the UK Government requires ISPs to block access to sites known to contain images of child abuse but which are domiciled outwith the UK, and which are therefore out of the direct control of UK laws. This is affected by a partnership between ISPs and an industry regulatory body known as the Internet Watch Foundation (IWF). The IWF operates the UK internet 'hotline' for the public to report potentially illegal online content (that is content portraying child abuse,[52] criminally obscene content hosted in the UK[53], content designed to incite racial or religious hatred content hosted in the UK,[54] and extreme pornography[55]). The IWF is a private industry body which is funded by industry partners and a European Union grant. It regulates content within its remit by creating a blacklist of sites which contain illegal content. This blacklist is then distributed to all UK ISPs who are expected to block access to all sites contained on the list. The blocking of access is therefore effected by private corporations (the ISPs) at the requirement of another private corporation (the IWF), but, it is a requirement of the UK Government that this private regulatory system be enforced.

This was illustrated in a Parliamentary written answer in 2006 when Home Office Minister Vernon Croaker noted that 'we are setting a target that by the end of 2007 all ISPs offering 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.'[56] Failure to implement a private regulatory system would have led to legislation compelling ISPs to filter access. This requirement has subsequently been implemented, without the need for legislation, by all major UK commercial ISPs under a variety of names or systems. The best known of which is Cleanfeed developed by British Telecom and used by BT and most other major UK ISPs under licence. Cleanfeed works by filtering all user requests through an internet router which compares requests for pages against the IWF blacklist, if the requested page is blacklisted the Cleanfeed system will reroute this request to a BT proxy server which issues an error message to the customer. In theory Cleanfeed is extremely efficient. Unlike older forms of content blocking Cleanfeed does not black entire sites only blacklisted pages. Thus if one page on the MySpace site contained an indecent image Cleanfeed should only block access

[51] In this final analysis network communitarianism in the internet regulation context shares core values with decentred regulation in mainstream regulatory theory. See, J. Black, 'Decentring Regulation: Understanding the Role of Regulation and Self Regulation in a "Post-Regulatory" World' (2001) 54 *Current Legal Problems* 103; C. Scott, 'Regulation in the Age of Governance: The Rise of the Post Regulatory State' in J. Jordana and D. Levi-Faur (eds) *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (2004).

[52] By s. 160 of the Criminal Justice Act 1988, as amended by the Criminal Justice and Public Order Act 1994, it is an offence for a person to have any indecent photograph or pseudo-photograph of a child in his possession. A pseudo-photograph is defined in s. 7(7) of the Protection of Children Act 1978 as 'an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph'.

[53] By s. 2 of the Obscene Publications Act 1959 it is an offence to publish an obscene article in the UK. The definition of an obscene article is found in s. 1 and defines it as: '[where] its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it'.

[54] Part 3 of the Public Order Act 1986 creates offences of use of words or behaviour or display of written material (s. 18), publishing or distributing written material (s. 19), public performance of a play (s. 20), distributing, showing, or playing a recording (s. 21), or broadcasting (s. 22), if the act is intended to stir up racial hatred, or possession of racially inflammatory material (s. 23). Part 3a was added by the Racial and Religious Hatred Act 2006 with the insertion of new sections 29A to 29N. This created mirror offences for acts intended to stir up religious hatred.

[55] By s. 63 of the Criminal Justice and Immigration Act 2008 it is an offence to possess an 'extreme pornographic image'. An extreme pornographic image is one which (1) is of such a nature that it must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal, (2) is grossly offensive, disgusting or otherwise of an obscene character, and (3) portrays, in an explicit and realistic way, any of the following: (a) an act which threatens a person's life, (b) an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals, (c) an act which involves sexual interference with a human corpse, or (d) a person performing an act of intercourse or oral sex with an animal (whether dead or alive).

[56] *Hansard*, 15 May 2006, Column 715W.

to that page not the entire MySpace network. The problem with ISP filtering of all types, including Cleanfeed, is that they simply block pages without explanation. The consumer simply receives an error message such as '404—page not found' or '403—forbidden'. There is no way for the consumer to differentiate between a page that you cannot see because the server is overloaded or has been relocated and one that has been blocked by the IWF.

