JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.1 (2013)

Code is Law? Assessing Architectural File Sharing Regulation in the Online Environment

Michael Filby, LLB, LLM, MPhil
School of Law
University of Hertfordshire

Abstract: Western legislatures tend towards the use of regulatory policies that favour strong intellectual property rights over public access in the battle to regulate file sharing. It has become apparent that the legislature is increasingly relying on code-based regulation in order to detect infringement, to identify those infringing, and to enforce the law through technical measures. This paper will assess the efficacy of regulation by code in the context of Lessig's assertion that "code is law", as applied to the file sharing community. The conclusion will reveal a significant asymmetry between the intended application of the regulatory influence of code and its de facto applicability in the online environment.

1. Introduction

Western legislatures are increasingly tending towards the use regulatory policies that favour strong intellectual property rights over public access in the battle to regulate file sharing. One of the ways in which such policies are being implemented is through the increase in the scope of the protections afforded in the digital age, specifically through the growing use of code-based regulation. The civil and criminal aspects of legislation largely operate as legal regulation imposed at the content level. But since the WIPO Treaty laid down obligations to protect digital rights management (DRM) and technical prevention measures (TPMs)[1], the regulatory latitude has increased its reach beyond the scope of the content level into the logical level. It has also become apparent that the legislature is increasingly relying on code-based regulation in order to detect infringement, to identify those infringing, and to enforce the law through technical measures. This paper will assess the efficacy of regulation by code in the context of Lessig's assertion that "code is law", as applied to the file sharing community. The conclusion will reveal a significant asymmetry between the intended application of the regulatory influence of code and its de facto applicability in the online environment[2].

2. Regulation Applied to the Institutional Ecology through Layering

The origins of the layers of regulation can be traced back to the seminal International Standards Organization / Open Systems Interconnection (ISO/OSI) depiction of layered architecture representative of the networked environment. The model presents seven layers that are organised hierarchically and depend upon one another in order to function. The seven layers, from top to bottom, are the application layer, the presentation layer, the session layer, the transport layer, the network layer, the data link layer and the physical layer[3]. Berners-Lee later demonstrated how the stack could be reformulated into a four-layered model, namely (again, from top to bottom) the content layer, the software layer, the computer

[1] This is embodied in the US by the Digital Millennium Copyright Act, and the UK by Arts 6 & 7 EU Copyright Directive which led to the required protections being added to the CDPA.

[2] Bambauer points out that "A generation of Internet scholars has sought to apply Lessig's New Chicago School modalities to regulatory problems. Yet, scholars have not acknowledged that these four forces are not merely ways of regulating – they also describe ways to *limit* regulation", at Bambauer DE, *Orwell's Armchair* (Research Paper No. 247, Brooklyn Law School 2011), 41. The assessment of the efficacy of regulation by code in this paper answers Bambauer's call by considering not only how the architecture of code is used to regulate, but also how it can be used to circumvent constraint, detection and enforcement.

[3] Comer DE, *Internetworking with TCP/IP principles, Protocols and Architecture* (4 edn, Prentice Hall 2004), 159.

hardware layer and the transmission medium layer[4]. By refining the ISO/OSI model, Berners-Lee effectively condensed the varied technical functions underpinning the online environment into a stack of software and hardware architectures that can more readily be considered in a regulatory context. The content layer broadly describes the end-user experience from the perspective of a user of the internet browsing the World Wide Web through a browser window, whereas the software layer is indicative of the internet protocol that allows the World Wide Web to function[5]. The computer hardware is indicative of the machines through which access is made and internet packets routed, whereas the transmission medium roughly describes the "wired" telephone system to which terminals are connected to access the internet[6]. Benkler refines the stack further still into a three-tiered environment[7] that he describes as the institutional ecology of the networked information environment[8]. The layers in Benkler's stack start at the top again with the content layer, which similarly encompasses the data and information that can be typically accessed by a user on an internet-connected device. The software layer is repurposed as the logical layer, but again encompasses the internet protocol that the World Wide Web is built upon. The lowest layer takes the bottom two layers of Berners-Lee's model and combines them into a single physical layer[9] encompassing the computer layer – namely, the machines that are connected to the internet, such as the user's PC and router – and the transmission layer that includes the hardware of which the internet itself is made up.

The majority of legal intellectual property regulation provided by the legislature is applicable at the content level, in that the granting of a monopoly right on informational content creates legal barriers that seek to prevent the end user from accessing, distributing, remixing, or carrying out any other action related to the work that has not been authorised by the rights holder. These legal barriers are artificial in the sense that they would not exist naturally in the digital environment, and thus they must be created and applied by the legislature. This becomes relevant when the interrelations between the hierarchies of the stack are considered[10]. It will be recalled that the ISO/OSI model and Berners-Lee's four-layered model are organised hierarchically, and are dependent upon one another to operate. The consequence of this is that each layer of the stack will always be capable of being influenced by the layer or layers below it, but not by the layer or layers above it. So in the case of Benkler's model of the institutional ecology, the content layer can be influenced by regulation on the content layer, the code layer and the physical layer. The code layer can similarly be influenced by regulation applied on the code layer and the physical layer, but regulation applied at the content layer cannot directly influence it[11]. Thus, the physical layer can only be influenced by regulation directly applied at that layer, but is unaffected by regulation applied to the upper layers[12]. To illustrate this rule in the context of intellectual property regulation, the legal construct of copyright tends to be directly applied at the content level[13]. With this in mind, it becomes clear why the legislature has become keen to apply regulation through the use of code to content that can be shared in the networked information environment. If regulation can be successfully applied at the code level, which by definition utilises the architecture of the internet, then the principle suggests that this would be more effective than the artificial barriers applied at the content level through direct legal regulation. In order to uncover why this has not proven to be the case, it is necessary to explore the code layer in more detail.

[4] Berners-Lee T, *Weaving the Web: The Past, Present and Future of the World Wide Web by its Inventor* (Texere Publishing 2000), 124 et seq.

[5] Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 384.

[6] Ibid. 384.

[7] Benkler Y, 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access' (2000) 52 Federal Communications Law Journal 561, 562.

[8] Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 395.

[9] Murray AD, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish 2004), 44.

[10] Bailey J, 'Of Mediums and Metaphors: How a Layered Methodology Might Contribute to Constitutional Analysis of Internet Content Regulation' (2004) 30 Manitoba Law Journal 197, 200.

[11] Lane TA, 'Of Hammers and Saws: The Toolbox of Federalism and Sources of Law for the Web' (2003) 33 New Mexico Law Review 115, 116.

[12] McTaggart C, 'A Layered Approach to Internet Legal Analysis' (2003) 48 McGill Law Journal 571

[13] Directly applied in this context means purely and directly through the application of rights, restrictions and enforcement at a purely legal level, applied to content or an end user. In the case of copyright, this will take the form of the rights given to the holder of the copyright granting them an exclusive monopoly to carry out certain actions with the work.

3. Regulating the Logical Protocols and Architecture of the Internet

One of the many motivations behind the formation of the internet was the desire for compatibility and interoperability. While communication was the driving factor, the US Advanced Research Projects Agency (ARPA) needed a network that was capable of effecting this communication between computers that were each built from differing hardware, and running software that was not inherently compatible with the software run by other computers. The solution to this problem was brought about by the development of the interface message processor (IMP). This was a form of black box that resided between the computer and the network, and acted as an interface that was capable of breaking down data into packets and sending them to other computers on the network via their IMPs through a series of hops. Although this sounds prima facie similar to roles undertaken by modern internet devices, modems and internet routers, the technique behind the packet transmission was in fact quite distinct. Although the system utilised packet switching, it had been designed in a time when computers were prohibitively expensive, and were thus used on a time-share basis. This meant that the system was designed to be reliable, but not expected to be slowed by congestion. Also, the fact that the packet-switching was handled by IMPs apart from the terminal meant that users had no real control over the network protocols[14]. In essence, the Network Control Program (NCP) was a closed system unsuited to managing a diverse set of traffic types or network loads[15]. A French researcher[16] sought to improve upon the design of the NCP over what had become known as ARPANET[17] and, with the funding of what was then known as the French Institut de Recherche d'lnformatique et d'Automatique (IRIA), designed an alternative network named CYCLADES. The key to the shift in the design ethic evident in CYCLADES was in the CIGALE packet switching network, which sacrificed some of the reliability of the NCP used by ARPANET by removing the verification of correct delivery in order to improve its efficiency. By changing the architecture of the packet-switching system so that the work was taken out of the network and placed in the hands of the host terminals, two key attributes present in the modern internet were born. These were the host-to-host principle of system design, and the layered architecture model which consisted of the data transmission layer, the transport layer and the application layer[18]. This openness allowed for a simplicity of design that provided a cheaper infrastructure, consisting of standard computers, that was vastly superior to ARPANET running NCP in that research was allowed to drive the evolution of network research and new technologies[19].

This was not lost on the researchers working to improve the NCP on ARPANET[20] who, with the assistance of one of the researchers who had originally worked with Pouzin on CYCLADES[21], went on to design the transmission control protocol (TCP) and internet protocol (IP) for ARPANET. This was based on the same open characteristics and design principles evident in CYCLADES and the CIGALE packet switching subnet[22]. Although fellow ARPANET researcher Roberts was sceptical of the value of moving the control of the network outside of the network itself and into the host computers in a public network[23], the TCP/IP protocol still forms the contemporary underlying structure of the internet[24]. The host-to-host principle at the heart of the design of TCP/IP that had been adopted from CIGANE/CYCLADES was described in a highly influential paper by the three former MIT researchers, Saltzer, Reed and Clark, as

[14] Roberts LG, 'Multiple Computer Networks and Intercomputer Communication' [1967] Proceedings of the First ACM Symposium on Operating System Principles 1, 3.1.

[15] Bennett R, *Designed for Change: End-to-End Arguments, Internet Innovation, and Net Neutrality Debate* (The Information Technology & Innovation Foundation 2009), 9.

[16] Louis Pouzin.

[17] Werbach K, 'The Centripital Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart' (2008) 42 University of California, Davis Law Review 343, 400.

[18] Bochmann GV and Goyer P, 'Datagrams as a public packet-switched data transmission service' (*Department of Communications of Canada*, March 1977) <http://www.rfc-editor.org/ien/ien17.pdf> accessed May 2012, 5.

[19] Pouzin L, 'CIGALE, The Packet Switching Machine of the CYCLADES Computer Network' (1974) Proceedings of the International Federation for Information Processing 155, 155.

[20] Vint Cerf, Robert Kahn, and Robert Metcalfe.

[21] Gerard Le Lann.

[22] Cerf V and Kahn R, 'A Protocol for Packet Network Interconnection' (1974) 22(5) IEEE Transactions on Communications 627, passim.

[23] Roberts LG, 'The Evolution of Packet Switching' (1978) 66(11) Proceedings of the IEEE 1, 3.

[24] TCP/IP systems took over from the last NCP hosts on ARPANET on 1st January 1983.

the end-to-end principle of network design[25]. The functioning of this principle in the context of TCP/IP can be thought of in terms of the three layers representative of the network. At the application layer is the application and software data and code that needs to be sent to other machines and received by the local machine. The protocol achieves this by taking the data into the transport layer and splitting it into small chunks known as packets[26]. The packets are then wrapped in a container of code that identifies where the packet has been created and what the destination is. The packets then, within the data transmission layer (i.e. the hardware, wires and radio spectrum that form the backbone of the network between hosts[27]), will individually begin hopping from node to node within the network until they arrive at their destination. The destination terminal will then utilise the protocol at the transport layer to remove the packets from their containers and reassemble them into a complete piece of code or instruction, where it re-enters the application layer[28].