Because of this, the practice of content filtering by the IWF and ISPs is not widely known or understood. Most UK internet users had probably not heard of the IWF at least that was the case until they became instantly famous in early December 2008.

Case Study Virgin Killer

In 1976 German band Scorpions released an album called Virgin Killer. The album has always been highly controversial as the cover art featured a naked prepubescent girl with a star of broken glass obscuring her genitals. The image has been widely circulated both offline and online for over thirty years, but sometime prior to 5 December 2008 it was reported to the IWF who determined that the image was illegal as being potentially in breach of the Protection of Children Act 1978. As a result on 5 December 2008, the IWF system started blacklisting a Wikipedia article and related image description page on the album. All major UK ISPs blocked access to the image and Wikipedia page.

This may have gone unnoticed as although popular, Scorpions remain a relatively obscure band in the UK, but for the peculiarities of the Wikipedia architecture. Wikipedia has a blacklist of its own which it uses to block individuals who have vandalised entries. As traffic to sites that are on IWF's blacklist is all channelled through Cleanfeed proxy servers it appeared to Wikipedia, once the page was blocked, that every visitor from the UK were coming from the same addresses. This block prevented UK users from amending Wikipedia pages, triggering an investigation by users and leading eventually to the discovery that this page had been blocked by the IWF/Cleanfeed. This immediately brought the IWF to public attention.

After Wikipedia instigated an appeal the IWF saw sense and on 9 December 2008 they removed the Wikipedia page and image from their blacklist stating that although 'the image in question is potentially in breach of the Protection of Children Act 1978 . . . the IWF Board has today (9 December 2008) considered these findings and the contextual issues involved in this specific case and, in light of the length of time the image has existed and its wide availability, the decision has been taken to remove this webpage from our list.'

The Wikipedia controversy has, it appears, done little to change the day to day workings of the IWF or the functioning of Cleanfeed. End users are still not aware why access to a website has been blocked and as the media fire surrounding the Wikipedia affair died down the IWF went back to its day to day role. More controversially government proposals for the policing of illegal file sharing have suggested a greater use of the ISP gatekeeper function, perhaps even so far as requiring ISPs to block internet access for customers found to be repeat offenders.[57] This is a highly controversial proposal which would see ISPs tasked with the job of policing illegal file sharing. If adopted it would see a two-stage approach: the first stage is a simple notification procedure which would require ISPs to inform customers that data had been gathered on them indicating they were involved in illegal file sharing. This is relatively uncontroversial (except for the question of cost) as it merely removes the need for a Norwich Pharmaceutical order thereby reducing the strain on the courts and the costs involved. Much more controversial are the measures relating to 'serious infringers'. At paragraph 4.23 the consultation proposes that: 'Ofcom should have a power to require ISPs to take technical measures (which will be specified in the legislation) against serious repeat infringers aimed at preventing, deterring or reducing online copyright infringement, such as: Blocking (Site, IP URL); Protocol blocking; Port blocking; Bandwidth capping (capping the speed of a subscriber's internet connection and/or capping the volume of data traffic which a subscriber can access); Bandwidth shaping (limiting the speed of a subscriber's access to selected protocols/services and/or capping the volume of data to selected protocols/services); and Content identification and filtering.' Although the media have widely reported that one option is disconnection of users this is in fact not the case as the proposal currently stands but paragraph 4.23 does indicate that future disconnection may be possible: 'It is entirely possible that the obligations on notification and collection of anonymised information on repeat infringers that may lead to legal actions taken by rights holders that we set out here will not, by themselves, deter some infringers. If that is established it is important that Ofcom should have the ability to take further steps to reduce copyright infringement significantly, in line with the long term objective'. This proposal is a half-way house between the stricter 'three-strike' laws seen in many countries which see an offender disconnected after two warnings and earlier UK proposals to have ISPs self-regulate. However it is packaged though it is clear that the gatekeeper function of the ISP is central to these proposals.

4.5 Regulators in cyberspace: states and supranational regulation

Of course it is not only private regulators who can utilise the architecture of the network to regulate end users. As Lawrence Lessig demonstrated states may use architecture-based modalities to control their citizens also. Most states use some form of filtering and/or content blocking. Australia is at the time of writing considering the mandatory installation of Cleanfeed filtering software,[58] while several other states use mandatory filtering or the operation of a State firewall to control access to content online. Probably the most famous example of this is the Chinese State firewall, colloquially known as 'The Great Firewall of China'. According to the Open Net Initiative 'China continues

[57] See Department of Business, Innovation and Skills, *Consultation on Legislation to Address Illicit Peer-to-Peer File Sharing*, 16 June 2009: http://www.berr.gov.uk/files/file51703.pdf.

[58] ABC News, *Conroy announces mandatory internet filters to protect children*, December 31 2007 http://www.abc.net.au/news/stories/2007/12/31/2129471.htm.

to expand on one of the largest and most sophisticated filtering systems in the world, despite the Government's occasional denial that it restricts any Internet content'.[59] The Great Firewall is kept constantly up to date and censors all types of comment with a particular focus on political and dissident speech. Major news organisations such as the BBC and Voice of America are blocked, along, not surprisingly, with the website of the *Epoch Times*.[60] The Ministry of Information Industry ensures the firewall remains secure by licensing a small number of ISPs, ten at the latest count, which for a country the size of China is an extremely small pool to police. These ISPs must ensure they comply with Ministry regulations, including new guidelines on video sharing sites issued immediately upon the widespread penetration of video sharing technology in China.[61] Underlying all regulation of the internet in China is an extensive list of proscribed content. Citizens are prohibited from disseminating between nine and eleven categories of content that appear consistently in most regulations;[62] all can be considered subversive and trigger fines, content removal, and criminal liability.[63] Because of the highly restrictive nature of state-based censorship in China much has been written about it[64] and systems and tools have been developed to subvert it.[65]

Despite this focus on China it is not the only State which uses filtering and blocking tools to control citizen access to the internet. Saudi Arabia for instance closely controls access. The authorities use a commercially available filtering tool allied to local government employees and reporting from ordinary citizens to aid the local implementation of the filtering regime. The Government makes no secret of its filtering, which is fully explained on a section of the ISU web site.[66] According to this, pornographic content is directly filtered by the State Information Services Unit, while other sites are blocked upon request from 'government security bodies'. The website also has forms through which internet users can request that certain sites be blocked or unblocked. In 2001 the Council of Ministers issued a resolution outlining content that internet users are prohibited from accessing and publishing. Among other things, it forbids content 'breaching public decency', material 'infringing the sanctity of Islam', and 'anything contrary to the state or its system'. The resolution also includes approval requirements for publishing on the internet and mechanical guidelines for service providers on recording and monitoring users' activities.[67] A new law, approved by the Saudi Shoura (Advisory) Council in October 2006, criminalises the use of the internet to defame or harm individuals and the development of websites that violate Saudi laws or Islamic values, or that serve terrorist organisations.[68] State based controls such as these are not unusual. The Open Net Initiative lists substantial filtering in a number of countries ranging from Bahrain to Yemen.[69]

4.5.1 WSIS and the IGF

With such a plurality of approaches and views on internet regulation and content regulation being displayed at national (state) level it is perhaps no surprise that until recently attempts to shape supra-national agreement on internet regulation were unsuccessful. Then in 1998 the International Telecommunications Union (ITU) recognised there was a need for supra-national cooperation on internet regulation. At their Plenipotentiary Conference in Minneapolis, that year they passed Resolution 73, which noted: that telecommunications were playing an increasingly decisive and driving role at the political, economic, social and cultural levels and called upon the United Nations: 'to ask the Secretary-General to coordinate with other international organizations and with the various partners concerned (Member States, Sector Members, etc.), with a view to holding a world summit on the information society'.[70] This request was heard at the ninetieth plenary meeting of the General Assembly of the United Nations in December 2001, where the General Assembly accepted and endorsed a proposal from the ITU that a World Summit on the Information Society

[59] http://opennet.net/research/profiles/china. [60] *ibid.*

[61] Xinhua News Agency, 'China to issue new regulations to censor online video programs', August 16, 2006.