Although this technically describes the internet, it was not until later that what has become known as the World Wide Web was developed on top of the TCP/IP protocol by Berners-Lee. What had been ARPANET had expanded greatly by this point, and had grown from a single closed network into an array of many networks that were interconnected so they operated as one. While working at the European Organisation for Nuclear Research (CERN), Berners-Lee designed and built a web that would run on top of TCP/IP protocols[29]. This included a browser that could access areas known as websites on what would become the World Wide Web that were written in Hypertext Markup Language (HTML), and served to end user terminals utilising HyperText Transfer Protocol (HTTP). This in itself formed an infrastructure. Like the TCP/IP protocols on which it relied to work, the World Wide Web was designed with a similar view to interoperability, compatibility and, crucially, with an open and end-to-end design ethic[30]. This mix of tools that allowed for web browsing and e-mail to become synonymous was then donated by CERN to the public domain, guaranteeing its continued openness[31]. This, along with the opening of the underlying network to the open market, spurred the World Wide Web to enter into ubiquity[32]. Together, the World Wide Web utilising the architecture of the internet saw a massive expansion in its online population during the 1990s, as the popularisation of the internet prompted businesses and the public alike to join what had become the digital revolution. As the end-to-end principle behind the design of the TCP/IP protocol had been preserved in the architecture of the World Wide Web, little had changed in terms of how data was transmitted[33]. Except now, the data at Berners-Lee's application layer could now also be content, which is why Benkler has repurposed this as the content layer. Any content that is capable of being rendered digitally and stored on a computer is now capable of being transmitted over the internet[34], such as, for example, a piece of music that has been converted into the mp3 format. Such an mp3 file is formed of data that can be split up into small data packets at the logical layer, or the code layer if Lessig's definition is to be preferred[35], and packed into a container that also holds the originating internet protocol (IP) address and the destination IP address. The data packet will then be passed into the

[25] Sometimes referred to as the e2e principle; see Saltzer JH, Reed DP and Clark DD, 'End-to-End Arguments in System Design' [1981] Second International Conference on Distributed Computing Systems, 509, 509; Reed DP, Saltzer JH and Clark DD, 'Comment on Active Networking and End-to-End Arguments' (1998) 12 IEEE Network 3, 69; & Lemley MA and Lessig L, 'The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era' (2000) 48 UCLA Law Review 925, 928.

[26] Bochmann GV and Goyer P, 'Datagrams as a public packet-switched data transmission service' (*Department of Communications of Canada*, March 1977) <http://www.rfc-editor.org/ien/ien17.pdf> accessed May 2012, 8.

[27] The data transmission layer is used here in the context of merging Berners-Lee's computer hardware layer and transmission layer.

[28] Ibid. 9; & Gralla P, *How the Internet Works* (Que 1999), 24.

[29] Sunstein points out that CERN unsuccessfully attempted to attract interest from private companies in the building of the World Wide Web, leaving Berners-Lee to take on the project independently: Sunstein CR, *Republic.com 2.0* (Princeton University Press 2007), 158.

[30] Berners-Lee T, Hendler T and Ora L, 'The Semantic Web' (2001) 5 Scientific American 35, 36.

[31] Murray AD, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish 2007), 72.

[32] Alesso HP, *Thinking on the Web: Berners Lee, Godel and Turing* (Wiley-Blackwell 2008), 64.

[33] Palfrey J and Rogoyski R, 'The Move to the Middle: The Enduring Threat of Harmful Speech to the End-to-End Principle' (2006) 21 Washington University Journal of Law & Policy 31, 57.

[34] Although the internet can specifically describe the network at the TCP/IP layer and the World Wide Web describes what we now view as "cyberspace", many commentators still also refer to the latter as the internet. As the World Wide Web runs within the TCP/IP layer, it is still technically part of the internet. Thus, these commentators are not at error, and so the internet will be occasionally used here to describe both the TCP/IP network and the World Wide Web as a whole.

[35] Lessig L, *The Future Of Ideas: The Fate Of The Commons In A Connected World* (Random House 2002), 48.

physical layer where it will hop from node to node through the network until it reaches the router or modem attached to the account associated with the destination IP address. This will pass the packet back into the code layer where the pieces can be reassembled and the container removed, before the completely reformed mp3 file is passed back into the content layer where it can be accessed by the end user. This broadly describes a greatly simplified version of the process that would take place if a user was to send an mp3 music file from their computer to another user over the internet.

4. Transposing Physical Architecture as Regulation to the Networked Environment

File sharing is frequently regulated through the application of legal barriers at the content level. From a purely technical point of view this means little, as barriers imposed by legal regulation at the content level can only be applied in an artificial sense that is separated from the concerns of the network[36]. However, as the popularity of the World Wide Web has continued to rapidly increase, it has been argued that regulation need not be restricted to being an artificial construct, but could also be applied at the logical layer in the guise of architectural design[37]. Reidenberg formulated this thesis as Lex Informatica[38]. Inspired by the mix of customs, norms and practices that formed what became Lex Mercatoria among European merchant seamen throughout the middle ages, Reidenberg observed that a similar blend of practice and conflicting laws could be shaped into an equivalent Lex Informatica on the internet using its plasticity[39]. Reidenberg took the theory much further than his analogy would have suggested by pointing out that regulation can not only be applied through the design of the internet, but that such regulation should be hard wired into the architecture of the network itself[40]. Further, the law should be used to provide backing for this. Lessig expanded upon this theory greatly, coining the concept that “code is law”[41]. Lessig observed the difference initially illustrated by Reidenberg concerning the distinction between regulation by law being influenced by government, and regulation by code being influenced by technologists, and categorised these as East Coast and West Coast law. While East Coast law traditionally takes a top-down approach to regulation, West Coast law tends towards taking a bottom-up approach[42]. However, although this often proves to be the focal point of conflict due to the technologists with whom West Coast law originates generally favouring openness and generativity over the restrictiveness preferred by the legislature, the two are not mutually exclusive. Just as regulation by code can be ordained by the legislature, so it can also receive legal backing. But if regulation at the code layer affects regulation at the content layer, it may be wondered why legal regulation does not take a back seat to regulation by code. The answer to this question lies in the underlying efficacy of how regulation by code can be applied to prevent users of the internet from engaging in file sharing, and how it can further be utilised to strengthen enforcement from the legal perspective.

[36] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 3.

[37] See, for example, Ibid. 1; & Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 17.

[38] Reidenberg JR, ‘Lex Informatica: The Formulation of Information Policy Rules Through Technology’ (1998) 76:3 Texas Law Review 553, 553.

[39] A term used by Licklider and Taylor to describe how, in the digital context, the medium through which information flows can be considered to be a programmable model that can be moulded to influence its outcome: Licklider JCR and Taylor RW, ‘The Computer as a Communication Device’ (1968) 4 Science and Technology 21, 22.

[40] Reidenberg, ibid.

[41] Lessig L, ‘The Limits in Open Code’ (1999) 14 Berkeley Technology Law Journal 759, 761.

[42] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 72.

5. Using the Law to Enforce Regulation by Code

5.1 The First Generation: Napster

The law has had some success in regulating file sharing through regulating against code itself. Its greatest achievements are centred on the legal battles against the peer-to-peer sites that started to appear at around the turn of the 21st century[43]. The first of these involved Napster. Napster was introduced as a US concern in 1999 as a centralised means of sharing files with other users on the Napster network, most commonly music in the form of mp3 files[44]. After registering on the website, client software could be downloaded and installed onto the end user's computer[45]. The client software would then index any music files that were stored in the shared folder on the user's computer. This index was then transmitted to the Napster server, where it was kept with the index files of all other users of the Napster network. A user would then be able to carry out searches through the client. These would involve entering the name of a track or artist into the search window, which would then prompt the search engine to check the indexes held on the central server for matches. The client would subsequently display any matches on the user's screen. When a file was selected, the client would then contact the host machine where the track was stored, which was usually a computer belonging to another individual user running the Napster client. The track would then be broken up and transmitted from the host computer to the computer of the user who had made the search[46] in a similar manner to the process described above. Assuming the user did not move the newly downloaded track out of their shared folder, it would then become indexed and available for other users of the network to download through the client. In the well-documented legal case that followed, it was the fact that Napster held a centralised index that ultimately led to the finding of liability for contributory infringement under the US Copyright Act[47]. But most significantly, it was the centralised architecture of Napster that allowed the network to be shut down with such relative ease[48]. By successfully ordering the central server to cease operation, the network became practically useless, and thus the computers of individual users who had Napster clients installed no longer operated as a file sharing network. Legal regulation, in the form of the order to close the central server, had successfully been used to regulate using code, in that the central server was removed from the network.

5.2 The Second Generation: Gnutella and FastTrack-based Networks

The second generation of peer-to-peer networks, including Kazaa and Grokster, moved away from the centralisation that has made Napster so technically and legally vulnerable[49]. In its stead was a largely decentralised network[50]. As with Napster, Kazaa required users to download client software from its website which created an index of all of the files[51] that the users had placed in their sharing folders. To make a search, a user would again submit a query through the client installed on their computer. However, instead of querying a central server, the client software would connect with a supernode[52]. Supernodes were in fact computers belonging to other users of the Kazaa network that the software had

[43] Johns describes the evolution of file sharing networks as being in three generations, that is, the first generation being Napster, the second being Gnutella and FastTrack-type networks like Morpheus, Grokster and Kazaa, and the third being BitTorrent, at Johns A, *Piracy: The Intellectual Property Wars from Gutenberg to Gates* (The University of Chicago Press 2009), 454.

[44] See David M, *Peer to Peer and the Music Industry: The Criminalization of Sharing* (Sage Publications 2010), 33; & Palfrey J and Gasser U, *Born Digital: Understanding the First Generation of Digital Natives* (Basic Books 2008), 132.

[45] Askanazi J and others, 'The Fate of Napster: Digital Downloading Faces and Uphill Battle' (2001) 13 Duke Law & Technology Review 1, para.5.

[46] Hence the term peer-to-peer.

[47] Ss.106, 115 & 501 US Copyright Act, 17 USC.

[48] David M and Kirkhope J, 'New Digital Technologies: Privacy / Property, Globalization and Law' (2004) 3(4) Perspectives on Global Development and Technology 437, 438.

[49] David suggests that the criminalisation of Napster drove the development of decentralised file sharing networks, at David, supra, 35.

[50] Askanazi J and others, 'The Fate of Napster: Digital Downloading Faces and Uphill Battle' (2001) 13 Duke Law & Technology Review 1, para.30.

[51] Not just music files, as with Napster.