[62] The nine types of content are: (1) violating the basic principles as they are confirmed in the Constitution; (2) endangering state security, divulging state secrets, subverting the national regime, or jeopardising the integrity of national unity; (3) harming national honour or interests; (4) inciting hatred against peoples, racism against peoples, or disrupting the solidarity of peoples; (5) disrupting national policies on religion, propagating evil cults and feudal superstitions; (6) spreading rumours, disturbing social order, or disrupting social stability; (7) spreading obscenity, pornography, gambling, violence, terror, or abetting the commission of a crime; (8) insulting or defaming third parties, infringing on legal rights and interests of third parties; and (9) other content prohibited by law and administrative regulations. Two categories of prohibited content were added in Art. 19 of the Provisions on the Administration of Internet News Information Services promulgated by the State Council Information Office and the Ministry of Information Industry on September 25, 2005. These two additional categories are (1) inciting illegal assemblies, associations, marches, demonstrations, or gatherings that disturb social order; and (2) conducting activities in the name of an illegal civil organisation. Translation at: http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

[63] Z. Jianwen, *The Current Situation of Cybercrimes in China*, International Centre for Criminal Law Reform And Criminal Justice Policy, December 2006: http://www.icclr.law.ubc.ca/china_ccprcp/files/Presentations%20and%20Publications/47%20The%20Current%20Situation%20of%20Cybercrime%20in%20China_English.pdf.

[64] See, e.g. G. Walton, *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China* (2001). R. Deibert, 'Dark Guests and Great Firewalls: The Internet and Chinese Security Policy' 58 *Journal of Social Issues* 143 (2002); A. Lin Neumann, *The Great Firewall: A CPJ Briefing:* http://planet.botany.uwc.ac.za/nisl/Scientific_methods/attachments/Great_Firewall.pdf.

[65] CBC News, *Software jumps China's firewall for news from Tibet*, March 20 2008: http://www.cbc.ca/arts/media/story/2008/03/20/tibet-firewall.html; P. Festa, 'Software rams great firewall of China', *cnet News* 16 April 2003: http://news.cnet.com/2100-1028-997101.html.

[66] http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm.

[67] Council of Ministers Resolution, Saudi Internet Rules, February 12, 2001: http://www.al-bab.com/media/docs/saudi.htm.

[68] Arab News, 'Shoura approves law to combat e-crimes', October 10, 2006: http://www.arabnews.com/?page=1&section=0&article=87941&d=10&m=10&y=2006.

[69] Substantial filtering is reported in Bahrain, Burma, China, Ethiopia, Iran, Libya, Oman, Pakistan, South Korea (in relation to security on the Korean peninsula), Saudi Arabia, Sudan, Syria, Thailand, Tunisia, UAE, Uzbekistan, Vietnam, and Yemen. They report no data on Cuba or North Korea but both are known to strictly control internet access.

[70] Resolution 73: http://www.itu.int/wsis/docs/background/resolutions/73.html. In effect what they were asking for was a UN Summit. Summits are designed to put long-term, complex problems like poverty and environmental degradation at the top of the global agenda. They are designed to provide leadership and to mould international opinion and to persuade world leaders to provide political support.

(WSIS) be convened, and instructed the Secretary-General of the UN to 'inform all heads of State and Government of the adoption of the present resolution'.[71] The WSIS was to take place in two phases, the first phase taking place in Geneva from 10–12 December 2003 and the second phase taking place in Tunis, from 16–18 November 2005. The objective of the Geneva phase was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake. The objective of the second phase was to put the Geneva 'Plan of Action' into effect and to find solutions and reach agreements in the fields of internet governance, financing mechanisms, and follow-up and implementation of the Geneva and Tunis documents. WSIS invited Heads of State/Government, International NGOs, and Civil Society representatives[72] to contribute to a series of preparatory meetings (PrepComms) and to the Geneva and Tunis rounds on a series of issues ranging from the digital divide,[73] to freedom of expression, network security, unsolicited commercial communications (SPAM), and protection of children.[74] Central to the WSIS programme was though the issue of internet governance.

WSIS envisaged a 'people-centred, inclusive and development-orientated Information Society where everyone can create, access, utilise and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life'.[75] Discussion as to how this was to be achieved began in the PrepComms. In these meetings numerous views were expressed about what was and was not 'internet governance', and the public policy involved. Some developing nations noted that they were unable to participate in many of the decision making processes central to management of the internet, such as management of the domain name system which was primarily in the hands of two American-based private regulators the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA).[76] Others, predominantly the US, called for the principle of private sector involvement and investment to be enshrined. In the final PrepComm briefing on 3 December 2003 US Ambassador David Gross outlined what he called the 'three pillars' of the US position.

[71] Resolution adopted by the General Assembly [on the report of the Second Committee (A/56/558/Add.3)] 56/183. World Summit on the Information Society, 21 December 2001.

[72] In UN parlance, civil society encompasses all those who are not part of government, private enterprise, or intergovernmental organisations: in other words private individuals.

[73] The 'digital divide' reflects the technology gap which has opened up between technology rich Western States and technology poor African and Asian States, and on the growing divide within States between the professional classes with stable and fast internet access and the working class, in particular immigrant communities, where access may be unstable, slow and difficult to obtain. See P. Norris, *Digital Divide: Civic Engagement, Information Poverty and the Internet Worldwide* (2001); M. Warschauer, *Technology and Social Inclusion: Rethinking the Digital Divide* (2004).

[74] For a discussion of WSIS see M. Raboy & N. Landry, *Civil Society, Communication and Global Governance: Issues from the World Summit on the Information Society* (2004).

[75] WSIS, Declaration of Principles, Geneva 12 December 2003, Principle 1.

[76] Further discussion of the domain name system and the role in particular of ICANN takes place in Ch. 12.

Highlight The US "Three Pillars" for ICT Regulation

1. As nations attempt to build a sustainable ICT sector, commitment to the private sector and rule of law must be emphasised so that countries can attract the necessary private investment to create the infrastructure;
2. The need for content creation and intellectual property rights protection in order to inspire ongoing content development; and
3. Nations must ensure security on the internet, in electronic communications and in electronic commerce.

Due to this divergence of views, when the Geneva Summit got under way the PrepComms had failed to produce agreement on the future development of internet governance. Although committed to a principle of multi-stakeholder agreement many developing nations, including China, Brazil, and most Arab States saw the US commitment to private sector initiatives as a barrier to progress while the US, and others including the EU, Japan, and Canada, feared that some governments wished to have a greater say in internet governance purely as a vehicle for censorship or content management. As a result agreement in Geneva proved impossible. Instead it was noted that: 'governance issues related to the internet are a complex challenge which needs a complex answer and which has to include all stakeholders—civil society, private industry and governments. No single body and no single stakeholder group alone is able to manage these challenges. This multi-stakeholder approach should be the guiding principle both for the technical coordination of the internet, as well as for broader public policy issues related to Cyberspace in general'.[77] To give effect to this recommendation, WSIS put together a Working Group on Internet Governance (WGIG) to report to the Tunis conference with recommendations. The group, chaired by Nitin Desai, Special Adviser to the Secretary-General for the WSIS, met four times between Geneva and Tunis, and published their final report on 18 July 2005.[78]

The group was asked to carry out their work under three broad heads: (1) to develop a working definition of internet governance; (2) to identify the public policy issues that are relevant to internet governance; and (3) to develop a common understanding of the respective roles and responsibilities of Governments, existing international organisations, and other forums, as well as the private sector and civil society in both developing and developed countries.[79] In dealing with the first the group suggested the following working definition: 'Internet governance is the development and application by Governments, the private sector and civil society, in their

[77] World Summit on the Information Society, *Visions in Process: Geneva 2003—Tunis 2005*, 41: http://www.worldsummit2003.de/download_de/Vision_in_process.pdf.