[52] Hyland M, 'MGM v Grokster: Has the Copyright Pendulum Started to Swing Towards Copyright Holders?' (2005) 11(8) Computer and Telecommunications Law Review 232, 233.

deemed superior to other computers in the network due to factors such as connection speed and processing power[53]. Supernodes would be given responsibility of around 100 other users of the network, known as nodes. After the client software successfully connected with the supernode, the supernode would query the nodes it was responsible for with the searched-for term. The supernode would also transmit the search-term to another supernode which would carry out an identical query with its own nodes, and again send the search term onto another supernode. If the search-term was matched to a file hosted on a node, this would be communicated back to the user who made the search. If the user chose to download the file, their computer would link with the node hosting the file, and it would be transferred similarly to the cases described above. Although Kazaa and other file sharing networks using the FastTrack protocol are often described as decentralised networks, this is only partially true, as some centralisation took place. When the client software was initially downloaded, it would contain a preliminary list of supernodes in its cache. This list would be also be updated from time to time from the central server. However, only the initial list of supernodes was strictly necessary, as supernodes contained updated lists of other supernodes it was aware of that could be transmitted to users connecting to them in order to update their caches with functioning nodes[54]. Although these types of network do not have a critical point of failure, as the Napster network has in its central server, networks using the FastTrack protocol nevertheless suffered when their central points were removed, as with Kazaa and Grokster. Without a central server to keep a list of supernodes updated, new users of the network who have managed to obtain the client software from alternative sources have to suffice with the initial list of supernodes. Although the supernodes themselves carry updated lists, the gradually shrinking network will become less and less efficient until new users have difficulty locating supernodes, and those that remain only have access to nodes with a limited selection of files available for sharing. So, although the shutting down of Kazaa and Grokster did not have the same catastrophic effect on their respective networks, the combination of the weakened supernode updating and the migration of users to alternative networks eventually had the same effect of crippling the networks of their effective function[55]. Thus again, the legal regulation had successfully been utilised to regulate through the use of code[56].

5.3 The Third Generation: BitTorrent

After the second generation of peer-to-peer networks came a transition into completely decentralised networking, and with it a change in regulatory approach. Where code had successfully been used to target the backbone of the networks themselves, the pinnacle of the third generation of file sharing networks, BitTorrent, was designed to be effectively immune from this kind of interference[57]. A user wishing to download a file would again be required to install client software but, unlike with the previous generation of file sharing networks, the client software does not carry out indexing of files on their host computers, and searches are predominantly carried out outside of the network. When a user wishes to share a file, the most common way of doing so is through creating a torrent file. This file contains information that will allow BitTorrent clients to identify the relevant file being shared and a list of trackers associated with it[58]. Trackers are servers that keep lists of other computers running the BitTorrent client software that contain all or part of the relevant file. If a user wishes to find a file that is being shared within the network, the most common way of doing so is by searching the World Wide Web for a torrent file that relates to the content the user wishes to download. This can be done through a general search engine such as Google or Microsoft Bing, or through a website that is dedicated to indexing torrent files such as The Pirate Bay[59]. The user can then download the torrent file associated with the file they wish to download. Once run, the torrent file gives the client information on the file to be downloaded so that it can be identified, and

[53] Strowel A, *Peer-to-Peer File Sharing and Secondary Liability in Copyright Law* (Edward Elgar Publishing 2009), 2.

[54] Akester P, 'Copyright and the P2P Challenge' (2005) 27(3) European Intellectual Property Review 106, 111.

[55] For discussion on how scalability affects efficiency in peer to peer networks based on the Gnutella protocol, which shares several fundamental similarities with Kazaa, see: Javanovic MA, Annextein FS and Berman KA, *Scalability Issues in Large Peer-to-Peer Networks: A Case Study of Gnutella* (University of Cincinnati 2001), 7.

[56] Vincents OB, 'When Rights Clash Online: The Tracking of P2P Copyright Infringements Vs the EV Personal Data Directive' (2007) 15(3) International Journal of Law & Information Technology 270, 273..

[57] David, supra, 36.

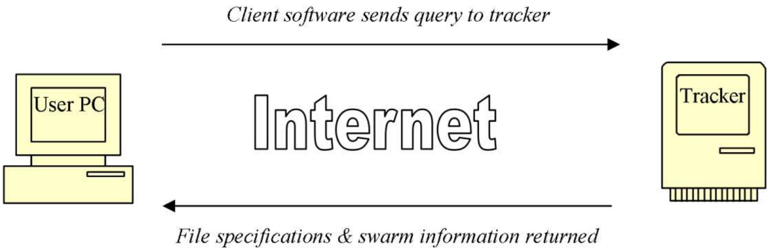
[58] Cohen B, 'Incentives Build Robustness in BitTorrent' (Wokshop on Economics of Peer-to-Peer Systems, University of Kansas, 22/5/2003), 2.

[59] Available at http://thepiratebay.se/ (accessed May 2012).

provides it with a list of trackers to connect to[60]. The client will then query the tracker with regards to the file, and the tracker will respond with the addresses of any hosts that contain all of the file (seeders), or part of the file (leechers).

Figure 1:

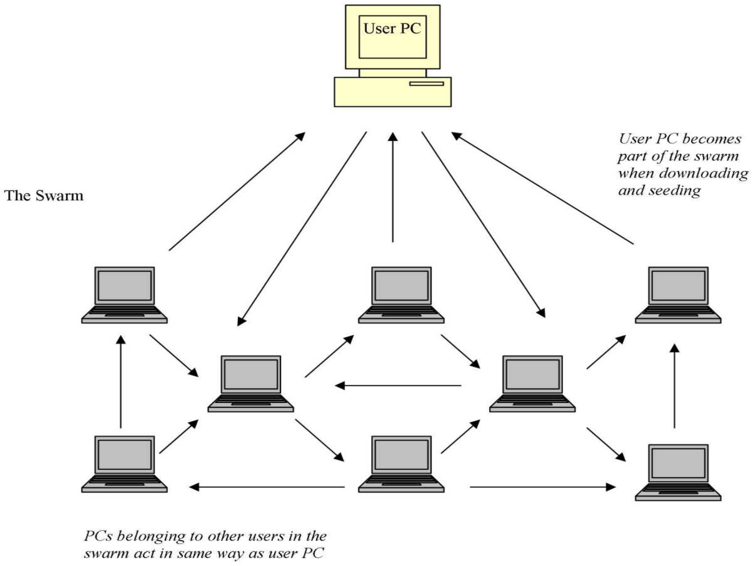
Activation of .torrent file


Client software sends query to tracker
User PC
Internet
Tracker
File specifications & swarm information returned

The client will then connect directly to any computers that contain all or some of the file, independently of the tracker. The clients on these computers then break up copies of whatever proportion of the file they are hosting into packets, and these packets are sent to the computer requesting the file. What sets BitTorrent apart from the networks described above is the distributed method it uses for getting the file to the downloader, as the only instance a complete file will be downloaded exclusively from a single seeder is if the seeder and downloader remain the only two computers in the web of computers uploading and downloading that particular file, which is called the swarm[61]. Often, another user will run the same torrent file before the first downloader has finished downloading a complete copy of the file. As they do so, their client will query the tracker which will pass on the details of both the original seeder and the new leecher, which is now seeding the packets that it has already downloaded from the original seeder. This new client will then enter the swarm by connecting to the original seeder and the first leecher, and will begin to receive different packets from the file from both computers. This too will begin seeding the packets it receives to other computers in the swarm as soon as it receives them.

Figure 2:

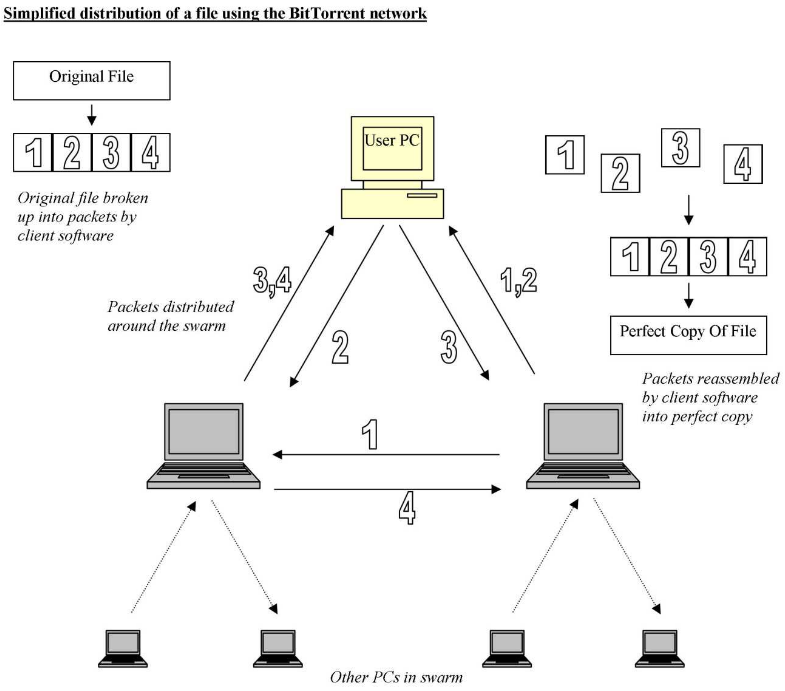
BitTorrent client software uploading & downloading


User PC
User PC becomes part of the swarm when downloading and seeding
The Swarm
PCs belonging to other users in the swarm act in same way as user PC

[60] Cohen, supra.
[61] Ibid, 1.

When a computer has received enough packets to form the complete file, the client software will reassemble the packets into a perfect copy of the original file, even though it may have received these packets from many different computers. The client will then continue to seed the packets that make up the complete file until the user intervenes or disconnects from the network.

Figure 3:


Simplified distribution of a file using the BitTorrent network
Original File
1 2 3 4
Original file broken up into packets by client software
User PC
1 2 3 4
1 2 3 4
Perfect Copy Of File
Packets reassembled by client software into perfect copy
3,4
1,2
Packets distributed around the swarm
2
3
1
4
Other PCs in swarm

Although there are many differences between the network architecture of BitTorrent and the previous generations of peer-to-peer networks described above, the most legally significant lies in the fact that the client software itself plays no role in the indexing and searching functions. Without the option to attack the network at client level, the next point of critical failure appears prima facie to be the trackers of unauthorised files. However, from a technical point of view, this is almost as challenging as attacking the supernodes in the networks that use the FastTrack protocol. Not only are they numerous, but they are also based in many different jurisdictions, which poses an obstacle to legal action[62]. Most significantly, the BitTorrent network is able to operate without trackers. Most recently, The Pirate Bay has begun phasing out the majority of the torrent files it hosts and replacing them with magnet links. These links (which are mere lines of code as opposed to files) contain far less information than torrent files, listing the metadata for the file to be downloaded and, if present, links to trackers. As magnet links take advantage of distributed hash tables (DHT), trackers are crucially not necessary. Instead, the client upon receiving the data contained in the magnet link will start querying other peers in the BitTorrent network using the metadata of the file that is being sought. The information that would normally be held by the tracker will be hosted by many different peers (hence the table being described as distributed) and, as soon as the client queries a peer that holds the DHT relating to the file, the client will be connected to the swarm that is sharing the file. Once connected to the swarm, the other seeders will provide the client with further information on other members of the swarm so that more and better connections can be made within the swarm. Thus, BitTorrent is not dependent on either trackers or traditional torrent files[63].

Although some success has been achieved in indirectly using regulation by code to impede file sharing by utilising the law to attack the weak points of the first two generations of file sharing networks, the third wave in the form of the BitTorrent network is proving more resilient. Without trackers or any

[62] As trackers are mere proxies as opposed to central servers, attacking them can be thought of as comparable to breaking up rhizomes only to propagate them further; see David, ibid, 63; and Deleuze G and Guattari F, *Anti-Oedipus: Capitalism and Schizophrenia* (Athlone Press 1984), 41.

[63] Dramatico Entertainment and others v British Sky Broadcasting and others [2012] EWHC 268 (Ch), para.24-25.

other critical point of failure to focus on, rights holders or law enforcement bodies have little option than to target either the indexing sites that host the torrent files and magnet links, or the users of the network itself. Although litigation against individuals alleged to be involved with the operation of The Pirate Bay website has so far resulted in criminal convictions, the site itself is still functional and regularly updated[64]. This is largely due to the moving of the hosting of the website to numerous jurisdictions that do not share the same approach to intellectual property regulation as the US and much of Europe[65], a task made less challenging by the space that the website takes up being dramatically reduced by the replacement of torrent files with magnet links. This and other websites are also capable of being hosted on what have been described as "PirateBox" units, which are mobile devices that are capable of broadcasting versions of any indexing site, including The Pirate Bay[66], to any other user within range of its WiFi signal. Although the fact that such devices are not only mobile but completely bypass the internet itself renders them even more difficult to trace than sites hosted on the World Wide Web, they are presently limited in range to their local areas. Development of the concept is aiming to allow users of Android smartphones to perform a similar function which could see the PirateBox concept become truly distributed and thus more widespread, which would place another obstacle in the path of the goal of preventing access to these indexing sites. Although targeting users of the BitTorrent network is also viable in legal terms, as was demonstrated in the case of *Chan Nai Ming*, it should be noted that this particular case was applied to an original uploader[67]. But in a purely technical sense, despite past successes, increasing decentralisation means the task of using legal regulation to apply code-based influence to the file sharing networks themselves at the logical layer is becoming increasingly impracticable[68].

6. Using Code to Enforce Regulation by the Law

But if the veins of the networks themselves cannot be stymied, what of the content that runs through them? The most direct application of code-based regulation to content is digital rights management (DRM)[69], which can take many different forms. May defines two categories of DRM, namely, soft and hard[70]. Soft DRM takes the form of software that is installed onto the computer of the consumer wishing to utilise DRM-protected content which then monitors the activity of the user. The most notable attempt at utilising soft DRM was carried out by SonyBMG, which bundled DRM software onto its compact discs that surreptitiously installed itself onto the computers of users who attempted to play them[71]. The software was technically indistinguishable from a rootkit in that it secreted itself on the computer of the user in a hidden area. When discovered, criticism was made of the fact that the software installed itself without the knowledge of the user, and that it made the user's operating system more susceptible to viruses[72]. It was also quickly rendered impotent by the hacking community, which cracked the software soon after it was discovered. The second type of DRM defined by May, hard DRM, is more common both

[64] Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v. Nell, Kolmisoppi & Warg (2009) (LJN: BK1067, 436360 / KG ZA 09-1809) (Amsterdam Court, Netherlands); Neij v Public Prosecutor, November 26, 2010 (Unreported) (HR (Stockholm)) (Sweden).

[65] Which Goldsmith describes as shifting sources of information flows, at Goldsmith JL, 'Against Cyberanarchy' [1998] University of Chicago Law Review 1199, 1222. See also Post DG, 'Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace' (1995) 3 Journal of Online Law 1, para.40.

[66] Aron J, 'PirateBox Lets You Share Files With Anyone Close By' (*New Scientist*, 2011) <http://www.newscientist.com/blogs/onepercent/2011/01/piratebox.html> accessed May 2012

[67] Discussed at Filby M, 'Big Crook in Little China: The Ramifications of the Hong Kong BitTorrent Case on the Criminal Test of Prejudicial Affect' (2007) 21(3) International Review of Law, Computers and Technology 275, passim; and Weinstein S and Wild C, 'The Copyright Clink Conundrum: Is Chan Nai Ming the Modern Day Josef K.?' (2007) 21(3) International Review of Law, Computers and Technology 285, passim.

[68] David argues that decentralisation of file sharing networks designed to facilitate greater anonymity for their users has been encouraged by the influence of the law, at David, supra, 37.

[69] In his assessment of the enforcement of intellectual property rights, Yu argues that DRM is a misnomer as is it more concerned with restrictions than rights, and suggests Government-Originated Legally Enforced Monopolies (GOLEM) as an alternative description, at Yu PK, 'Intellectual Property and the Information Ecosystem' (2005) 1 Michigan State Law Review 4, 6.

[70] May C, *Digital Rights Management: The Problem of Expanding Ownership Rights* (Chandos Publishing 2007), 67.

[71] Mulligan DK and Perzanowski A, 'Magnificence of the Disaster: Reconstructing the DRM Rootkit Incident' (2010) 22 Berkeley Technology Law Journal 1157, 2007.

[72] deBeer JF, 'How Restrictive Terms and Technologies Backfired on Sony BMG' (2006) 6(12) Internet & E-Commerce Law in Canada 1, 6.

in terms of use and in meeting the characteristics of what is traditionally thought of as DRM[73]. Hard DRM is usually encoded into content such as music files, and is designed to restrict access to the file without permission most often through the use of encryption[74]. A music file that has been encrypted cannot be played, but if the user has been provided with the key to the encryption because they have legitimately purchased the track, or if the encryption has been matched to the user's computer or playback device, then the file will be temporarily decrypted which will enable it to be played normally. DRM that uses encryption has two fundamental flaws. The first lies in the fact that a user who has permission to play the music file necessarily has to be given the key so that the file can be temporarily encrypted. The problem with this approach is that any encryption can be easily broken if the cracker has access to the key[75]. Thus, all DRM that uses encryption can be easily and quickly cracked. The second problem has been described as the analogue hole,[76] which refers to the fact that the encrypted file must be capable of being played by the authorised user. When a music file is played, the sound can be recorded[77], creating a DRM-free version of the file[78]. Thus DRM is less an effective a block to access as a brick wall in the physical world, and more of a keep out sign that requires "the buttressing of non-technological powers – states, norms, and laws – in order to remain effective"[79]. May argues that due to the weaknesses in this type of DRM that inevitably lead to its failure, hard DRM can only ever be considered to be a variation of soft DRM, serving little more than a monitoring function[80].

7. Using Code to Circumvent Surveillance and Detection

If code cannot be relied upon to directly prevent access, then performing a reliable monitoring function could theoretically, when combined with legal regulation, improve the application of enforcement. In order to take action (of a legal or technical nature) against an infringing user, the identification of the user must be successfully established along with the jurisdiction in which the infringement took place, and what particular infringement has occurred. This model of network regulability is described by Lessig as "who did what, where"[81]. This essentially describes the technical function that is intended to be carried out by the Digital Economy Act 2010, where rights holders are able to carry out a monitoring function that establishes all three of these criteria before the graduated response system is triggered. Enforcement of the Act is provided for with what are termed technical measures. These measures aim to curb file sharing by using what would be termed by Lessig as code to prevent the alleged infringer from utilising their account to access file sharing networks, or to reduce the efficiency of the networks themselves.

[73] May C, *Digital Rights Management: The Problem of Expanding Ownership Rights* (Chandos Publishing 2007), 67.

[74] Usually on a perpetual term; see Boyle J, *The Public Domain: Enclosing the Commons of the Mind* (Yale University Press 2008), 104.

[75] Doctorow attributes the speed at which most DRM is broken is being because: "all DRM systems share a common vulnerability: they provide their attackers with the ciphertext, the cipher, and the key. At this point, the secret isn't a secret anymore." Doctorow C, *Content: Selected Essays on Technology, Creativity, Copyright, and the Future of the Future* (Tachyon Publications 2008), 7.

[76] Woodford C, 'Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management' (2004) 75 University of Colorado Law Review 253, 275.

[77] Audio-visual tracks can be similarly recorded just as trivially.

[78] David describes further ways in which the DRM in music files can be defeated: "Strong encryption runs up against the fact that all currently available music in the world is available in non-encrypted format, as CDs are not currently encrypted. Even if every new piece of music were encrypted, it would only take someone to hold a microphone next to a speaker to make a recording of it." David, supra, 5. See also Boldrin and Levine, who identify the limits of DRM in the context of the analogue hole: "This goes to the technical weakness of all content-protection schemes – at some point, the purchaser will want to see the music or watch the video. What human beings can hear or see, technology can record. So what is next? Mandatory content protection for microphones? If a microphone detects a special copyright watermark, will it refuse to record the offending material? So, then we can't make home movies if our neighbor is playing loud copyrighted music next door?" Boldrin M and Levine DK, *Against Intellectual Monopoly* (Cambridge University Press 2008), 119.

[79] Johns A, *Piracy: The Intellectual Property Wars from Gutenberg to Gates* (The University of Chicago Press 2009), 506.

[80] May C, *Digital Rights Management: The Problem of Expanding Ownership Rights* (Chandos Publishing 2007), 103; May also observes that with the use of DRM, recorded file sharing only appears to decline marginally, ibid.

[81] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 39; Smith points out that this is based on the essential ingredients required to effectively prosecute individuals online, at Smith SM, 'Back to the Future: Crime and Punishment in Second Life' (2009) 36 Rutgers Computer and Technology Law Journal 18, 51.

These powers will be available for use in addition to the existing power provided in the Copyright, Designs and Patents Act 1988 to block access to indexing websites. The question of just how efficacious monitoring and enforcement measures such as these are in practice is crucial to the success of the ability of the overall regulatory regime to carry out its function. To address this, it must be considered how users and the piracy anti-industry can themselves utilise code in order to circumvent such measures.

7.1 Who is Infringing?

Rights holders presently use third parties to monitor file sharing networks such as BitTorrent. Establishing the identity of a file sharer requires the discovery of the internet protocol (IP) address of the infringer. IP addresses are assigned to everything that connects to the internet, and are crucial to the operation of the internet in that they form the addresses that data packets are given so that the TCP/IP protocol knows where to send them at the transmission and carrier level. In simple terms, a user without an IP address could not send packets (as there would no originating IP to assign them), and could not receive packets (as the network would not know where to deliver them). IP addresses are assigned in blocks to the ISPs that provide accounts to anyone wishing to access the internet, and the IP addresses in these blocks are assigned to each point of entry to the internet. To discover the IP address of an infringer, the rights holder can harvest these from individual BitTorrent swarms, for example by joining a swarm and scraping the tracker (which, it will be remembered, maintains lists of IP addresses of users currently sharing an individual file in a swarm)[82]. The IP address, once obtained, can be traced back to the ISP or other body to which it was assigned by carrying out a reverse-DNS lookup[83]. As ISPs keep logs of which user is assigned to which address at any particular point in time, the rights holder can then obtain the details of the account holder associated with the IP address at the time of the alleged infringement.