[78] Full details of WGIG may be found at http://www.wgig.org/.

[79] Taken from WGIG, *Report of the Working Group on Internet Governance*, Château de Bossey 18 June 2005, [5].

respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet'.[80] From this base the group then moved on to its second head of study and listed thirteen public policy issues 'of the highest priority'.[81] With this achieved the group than made its critical recommendations on the respective roles and responsibilities of governments, existing international organisations, and other forums. It recommended that governments were to drive public policymaking and coordination and implementation, as appropriate, at the national level, and policy development and coordination at the regional and international levels.[82] This was to include development of best practices, capacity building, and promoting research and development. The private sector meanwhile was called upon to develop policy proposals, guidelines, and tools for policymakers and other stakeholders, this including industry self-regulation and arbitration and dispute resolution.[83] To manage the relationship between the public and private sector (and other stakeholders) WGIG recommended the creation of a new Internet Governance Forum (IGF) which would provide the opportunity for the free exchange of ideas between stakeholders and which would provide public policy guidance.[84] The mandate for the new forum is set out in paragraph 72 of the Tunis Agenda for the Information Society[85] which states:

Highlight IGF Mandate

The Forum is to:

a. Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.

b. Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.

c. Interface with appropriate intergovernmental organizations and other institutions on matters under their purview.

d. Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities.

e. Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world.

→

f. Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries.

g. Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.

h. Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise.

i. Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes.

j. Discuss, *inter alia*, issues relating to critical Internet resources.

k. Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.

l. Publish its proceedings.

At the date of writing the IGF has met on four occasions with little in the way of hard policy emerging from the meetings. At the most recent meeting in Sharm El Sheikh in November 2009 the event reports made for depressing reading. The meeting considered a synthesis paper, *On the desirability of the continuation of the Forum*.[86] Although this ultimately (and fortunately) concluded that: 'the General Assembly, when deliberating on the Forum's continuation, should decide on its continuation for another five-year period. Following that period, another review of the desirability of a further extension should take place in the process of an overall review of WSIS outcomes,'[87] the prior deliberation was not without the identification of clear failures of the IGF process. As the report noted: 'One commentator suggested that the Forum had a long way to go in fulfilling the real objective for which it was established—to assist in the democratic development of global public policies and, if necessary, new institutions, in the area of Internet governance, in the spirit of the Geneva Declaration of Principles,'[88] while another 'wrote that the IGF had only fulfilled its mandate selectively'[89] while a third 'felt that the Forum had only just begun to fulfil its mandate and that the first years' activities had clarified the breadth and scope of work to be undertaken.'[90] Many felt the Forum to be too reactive noting that the Forum should be proactive in encouraging institutions involved in internet governance to debate and discuss by providing an open space specifically for such activities at its annual meetings, and that the IGF should take an adaptive approach to its work' and extend its focus to other areas affected by internet

[80] *ibid*, [10].

[81] These were: (1) Administration of the root zone files and system; (2) Interconnection costs; (3) Internet stability, security and cybercrime; (4) Spam; (5) Meaningful participation in global policy development; (6) Capacity-building; (7) Allocation of domain names; (8) IP addressing; (9) Intellectual Property Rights; (10) Freedom of expression; (11) Data protection and privacy rights; (12) Consumer rights; and (13) Multilingualism. Full discussion of these may be found at [15]–[27].

[82] *ibid*, [30]. [83] *ibid*, [31]. [84] *ibid*, [35]–[51].

[85] WSIS, *Tunis Agenda for the Information Society*, 18 November 2005: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

[86] IGF Secretariat, *On the desirability of the continuation of the Forum*, August 2009: http://www.intgovforum.org/cms/2009/synthesis_paper/K0952729.E.IGF.Synthesis.Paper.final.pdf.

[87] *ibid*, [99]. [88] *ibid*, [22]. [89] *ibid*, [23]. [90] *ibid*, [24].

policy and technology.[91] This chimes with earlier findings in the official publication reviewing the first two IGF meetings,[92] where Markus Kummer, eEnvoy of the Swiss Government, notes that: 'governments remain the decision makers'.[93]

The formation of the IGF is a step in the direction of cooperative supranational internet regulation, but the nature of the IGF as a forum to 'discuss public policy issues related to key elements of Internet governance' means it falls far short, currently, of playing a meaningful role in the regulation of the internet and digital content. Worse, the IGF though may never play a meaningful role in internet governance. The PrepComms provided an insight into why international cooperation at an operational level is unlikely to follow from discussion at IGF meetings. There is a digital divide between most developed and developing nations which means that there are different economic interests in play. Further, there appears to be a societal divide between the key states members of the IGF. The US in particular seems quite unshiftable on its twin positions of private sector investment and allowing the market to regulate. This is not acceptable to many nations including China, the other major states party at the IGF. Without agreement between these two digital superpowers the IGF will remain locked down and will prove to be merely a forum for discussion. This is not to belittle the potential contribution of the IGF which discusses open access, network standards, protection for freedom, and network stability and security, merely to say that the existence of the IGF does not change, and is unlikely to change, the established primacy of the nation state in internet governance.

4.6 **Conclusion**

What does all this mean for the study of cyber-regulation? The cyberpaternalists may argue that the effectiveness of filtering tools in countries such as China, Saudi Arabia, and Burma prove that by using legal controls to mandate changes the network architecture, either by filtering content or by restricting the ability of users to get online control may be effected in the digital environment. They may further point to the fact that when the IWF blacklisted the Wikipedia entry of *Virgin Killer* reports of the effectiveness of the Cleanfeed system ranged between 85–95% effective, demonstrating that even in democratic nations effective controls may be implemented at network architecture level. Cyber-libertarians may respond by citing that tools such as Peacefire.org's *Circumventor* software allow a large proportion of end-users in even the most regulated of states to circumvent state based controls.[94] The problem faced by cyberlibertarians is that it is impossible to deny that in each case the state *is* effectively controlling the online actions of their citizens, and that these controls may only be circumvented using specialist tools or with expert knowledge of computer networks. This is far removed from John Perry Barlow's claim that real world regulators 'do [not] possess any methods of enforcement we have true reason to fear'. The experience of the real world and the development of the Cyberpaternalist School seem to have consigned cyberlibertarianism to the pages of the history books. What of network communitarianism? Surely these real life examples of control implemented either at the network gatekeeper level or at state level undermine the network communitarian claim that 'regulation is a process of discourse and dialogue between the individual and society'? The network communitarian response would be that each of these real world examples can be perfectly rationalised with network communitarian thought. The UK *Virgin Killer* example is a perfect example of network communitarian regulation in action. Once the action of the IWF was brought into the public domain an extensive discourse took place and it only took four days for the block to be removed, this despite the assertion from the IWF that 'the image in question is potentially in breach of the Protection of Children Act 1978'. In other words the IWF still believe the image may be illegal to download and possess in the UK, but rather than fulfil their remit to 'minimise the availability of this (abusive) content' they chose to listen to the overwhelming view of British internet users that content of this type should not be blocked without consultation. This is network communitarianism in action. What about effectiveness of state level filtering though? Well if one looks at the lists of states which effectively filter at a state level we find that overwhelmingly they fall into one of two categories. The first are states where political discourse is routinely suppressed, states such as China, Burma, and Pakistan. The second are Islamic states where religious teachings forbid certain types of content, in particular anti-Islamic content or pornographic content. In each of these examples because political discourse is suppressed naturally in the real world we see a similar suppression of discourse in the online environment. Thus it appears one may choose to see the regulation in the digital environment in a similar fashion as regulation in the physical environment. It may either be centred, command and control regulation or it may be decentred and part of the democratic process. What is clear is that there is nothing particularly special about designing effective regulation in the digital environment.