The technical problem with this form of detection is that it assumes that the user is connected directly to the swarm with his or her own IP address, but there are a number of ways that users can conceal their identities. For example, a user may connect to the swarm using a proxy server or by connecting to a virtual private network (VPN)[84], with such services usually being hosted extra-judicially to avoid legal sanction[85]. Once the connection to the VPN or proxy server is established, the user can access the internet and join torrent swarms in the usual way. However, it will appear to any website visited or any tracker in the swarm that the user's connection originates at the VPN or proxy, and thus has an IP address registered to the VPN or proxy server. The disadvantage from the perspective of the user is that VPNs and proxy servers that are available for use in file sharing networks often apply a charge for using bandwidth, although some free services are also available. Routing peer-to-peer traffic through a proxy or VPN can also result in a slower upload and download speed, but this is again an issue that varies greatly amongst services. In terms of surveillance, there is technically little that can be done to trace a connection beyond the VPN or proxy from which it appears to originate. Another similar option available to file sharers is a seedbox[86]. These operate similarly to VPNs in that they are networks that connect to BitTorrent swarms on behalf of users, the difference being that users do not have to be connected to the seedbox at the time of the transfer. This means the user can connect to the seedbox at a later time and download the file directly from it, thus leaving only the IP address of the seedbox with the swarm tracker[87].

True IP addresses are also hidden when utilising what are referred to as darknets[88]. One example of a darknet is provided by The Onion Router (Tor)[89]. After installing client software, the computer of the user

[82] Zhang C and others, 'Unraveling the BitTorrent Ecosystem' (2007) 22(7) IEEE Transactions on Parallel and Distributed Systems 1164, 1170.

[83] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 44.

[84] Kariyawasam R, 'Defining Dominance for Bits & Bytes: A New "Layering Theory" for Interpreting Significant Market Power?' (2005) 26(10) European Competition Law Review 581, 588.

[85] Many VPNs and proxy server services often do not keep logs of user IP addresses in order to further frustrate attempts at tracing their users.

[86] Chen X and Chu X, *Understanding Private Trackers in BitTorrent Systems* (Hong Kong Baptist University 2010), 4.

[87] Ibid.

[88] Different commentators apply the term "darknet" to different scenarios. For example, some describe peer to peer networks such as BitTorrent as darknets, whereas Biddle et al apply the term to file sharing networks that are not generally accessible to those not already within that community of sharers, at Biddle P and others, 'The Darknet and the Future of Content Distribution' (2002 ACM Workshop on Digital Rights Management, Washington DC, USA), 1; The combined application to an extra layer built into the internet and configured as a hidden service is the more generally accepted definition of the term, which will be used here.

can connect to a network of computers whereby identity is hidden through the use of a number of proxy servers that are donated by supporters of the Tor project. When a user wishes to use the Tor hidden service protocol, the client software can request access by connecting with a circuit that runs from the Tor network of proxies. This will provide the client with encrypted information that allows it to connect to other Tor proxies via the use of a distributed hash table (which is spread amongst nodes of the network much like in a BitTorrent swarm) and, eventually, to the hidden server. In the context of file sharing, a popular network that utilises the hidden service protocol is FreeNet[90]. The client software, when set to darknet mode, connects to the network of other users running the software in the manner described above, and can then access files that are being shared amongst them[91]. Unlike in a BitTorrent swarm, files are split up amongst the computers forming the FreeNet network, as opposed to being seeded as complete files by one or more clients. Due to the architecture of the hidden services protocol and the fact that downloading data through a relay of servers means that the speed of the operation will only be as high as the slowest connection speed of a computer in the network, file sharing through this tends to take longer to successfully complete than with a non-darknet network. However, in both of these instances, it is impossible to collectively harvest lists of IP addresses and link them to specific infringements. In the case of FreeNet running in darknet mode, it is more appropriately referred to as a friend-to-friend network as opposed to peer-to-peer, as the client will only connect to those specifically trusted by a community known to the user[92]. The use of a friend-to-friend community can be a double-edged sword in that, on the one hand, small friend to friend networks make infiltration less likely, but the smaller size of the group will increase the scope for identification of individuals once infiltration has taken place. On the other hand, while larger friend to friend networks increase the likelihood of infiltration, identification of individual members is more difficult as the group is larger[93]. In fact, the design of Freenet makes the larger network more attractive to file sharers due to the fact that the more nodes there are in a network, the more hops will take place when packets are delivered to the end user[94]. When an infiltrator is monitoring which packets are being delivered to which user, it cannot be determined whether the user another user is delivering packets to the end user, or merely just another intermediary node[95]. The packets themselves are also encrypted, adding a further layer of complication to the task of matching data packets to specific files.

An extra layer of anonymity can also be achieved by users utilising any of these types of file sharing networks by employing blocklists. Blocklists are lists of IP addresses that are known to belong to bodies that carry out network surveillance, often for the purposes of detecting file sharers. By importing updated blocklists into a BitTorrent client or by utilising a separate piece of software that sits between the user's computer and the internet in the same way as a firewall, connections to these bodies to the user's computer through file sharing networks can be refused. When Banerjee et al conducted a trial to assess the effectiveness of blocklists in peer to peer file sharing networks, they discovered that blocking the top five most active IP address ranges reduced the chances of connecting to an address belonging to a monitoring firm to 1%. Further reductions in the chance of detection were apparent when more ranges were added to the blocklist[96]. In contrast, it was found that without the use of blocklist filtering, the chance of a user connecting to a monitoring firm over the period of time that testing was carried out increased to 100%[97].

[89] Syverson PF, Reed MG and Goldschlag DM, 'Private Web Browsing' (1997) 5(3) Journal of Computer Security 237, 237.

[90] Clark I and others, 'Freenet: a Distributed Anonymous Information Storage and Retrieval System' in *Designing Privacy-Enhancing Technologies: Procedures of the International Workshop Design Issues in Anonymity and Unobservability* (Springer 2001), 46.

[91] David M and Kirkhope J, 'New Digital Technologies: Privacy / Property, Globalization and Law' (2004) 3(4) Perspectives on Global Development and Technology 437, 442.

[92] David M, *Peer to Peer and the Music Industry: The Criminalization of Sharing* (Sage Publications 2010), 83.

[93] Ibid, 84.

[94] A similar theory is the "Gnutella paradox", which posits that smaller networks are less subject to government control, but will equally be more difficult to find and contain fewer files to be shared, although this theory pre-dates the popularisation of BitTorrent: see Brown J, 'The Gnutella Paradox' (*Salon.com*, 29/09/00) <http://www.salon.com/2000/09/29/gnutella_paradox/> accessed May 2012; and Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2008), 123.

[95] Hand S and Roscoe T, 'Mnemosyne: peer-to-peer steganographic storage' (Proceedings of the First International Workshop on Peer-to-Peer Systems 2002), 1.

[96] Banerjee A, Faloutsos M and Bhuyan LN, *P2P: Is Big Brother Watching You?* (University of California 2006), 4.

[97] Ibid.

It will be remembered that Benkler's three layers of regulation – the content, code and physical layers – can only influence the layers below them, which is why surveillance applied at the content level can be circumvented with counter-surveillance applied at the code level. An even more effective way of hiding an IP address can therefore be achieved by bypassing the code layer and circumventing at the physical layer. In the physical world, this can be achieved by entering the internet through an access point that is not traceable to the user[98]. The most straightforward means of doing so would be to connect via an open WiFi signal. This would mean the activities of the user connected to the internet would be traceable, as a theoretical maximum, to the IP address that is registered to the company or individual that has left its access point unsecured, leaving no physical world connection between the two. Although connecting to an open WiFi connection would be the easiest option available to a user assuming such a connection was within range, a user who was extremely determined to avoid detection could connect through a secured wireless connection by bypassing any security measures applied by its owner. In architectural terms, weaker WEP WiFi security can be defeated by a user with the requisite technical knowledge within less than a minute[99]. The vulnerability of WPA/WPA2 security is more dependent on the strength of the password that has been used, with weaker passwords[100] being susceptible to dictionary attacks over a short length of time, and stronger passwords[101] being susceptible to brute force attacks over a longer amount of time[102]. Although this method of counter-surveillance is impossible to trace if the user carries out certain precautions[103], it can be construed in certain circumstances as a criminal offence[104]. This is in contrast to the other means of counter-surveillance described above which, considered independently of illicit activities carried out whilst using them, the use of which are not in themselves unlawful.

7.2 What is the infringement?

A number of problems associated with detecting infringement through BitTorrent swarms by harvesting IP addresses from trackers related to particular files were highlighted in the case of *MediaCAT v Adams*[105], which can largely be attributed to the evidential certainty of establishing that an individual IP address has been used to download a legally significant proportion of an unauthorised copy. This is because the IP address is taken from the tracker, but what data has passed to or from the user registered to the IP address has not been monitored. However, in *Chan Nai Ming*[106], it was deemed sufficient by the court when Hong Kong Customs and Excise connected to the swarm and downloaded complete copies. This method can be used to establish that an unauthorised copy exists in a swarm, but linking them to specific IP addresses can be problematic. Although the court accepted that the original uploader was liable despite there being a high possibility that parts of the files would have been downloaded by other users in the swarm[107], this was due to no meaningful effort being expended by him to hide his physical world identity[108].

[98] Wang W, *Steal This File Sharing Book* (No Starch Press 2004), 85.

[99] Taylor M and Logan H, 'Wireless Network Security' (2011) 17(2) Computer and Telecommunications Law Review 45, 45.

[100] For example, passwords that use plain English words from the English dictionary.

[101] For example, passwords that are long and comprise of characters that do not form words that are mixed in with numeric characters.

[102] The length of a brute force attack on a password is dependent on the speed of the CPU and GPU of a computer and the number of characters used in the password itself.

[103] The most important of which are the spoofing of the MAC address associated with the device with which the user connects to the wireless account, which would evidentially attach the user's network access device to the activity, and the encryption of internet traffic that travels through the unsecured network, in case another user of the network is monitoring network traffic and intercepts data that would identify the user in the physical world.

[104] See, for example, s.1 Computer Misuse Act 1990.

[105] [2011] EWPCC 006.

[106] *Hong Kong Special Administrative Region (HKSAR) v Chan Nai Ming* [2005] (unreported)

[107] Ibid, para.34.

[108] The defendant had uploaded the files using the IP address provided to him by his ISP, and had further linked his IP address to posts made on websites advertising the torrent files he had created.

Another more direct way of determining what users of the internet are downloading is by carrying out deep packet inspection[109]. This is a form of monitoring that can be carried out at the network and ISP levels, and thus can be considered to be implementable at the physical layer. It will be remembered from the explanations above that computers connected to the internet send and receive packets of data that are placed in a container indicating the originating IP address and destination IP so that the transmission carrier knows where to send it. By intervening at the point between the internet and the user, the packets can be intercepted and inspected[110]. The inspection goes past the shallow layers of the TCP/IP container levels, and into the data level of the packet which contains the content. Successful deep packet inspection can, in some circumstances, theoretically detect when the packets of data the user is sending or receiving are portions of an unauthorised copy, or from what file sharing networks they originate. This would trigger enforcement through legal regulation, or by regulating at a technical level by filtering out the prohibited packets[111]. Although there are legal ramifications of carrying out deep packet inspection at the ISP level[112], there are also frailties at a technical level. For example, if a user was connected to the internet through a VPN (as described above), traffic between the VPN and the user can be encrypted. By utilising VPN tunnelling, any data that is being uploaded or downloaded will go via the VPN which will securely encrypt the data stored in the packets before sending them directly to the user's computer where they will be decrypted and vice versa. Thus any data intercepted between these two points, such as at the ISP level, that is subjected to deep packet inspection will only reveal encrypted fragments of data. The body carrying out the monitoring will therefore be unable to determine what data the user is uploading or downloading unless the encryption is broken, which is both time consuming and hardware intensive. As deep packet inspection is usually put in place at the ISP level where it sits between the user's computer and the internet, it can be thought of as existing on the interface between the logical and physical layer. It can thus also be bypassed entirely by accessing the physical layer (i.e. the internet) via an account or access point that is not subject to surveillance.