FURTHER READING

Books

- L. Lessig, *Code Version 2.0* (2006).
- A. Murray, *The Regulation of Cyberspace: Control in the Online Environment* (2007)
- J. Zittrain, *The Future of the Internet and How to Stop It* (2008)
- J. Goldsmith & T. Wu, *Who controls the Internet?* (2006)
- L. Bygrave & J. Bing, *Internet Governance: Infrastructure and Institutions* (2009)

Chapters and Articles

- J. Reidenberg, 'Lex Informatica: The Formation of Information Policy Rules Through Technology' 76 *Texas Law Review* 553 (1998)

[91] *ibid*, [87]–[88].

[92] A. Doria & W. Kleinwächter, *Internet Governance Forum (IGF) The First Two Years:* http://www.intgovforum.org/cms/hydera/IGFBook_the_first_two_years.pdf.

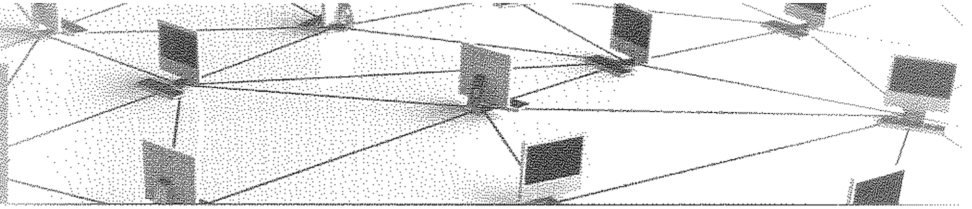
[93] *ibid*, 16.

[94] Festa, above n. 65; S. Olsen, 'Maxthon: China's hip browser' *cnet News*, 22 June 2006: http://news.cnet.com/2100-1032_3-6086632.html.

V. Mayer-Schönberger, 'Demystifying Lessig' [2008] *Wisconsin Law Review* 714

P. de Hert, S. Gutwirth., & L. de Sutter, 'The trouble with technology regulation from a legal perspective: Why Lessig's "optimal mix" will not work' in R. Brownsword & K. Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (2009)

5



Digital ownership

The law of property forms one of the central tenets of modern legal systems. The functioning of modern society, based upon principles of free markets and the ability to trade, requires that the legal system recognise rights in things as well as obligations between persons. Attempting to define property law, and property rights, is difficult in the physical world, but as we shall see is even more challenging in the digital environment where traditional values such as possession and rivalrousness are rendered ineffective by the limitless nature of bits.[1]

The starting point for any discussion of digital ownership is to examine how property law functions in the real world. Definitions of property differ but they all appear to have some elements in common. The first is that property defines a relationship between a person and a thing. Unlike obligations which normalise relations between persons, one tangent of the axis in a property relationship must be a thing. This is because property, and property law, regulate one's right to own, buy and sell, dispose, or destroy. These rights may only be exercised over things: it has been illegal to take rights such as these over persons in the UK for almost 200 years.[2] The second common theme of property law is that it is exclusive. The rights that property law confers upon the owner, or other rightsholder such as a lessee, are of the nature of rights *in rem* as opposed to rights *ad personam*. This means that the property rights holder has a right which may be exercised against any individual who attempts to interfere with his or her property right without the need for a prior relationship with that person. This may be contrasted with obligations which arise out of a prior relationship such as a contractual relationship or a relationship which establishes a duty of care in tort.[3] As James Penner explains in his book *The Idea of Property in Law*, the essential element of these rights is the right to exclude others from exercising competing rights over your property.[4]

We tend not to notice the monopolistic nature of property rights when we are dealing with everyday items such as cars, computers, or shoes as the monopoly one person exercises over *their car, their computer*, or *their shoes* cannot effect the wider market for shoes, cars, or computers, but when we are dealing with rare or unique items this becomes more apparent as with rare artworks such as L.S. Lowry's *A Fairground* which was kept

[1] Rivalrous and Nonrivalrous goods are discussed in Ch. 1, while at least some of the effects of digitisation and the limitless supply of bits are discussed in Ch. 3.

[2] Slavery Abolition Act 1833.

[3] See *Donoghue v Stevenson* [1932] AC 562.

[4] J. Penner, *The Idea of Property in Law* (1997), Ch. 4.