7.3 Where is the Infringement Taking Place?

Assuming the identity of an individual file sharer has been established and the particular infringement recognised, the final step is to ascertain the location in which the infringement took place. This is a task similar in nature to determining identity in that it requires the analysing of the IP address of the user who is being traced. Much can be gleaned from something as simple as a reverse-DNS lookup[113], which can reveal the ISP the IP address is assigned to, and thus the likely location of the subscriber. This can be improved upon by cross-referencing the IP address against databases held by geolocation bodies[114]. Goldsmith and Wu assert that through combining these geolocation databases and subjecting them to computer analysis, "the geographical location of Internet users can be determined with over 99 percent accuracy at the country level"[115]. However, as geolocating involves the use of the IP address to which the user is connected to the internet, the process can be similarly frustrated by any of the measures outlined

[109] Jain S, 'The Promise and Perils of Deep Packet Inspection' (2009) 4(3) World Communications Regulation Report 33, 33.

[110] Williams R and Burbridge C, 'Net Neutrality and Deep Packet Inspection' (2008) 10(11) E-Commerce Law & Policy 11, 11.

[111] Lessig describes the promise made by one service advertised to business owners: "The Ipanema Systems "deep" layer 7 packet inspection automatically recognizes all critical business and recreational application flows running over the network. Real-time graphical interfaces as well as minute-by-minute reports are available to rapidly discover newly deployed applications." Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 55.

[112] The main obstacle lies in the E-Commerce Directive art 15(1) which prohibits requiring internet service providers to monitor the traffic of their subscribers.

[113] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 44.

[114] According to Lessig, to successfully derive a physical location from an IP address, "one needs to construct a table of IP addresses and geographic locations, and then track both the ultimate IP address and the path along which a packet has traveled to where you are from where it was sent. Thus while the TCP/IP protocol can't reveal where someone is directly, it can be used indirectly to reveal at least the origin or destination of an IP packet." Lessig, ibid, 58.

[115] Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2008), 61. Goldsmith and Wu go on to point out that refining the location to within the country-level, such as locating the user to being within a specific city, is "less reliable", at ibid, 62.

above that involve hiding the original IP address and substituting it for another[116]. For example, by connecting via a proxy server or VPN, attempts to geolocate the user utilising what appears to be their IP address would reveal the country the proxy or VPN was based in which, if hosted in a different territory, would not even accurately reflect the home country of the user[117]. Therefore, the location of the infringement can be determined at a country level only if the user has taken no measures to avoid such tracking or hide their identity whilst online.

8. Using Code to Circumvent Enforcement

8.1. Site Blocking

In addition to using code to monitor users of the internet in order to detect infringements, legal regulation can utilise several different means of using code to apply enforcement. It will be remembered from the discussion above that legal regulation can indirectly affect file sharing behaviour by influencing code. This has so far been evident in the successful suppression of the Napster first generation of file sharing networks, and the Grokster / Kazaa second generation. As the third generation, BitTorrent, as of yet remains relatively immune to the effective impediment of its network due to there being no critical points of failure that can be easily attacked, regulators have instead opted to target indexing sites by using a mix of legal sanction and enforcement by code. The US approach of attacking such sites has taken a two-pronged strategy. By ordering (or persuading) US-based (and thus controllable) firms that offer hosting, advertising or financial services to these websites to withdraw the use of their facilities from such sites, even if they are based overseas, the sites can be driven out of business[118].

The second prong has involved ordering US-based (and, again, controllable) bodies such as Verisign to redirect the domain name of indexing sites to another site, which involves manipulation of the domain name system (DNS)[119]. As has already been discussed above, websites hosted on the World Wide Web require an IP address so that browsers know where to connect in order to view them. As IP addresses are long strings of numbers that are difficult to remember, DNS allows more descriptive strings to be assigned to these IP addresses[120]. There are many DNS servers placed around the internet that hold a distributed database[121] of which domain names have been registered to which IP addresses. When a user types a domain into their browser, such as Google.com, the browser will connect to a DNS server to query what IP addresses are registered to that domain. As the database is distributed, the DNS server may refer the query onto another DNS server until it finds the correct domain. These DNS servers work in tandem under the auspices of a smaller number of root servers. When the correct domain has been identified, the IP address associated with it is sent back to the browser so that it can connect directly to the correct web site. In the US, Immigration and Customs Enforcement have “seized” a number of domains associated with alleged infringing websites[122]. This involves ordering Verisign, which is responsible for registrations under the .com top-level domain, to disassociate the domain names of infringing websites with the server on which they are actually based, and instead associate them with a website held by ICE that explains the domain has been seized. The US has sought to expand upon the legal power to perform this technical function with legislation such as the Stop Online Piracy Act, which would allow the DNS

[116] See, for example, Goldsmith J and Wu T, ibid, 62; and Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 59, where Lessig discusses the relative ease at which civil liberties activist Seth Finkelstein evades tracking through geolocation.

[117] See Johnson DR and Post DG, ‘Law And Borders - The Rise of Law in Cyberspace’ (1996) 48 Stanford Law Review 1367, 1371, where it is pointed out that the system is indifferent to the physical location of a connected computer.

[118] Ofcom describes this tactic as squeezing revenues, at Ofcom, '"Site Blocking" to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (Ofcom 2011) <http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf> accessed May 2012.

[119] Heverly RA, ‘Breaking the Internet: International Efforts to Play the Middle Against the Ends: A Way Forward’ (2011) 42 Georgetown Journal of International Law 4, 26.

[120] Froomkin AM and Lemley MA, ‘ICANN and Antitrust’ (2003) 1 University of Illinois Law Review 6, 12.

[121] I.e. not every server has a complete copy of a single database.

[122] Heverly points out that contrary to the insinuation of the vernacular, no actual seizure is made as a domain name cannot be held; at Heverly RA, ‘Breaking the Internet: International Efforts to Play the Middle Against the Ends: A Way Forward’ (2011) 42 Georgetown Journal of International Law 4, 26.

redirections to take place further down in the hierarchy than at the top-level domain. By requiring US ISPs to amend their DNS servers, rather than requiring Verisign to change the root server, the websites would only be blocked to users who access the internet through US ISPs. Also, websites that use top-level domain extensions outside of US control can also be affected. This is similar in nature to the blocking of the Newzbin2 website ordered to be carried out by the ISP BT in the UK[123], although this form of filtering does not involve tampering with DNS. The CleanFeed system employed by BT operates at the ISP level, and sits between the user and the wider internet[124]. As the user's software sends out data packets, these packets are intercepted by the CleanFeed system and subjected to packet inspection[125] to determine their destinations. The CleanFeed system carries a database of blacklisted IP addresses and URLs, which are checked against the destination of the packets. If the destination of any of the packets matches an IP address held in the database, the packet is forwarded to a secondary database of blacklisted URLs. If the destination of a packet matches the URL blacklist, the packet will be filtered out so that it cannot reach its end point. The practical consequence of this is that the user cannot connect to the blacklisted website[126].

These means of web blocking are effective in that users from the affected ISP or country will not be able to access the websites that are subject to the blocking measures[127]. However, there are countermeasures that can be employed by owners of the websites and the users to circumvent all of these types of blocking. In terms of blocking websites at the top level domain, many site owners choose to register a new domain utilising a top level domain from a different country that does not recognise the legal influence of the originating country. These new domains can then be advertised to their users so that access can be re-established. There is also software available to users to install in their web browsers that maintain a list of domains that have been blocked, along with alternative domains that have since been registered[128]. If the user attempts to visit a blocked domain by typing its URL into the address bar of their browser, the software will detect the blocked URL and replace it with the newly registered alternative URL or IP address[129]. If the blocking takes place at the DNS server level, then users can configure their computers to bypass ISP-level DNS servers in favour of DNS servers that have not been required to remove or redirect the listing for the blocked domain[130]. Software is available for users to install that automates this process, removing the need for the intermediate degree of technical knowledge that would otherwise be required. The browser software described above would also be able to successfully circumvent this type of block[131]. As the CleanFeed system does not rely on altering DNS to effect blocking, a slightly different approach to circumvention is required. If the blacklisted website sets up a number of alternative domains, the user can use the redirection software described above to automatically redirect to the site using URLs that have not been blacklisted before the CleanFeed database is updated[132]. The blacklisted URL can also be disguised utilising proxy services, which would again bypass CleanFeed's detection. Newzbin2 has also made software available for users to install that automatically bypasses the CleanFeed system. Finally, the user can set up an encrypted tunnel to a proxy or VPN from which the blacklisted site can be accessed. As the packets are encrypted between the user and the proxy, CleanFeed will be unable to carry out any inspection of them, and thus again be frustrated.

[123] See *Twentieth Century Fox Film Corp and Others v British Telecommunications Plc* [2011] EWHC 1981 (Ch).

[124] Clayton R, *Anonymity and Traceability in Cyberspace* (Technical Report No. 653, University of Cambridge 2005), 115 et seq.

[125] As the Cleanfeed system is only interested in the destination of the packets as opposed to the content of them, a form of shallow packet inspection is employed, not the deep packet inspection described above.

[126] Clayton, ibid.

[127] Clayton, ibid.

[128] Bambauer DE, *Orwell's Armchair* (Research Paper No. 247, Brooklyn Law School 2011), 42.

[129] Chaitovitz A and others, 'Responding to Online Piracy: Mapping the Legal and Policy Boundaries' (2011) 20 Commercial Law Conspectus 1, 261.

[130] Ofcom, '"Site Blocking" to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (Ofcom 2011) <http://www.scribd.com/doc/61521898/Ofcom-Site-Blocking-Report-With-Redactions-Removed> accessed October 2011, 33.

[131] Bambauer DE, *Orwell's Armchair* (Research Paper No. 247, Brooklyn Law School 2011), 42.

[132] Clayton R, *Anonymity and Traceability in Cyberspace* (Technical Report No. 653, University of Cambridge 2005), 123.

8.2 Technical Measures: Throttling / Disconnection

The DEA creates a new set of enforcement tools to be applied to ISP subscribers in receipt of three infringement notifications described as technical obligations, which UK ISPs can be required to put into place. These obligations are defined in the Act as limiting the speed or capacity of the internet connection of a subscriber (throttling), preventing the subscriber from accessing particular material[133], suspending the account of the subscriber (disconnection), or limiting the service in another unspecified manner. It is difficult to fully assess the ramifications of these technical measures without more details on what they specifically entail. For example, if preventing the subscriber from accessing particular material means blocking the use of file sharing networks such as BitTorrent, means of circumvention would depend upon whether traffic shaping was implemented by, for example, port blocking or packet inspection[134]. Suspending the account of the subscriber is a sanction that would take place at the physical layer in that the ISP would remove permission for the user to connect to the internet via their servers, and cannot therefore be circumvented through the use of code. However, as the removal of service is peculiar to the home account of the subscriber, it can be thought of as being effective at one particular interface between the logical and physical layers. As the internet itself is still available at all other access points, the user can still utilise other unaffected points of access to the internet[135]. To do this legally, the user could connect using a mobile data connection or seek permission to connect to the account of a WiFi network that is within range of their domicile[136]. Alternatives that would attract criminal sanctions if detected include connecting using unsecured WiFi without permission, or circumventing the security of WiFi that is password-protected.

9. The Threat of Plasticity to Design-Based Influence

The purpose of this paper has been to test the “code is law” thesis in the context of Lessig’s modalities of regulation. Both Lessig and Reidenberg have asserted that code is a crucial element of regulation, particularly in the context of regulating intellectual property rights[137]. Lessig in particular has emphasised the contrast between the imposition of legal barriers in the physical world and code barriers in the networked information environment – where legal barriers can influence behaviour through monetary fines and imprisonment, code barriers do not so much influence behaviour as prevent it entirely[138]. This rationale is explained by comparing the architecture or design of the internet to a door or wall in the physical world, so whereas legal sanctions are designed to influence your behaviour in order to avoid them, code barriers perform the virtual equivalent of physically preventing you from engaging in certain behaviour[139]. This analogy holds to a certain extent. It is true that a door can be circumvented by picking its lock or breaking it down, but the former requires specialised knowledge and equipment whereas the latter requires a great deal of strength. The circumvention of a digital lock in the form of DRM, for example, requires specialised knowledge. But the crucial difference lies in the fact that a digital lock can also be defeated by anyone without specialised knowledge as soon as a single person has broken it and shared the tool (in the form of software), or the information that can be used to defeat it without any specialised knowledge at all[140]. The same distributed dissemination of knowledge that makes file sharing possible also makes mass circumvention possible.

[133] Which appears to mean traffic shaping.

[134] Although it should be noted that both of these methods are easily circumventable by the user.

[135] Bambauer describes some of the numerous ways an attempt to close down internet access in its entirety in Egypt was circumvented, at Bambauer DE, *Orwell's Armchair* (Research Paper No. 247, Brooklyn Law School 2011), 41.

[136] Wang W, *Steal This File Sharing Book* (No Starch Press 2004), 85.

[137] Lessig L, ‘The Limits in Open Code’ (1999) 14 Berkeley Technology Law Journal 759, 761; & Reidenberg JR, ‘Lex Informatica: The Formulation of Information Policy Rules Through Technology’ (1998) 76:3 Texas Law Review 553, 582.

[138] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 121 & 124.

[139] Ibid.

[140] Doctorow recounts the true story of a mother who is “smart, college-educated, and knows nothing about electronics” who purchases a legitimate copy of a DVD for a her children. When she attempts to copy the DVD to VHS for her children to use without damaging the original, she is unable to do so due to the Macrovision copy-protection DRM. Although the technically knowledgeable would be able to circumvent the DRM utilising a particular type of cable, the mother instead learns about file sharing networks that offer copies of movies that contain no DRM. Thus the ease at which file sharing networks can be accessed and the menu of digital goods on offer that are superior

The plasticity of the end-to-end architecture of the internet allows the regulator to customise its approach to regulating the online environment, but this is a double-edged sword[141]. While information flows can be shaped, diverted and blocked by the imposition of digital barriers, this paper has demonstrated that the same architecture allows for it to be remoulded so that efficiency of the flows remains optimal. Several commentators argue that this equality of design can be construed as a logical commons, in that the network does not discriminate[142]. This is accurate in that the ability to make use of the internet without encumbrance at the logical layer is equally available to all in terms of opportunity. But there exists a digital divide in which, on one side, exists an online citizenship that have the means, the knowledge, the will and the ability to seize this access[143.] On the other lies a group that may not have the desire to take advantage of the networked information environment, or certain aspects of it. But the proportion of this group that does not have the opportunity to acquire the knowledge or ability is diminishing, due to the increase in efficient dissemination and access[144]. Further, this efficiency in dissemination is being driven not only by network design, but by the intended use of code as an impediment to it[145]. It is this equality of opportunity that forms the logical commons.

Although the fear that blocks implemented at the code layer may lead to censorship is acknowledged[146], Reidenberg suggests that the possibilities of circumvention of the Lex Informatica default can be reduced by "forcing the technical rule lower in the network protocol"[147]. This suggestion of hardwiring barriers into the architecture of the internet would realise Lessig's analogy to the extent that they would become as impenetrable as a door or wall in the physical world. But the end-to-end design of the internet requires intelligence only at the ends of the networks, with the "dumb" middle a mere medium through which packets are transmitted[148]. Currently, it is the intelligent ends that are being manipulated in order to circumvent the barriers that are constructed in open code layers accessible and mouldable by open terminals, i.e. PCs[149]. To integrate barriers more deeply into the stack would be to

to the authorised versions have allowed a person with no specialist knowledge to circumvent DRM; at Doctorow C, *Content: Selected Essays on Technology, Creativity, Copyright, and the Future of the Future* (Tachyon Publications 2008), 8-9.

[141] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 127.

[142] See, for example, Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 412; Lessig L, *The Future Of Ideas: The Fate Of The Commons In A Connected World* (Random House 2002), 48.

[143] Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 236. Palfrey & Gasser describe the digital divide as a participation gap, at Palfrey J and Gasser U, *Born Digital: Understanding the First Generation of Digital Natives* (Basic Books 2008), 14.

[144] May points out that peer-to-peer file sharing is slow, time-consuming and beyond the technical abilities of many, at May C, *Digital Rights Management: The Problem of Expanding Ownership Rights* (Chandos Publishing 2007); but David argues that amongst the core demographic of the music industry, this is no longer the case, at David, supra, 88.

[145] The story recounted by Doctorow, supra, illustrates how a barrier to access can trigger the user to route around it. Another example is highlighted by Clayton in his Technical Report on CleanFeed, the packet filtering system used by ISP BT. The Internet Watch Foundation (IWF) has for some time maintained a list of websites that contain child pornography. CleanFeed was originally put in place by BT with the intended purpose of blocking attempts by its subscribers to access the blacklisted URLs contained in the IWF database. Due to the relative moral certainty behind the blocking of child pornography, the circumvention of CleanFeed has only been subject to analysis by a niche of curious technical experts who have no interest in making it easier to circumvent. However, by increasing the reach of CleanFeed to include websites that make it easier to share copyrighted material, the size of the audience of those who wish to circumvent the filter increases significantly, and changes the motivation of the technical experts in this group from curiosity to direct desire to circumvent: "Although legal and ethical issues prevent most experimentation at present, the attacks are extremely practical and would be straightforward to implement. If CleanFeed is used in the future to block other material, which may be distasteful but is legal to view, then there will be no bar to anyone assessing its effectiveness. It must be expected that knowledge of how to circumvent the system (for all material) will then become widely known". Clayton R, *Anonymity and Traceability in Cyberspace* (Technical Report No. 653, University of Cambridge 2005), 147; For more on the IWF, see Akdeniz Y, 'Internet Content Regulation: UK Government and the Control of Internet Content' (2001) 17 Computer Law and Security Report 303, 303.

[146] See, for example, Weinberg J, 'Rating the Net' (1997) 19 Hastings Communications and Entertainment Law Journal 453, 455.

[147] Reidenberg JR, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76:3 Texas Law Review 553, 582.

[148] Palfrey J and Rogoyski R, 'The Move to the Middle: The Enduring Threat of Harmful Speech to the End-to-End Principle' (2006) 21 Washington University Journal of Law & Policy 31, 57.

[149] Zittrain argues that the crucial element of the success of the PC lies not only in cheap components, but also in its ability to produce generative programming and repurposing, at Zittrain J, *The Future of the Internet: And How to*

transcend the intelligent ends where regulation by code is usually implemented[150], and would thus require the orchestration of fundamental changes to the internet protocol[151] so that the middle can become intelligent enough to itself be coded to discriminate[152]. But it is warned that to change the internet protocol is to destroy the networked information environment as it now exists[153.] The protocols of the internet were deliberately designed to accommodate the end-to-end principle so the underlying network could be as open and mouldable to future technologies (one of which was the World Wide Web) as possible[154]. Lessig points out that "This minimalism in the Internet's design is not an accident. It reflects a decision about how best to design a network to perform a wide range over very different functions".[155] Goldsmith and Wu go further than this in describing the "open, minimalist, and neutral" design of the internet as distrusting of centralised control, which was an embodiment of "American libertarianism, and even 1960s idealism, into the universal language of the Internet"[156.] If the internet was deliberately designed this way, then any proposed change to its infrastructure must be questioned[157]. In the case of an admired ecosystem, the burden of proof must fall on those seeking to alter the fundamental assumptions that brought it about in the first place[158.] Goldsmith and Wu proclaim that Vint Cerf's assertion that there is something necessary or unchangeable about the architecture of the internet is a mistake[159]. This point of view is described by Lessig as "is-ism", that because technology is plastic and mouldable, the way something is is not necessarily the way it should be[160.] Lessig justifies his point of view by highlighting Zittrain's observation that the generativeness of the end-to-end network is good for creating technologies such as Hotmail and Google, but just as good for creating viruses, a view that he describes as "Z-Theory"[161.] This is correct insofar as it cannot be assumed that the positive effects attributable to the architecture of the internet in themselves justify their continued existence, but it must also not be assumed that just because the undefined threat that lies at the heart of Z-Theory can potentially technically be created by the same principles, that they necessarily will. To frame the argument in the spirit of Lessig's own theory of is-ism, just because a threat can potentially materialise, it does not necessarily mean that it will[162].

Stop It (Penguin 2009), 19; Benkler describes attempts to bind the openness of PCs with proprietary operating systems as a symptom of enclosure in the institutional ecology. at Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 395 & 409.

[150] Described by Murray as leveraging control into the carrier layer, at Murray AD, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish 2007), 87.

[151] Reidenberg JR, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76:3 Texas Law Review 553, 577.

[152] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 44.

[153] Lessig describes that if the core TCP/IP protocols were required to change, "you'd break the Internet." Ibid. 143. According to Doctorow, "You could stop spam by simplifying email: centralize functions like identity verification, limit the number of authorized mail agents, even set up tollbooths where small sums of money are collected for every email… If you did all these things, you'd solve spam. By breaking email." Doctorow goes on to liken this situation with DRM which he compares with Trusted Computing, and points out that burdening a complex ecosystem with centralised verification would similarly be "razing the rainforest". Doctorow C, *Content: Selected Essays on Technology, Creativity, Copyright, and the Future of the Future* (Tachyon Publications 2008), 190-194. See also Heverly RA, 'Breaking the Internet: International Efforts to Play the Middle Against the Ends: A Way Forward' (2011) 42 Georgetown Journal of International Law 4, 27.

[154] See Clark DD, 'The Design Philosophy of the DARPA Internet Protocols' (1988) 18(4) Computer Communication Review 106, 106-108; and Hafner K and Lyon M, *Where Wizards Stay Up Late: The Origins of the Internet* (Simon and Schuster 1998), 147.

[155] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 44.

[156] Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2008), 23. This attitude was not peculiar to either the US nor the 1960s though, as Berners-Lee's embracing of them when creating the World Wide Web in Europe, and ultimately donating it to the public domain, indicates: Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 412-413.

[157] Ackerman B, *Social Justice in the Liberal State* (Yale University Press 1980), 174.

[158] Brin D, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Perseus 1999), 324. See also Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 78; & Boyle J, 'The Second Enclosure Movement and the Construction of the Public Domain' (2003) 66 Law and Contemporary Problems 33, 43.

[159] Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2008), 58.

[160] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 32.

[161] Ibid, 74; Zittrain JL, 'The Generative Internet' (2006) 119 Harvard Law Review 1974, 2010-2012.

[162] As Lessig himself acknowledges, where uncertainty is high, end-to-end design maximises the value of a network: Gaynor M, 'A Real Options Framework to Value Network, Protocol, and Service Architecture' (2004) 34(5) ACM

So far, this paper has explored the influence of the legislature in attempting to regulate informational flows in the networked information environment, and the consequence of technological end-to-endian plasticity in the application of this regulation. We have seen that the regulator uses code in two distinct ways, namely, to act as a substitute for or extension of legal regulation (i.e. code as law), and as a bolster for regulability in terms of surveillance. These uses on both counts are, on a technical level, ineffective. However, it has been argued that technical ineffectiveness of regulatory code need not defeat the purpose of it[163]. The theory of bovinity posits that "tiny controls, consistently enforced, are enough to direct very large animals… I think it is as likely that the majority of people would resist these small but efficient regulators of the Net as it is that cows would resist wire fences"[164.] Framed in the context of a largely self-executing structure, the driving force of the theory lies in the assertion that the average person will have neither the time nor patience to circumvent structural barriers, and will thus default to a desired course of conduct[165.] Hull suggests that the inconvenience of circumventing DVD copy protection will prevent even those who are technologically adept and unconcerned about breaking the law from circumventing DVD DRM[166,] whereas Sydnor observes that the theory of bovinity casts the government in the role of the wise regulator, able to defend users of the internet against threats from malevolent market forces and rules[167.] But this highlights a crucial flaw: "Lessig's 'bovine account' of human nature equates most people with witless cows"[168.] Sydnor et al contextualised the theory with a data set that indicated that the architectural design of file sharing software significantly raised the incidence of uploading for a short period, before it was greatly reduced again. This suggests that the users of the software in this example were not as willing to allow their behaviour to be shaped as the theory of bovinity would dictate "given time, information, and incentives"[169,] which lends further support to the assertion that Lessig's assumption is without foundation. This scepticism is shared by Doctorow, who categorises the two flaws in the "fallacy" behind the theory as technical and social. In the former sense, a user does not require the technical knowledge necessary to circumvent the surveillance or control, merely the ability to locate the knowledge on how to achieve circumvention from another person[170.] In the latter sense, small controls are designed to influence "the most unsophisticated and least capable among us"[171]. That the file sharing community is defined by a joint purpose of obtaining and sharing free copies, and has gone to great lengths to establish an infrastructure that enables its members to achieve this aim, does not fit in with the characteristics described by Doctorow, and thus undermines the theory further still. As Froomkin suggests, bovinity "only works so long as there is no particular felt need for what is being blocked, and no one is providing instructions on how to circumvent the blocks. The example of DVD region codes suggests to me that bovinity is overrated"[172.]

SIGCOMM Computer Communication Review 42, 42 et seq; & Baldwin CY and Clark KB, *Design Rules*, vol 1 (MIT Press 2000), 234.

[163] See, for example, Goldsmith JL, 'Against Cyberanarchy' [1998] University of Chicago Law Review 1199, 1229.

[164] Lessig L, *Code Version 2.0* (2nd edn, Basic Books 2006), 73.

[165] Cheng EK, 'Structural Laws and the Puzzle of Regulating Behavior' (2006) 100 Northwestern University Law Review 655, 664-665;

[166] "So we all watch the commercials", Hull G, 'Coding the Dictatorship of 'the They:' A Phenomenological Critique of Digital Rights Management' in Wisnewski JJ and Sanders M (eds), *Ethics and Phenomenology* (Lexington Books 2011), 29.

[167] Sydnor TD, 'Tragedy and Farce: An Analysis of the Book Free Culture' (2008) 15.5 Progress & Freedom Foundation Progress on Point 1, 6.

[168] Ibid.

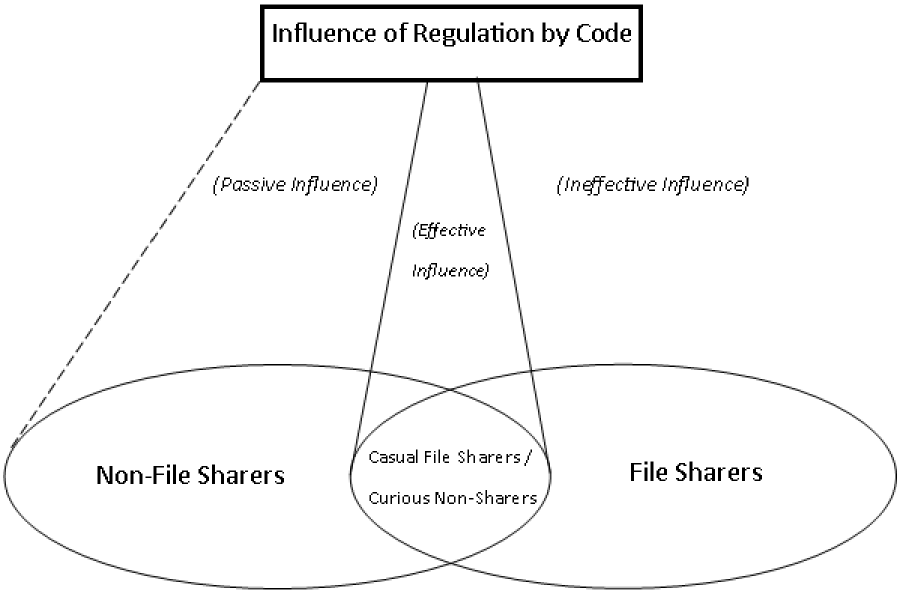
[169] Sydnor TD, Knight J and Hollaar LA, *Filesharing Programs and 'Technological Features to Induce Users to Share': A Report to the United States Patent and Trademark Office from the Office of International Relations* (U.S. Patent and Trademark Office 2006), 51.

[170] Doctorow C, *Content: Selected Essays on Technology, Creativity, Copyright, and the Future of the Future* (Tachyon Publications 2008), 8.

[171] Ibid.

[172] Froomkin AM, 'Toward a Critical Theory of Cyberspace' (2003) 116(3) Harvard Law Review 749. 780.

Figure 4: **Influence of Regulation by Code over Online Communities**



The above figure demonstrates the extent of the impact of code, and thus legal regulation that relies upon it, on the behaviour of two simplified representations of online sub-communities based on the outcome of the above assessment of bovinity. Where a group chooses not to engage in file sharing, regulation by code exerts control that is effective insofar as the group does not engage in file sharing, but passive in that the group exhibits no desire to do so in the first place. Where a group does choose to engage in file sharing then, assuming they meet the characteristics necessary to be part of the file sharing community, they will be likely to possess the desire, the will and the ability to circumvent the surveillance or enforcement measures of code to the extent that they will not allow minor inconvenience to sway their behaviour. The overlap between the two groups represents non-file sharers who are showing a mild curiosity about file sharing, and the most casual of file sharers who do not share the intense motivations or drive of their community. This group is the most susceptible to being influenced by the inconvenience of circumvention, and thus will be the most likely to become non-file sharers. In a sense, Lessig's bovinity is correct to a point, as this sub-section of the online community is positively influenced successfully by code. However, the theory falters in that the demographic over which code has the least effect is the same demographic that the regulator is most actively targeting; namely, the file sharing community. Thus, any legal regulation that relies on code to detect infringement or apply sanctions is liable to the same weaknesses that code itself is subject to, and will hence be limited in its ability to influence norms of file sharing to any meaningful degree[173].

10. Conclusion

The two positions defined in this paper of this modality of regulation illustrate the two policy approaches available for the regulator to take in the institutional ecology. On one side there is openness, as characterised by Benkler as the TCP/IP protocol and the peer-to-peer networks that operate on top of them[174]. This is the approach that has been taken by the architects of the internet, the World Wide Web,

[173] See also Benkler, who defines the tension between those subject to bovinity and those who choose to accept its influence as the "battle over the institutional ecology of the digitally networked environment", at Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 385; a battle that is framed by David as corporate and legislative attempts to control, versus "a hacker culture and a global Internet file-sharing community prepared to defend", at David, supra, 91.

[174] Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 395.

and now those who seek to enable efficient file sharing[175]. On the other side there is enclosure, characterised by legal anti-circumvention regulation and proprietary software that seeks to block, filter and exclude[176]. This is where the regulator is choosing to apply regulation by code, and this is where those who lie on the wrong side of the opportunity divide, or do not choose to step beyond it, are subject to it. If regulation by code were to be deemed effective, this would mean the strict application of paracopyright, a version of perfect control that trumps limited duration, fair dealing and de minimis[177]. If the present regulation by code were to be entrenched into a deeper layer in order to make it more effective, then the net, in the words of Lessig and Doctorow et al, would be broken. If regulation by code is not considered to be effective, then regimes that rely on code such as the DEA would predominantly fail to influence on a technical level the behaviour of those who choose to engage in file sharing. Yet the spillovers of the associated legal backing will still persist by affecting other avenues of openness, such as the provision of open WiFi[178]. At their worst, the legal overhangings might impede the innovation encouraged by the absence of barriers that has fed the success of the internet[179]. The gulf that exists between the approach of the regulator and the technical effect of the code is indicative of a fundamental disconnect between regulation by law and by code. This distantiation of approaches must be recognised by the regulator, or the result may well prove to be a "continual, and unedifying battle between designers of digital rights management systems and hackers, crackers and peer-to-peer systems"[180].

.* * * * *

Cite as: Filby, Michael. Code is Law? Assessing Architectural File Sharing Regulation in the Online Environment. *Journal of International Commercial Law and Technology,* Vol.8 No.1 (January, 2013)

[175] "Would control be better?... when future uses of a technology cannot be predicted – then leaving the technology uncontrolled is a better way of helping it find the right sort of innovation. Plasticity – the ability of a system to evolve easily in a number of ways – is optimal in a world of uncertainty." Lessig L, *The Future Of Ideas: The Fate Of The Commons In A Connected World* (Random House 2002), 39.

[176] Benkler, supra, 39.

[177] Netanel NW, *Copyright's Paradox* (Oxford University Press 2008), 66 & 186.

[178] Zittrain argues that shifting liability for the content of packets onto intermediaries will encourage further efforts to control, beyond what is mandated, in order to avoid liability, at Zittrain J, 'Internet Points of Control' (2003) 44 Boston College Law Review 653, 685.

[179] Boyle attributes the rapid expansion of the internet to the TCP/IP protocol and, subsequently, HTML being open, at Boyle J, 'The Second Enclosure Movement and the Construction of the Public Domain' (2003) 66 Law and Contemporary Problems 33, 62; Zittrain describes the generative nature of the internet as valuable, powerful, and instrumental to the development of the World Wide Web, at Zittrain J, *The Future of the Internet: And How to Stop It* (Penguin 2009), 42; Lessig further describes file sharing networks as the internet's "killer app": Lessig L, *Free Culture: The Nature and Future of Creativity* (Penguin 2004), 296.

[180] Murray AD, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish 2007), 124; see also Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedoms* (Yale University Press 2006), 469; and David, who highlights "the vulnerability of even the largest corporate research and development budgets when faced with a hacker culture and a global Internet file-sharing community prepared to defend and celebrate the actions of those programmers willing and able to perform the next great leap forward – and to make it available to the world", at David, supra, 91.