The role of non-state actors and institutions in the governance of new and emerging digital technologies

Leiser, M.R.; Murray, A.D.; Brownsford, R.; Scotford, E.; Yeung, K.

CHAPTER 28

THE ROLE OF NON-STATE ACTORS AND INSTITUTIONS IN THE GOVERNANCE OF NEW AND EMERGING DIGITAL TECHNOLOGIES

MARK LEISER AND ANDREW MURRAY

AQ:The order of author is different in TOC. Please confirm.

1. Introduction

1.1 Traditional, Nodal, and Transnational Governance Models

Traditional models of regulation and governance draw authority from the sovereign power of the state and convert that authority into an action in regulation or in governance.[1] As Morgan and Yeung outline in their classic *Introduction to Law and Regulation* (Morgan and Yeung 2007) traditional models of regulation and

governance begin from the cybernetics principle. Such a model begins with three components of a control system: capacity for standard setting; capacity for information gathering; and capacity for behaviour modification. In essence a model for regulation or for governance is predicated upon a standard-setting authority, a monitoring system which detects deviation from these standards and a form of corrective action to remedy deviation. Lawyers tend to more commonly apply a narrow definition of regulation: 'At their narrowest, definitions of regulation tend to centre on deliberate attempts by the state to influence socially valuable behaviour which may have adverse side-effects by establishing, monitoring and enforcing legal rules' (Morgan and Yeung 2007: 3). Some, however, employ a wider definition of what some may more properly suggest is governance: 'At its broadest regulation is seen as encompassing all forms of social control, whether intentional or not, and whether imposed by the state or other social institutions' (Morgan and Yeung 2007: 3–4). The true nature of regulation and governance, as applied in the real world, is probably closer to the latter than the former, but the study of such an ill-defined sphere would be nigh-on impossible as almost any social action by any institution could be defined as a regulatory act. Thus studies of regulation and governance have developed a number of refinements and supplementary models. Many such as risk based regulation (Black 2010) and responsive regulation (Ayres and Braithwaite 1992; Baldwin and Black 2008) are modelled upon specific relationships between an industry or sector and its regulator. They assume commonality of experience and language: in essence these approaches are institutional approaches to both regulation and governance. Another set of models examines the social structures of regulation and governance such as libertarian paternalism and empirical regulation (Sunstein and Thaler 2003; Sunstein 2011), and 'smart' regulation (Gunningham and others 1998). These are valuable additions to both the normative cybernetic model and the risk/responsive institutional models. They are not particularly helpful to the current analysis as their focus is on responses of the social actor in the regulatory matrix whereas the instant analysis is on technology and technological actors. Therefore, although we acknowledge the importance these contributions make to wider discourse on regulation and governance, and in particular their contribution by acknowledging the potential exploitation of biases and heuristics in human actors, we do not intend here to examine such socially mediated forms of regulation.[2]

Some regulatory models do capture the role played by technology as an actor. The most relevant are applications of actor–network theory (ANT) or science and technology studies (STS) (Kuhn 1962; Latour 2005). ANT is often associated with Michel Callon and Bruno Latour and is closely linked to the work of the Centre de Sociologie de l'Innovation, Paris. It was not developed particularly to deal with computer networks (Latour 1996) but rather was designed to model the semiotic relationships between all actants in a network human or non-human. It can be

extremely difficult to model without years of study but a good and simple description is given by Ole Hanseth and Eric Monteiro:

> When going about doing your business—driving your car or writing a document using a word-processor—there are a lot of things that influence how you do it. For instance, when driving a car, you are influenced by traffic regulations; prior driving experience and the car's manoeuvring abilities, the use of a word-processor is influenced by earlier experience using it, the functionality of the word-processor and so forth. All of these factors are related or connected to how you act. You do not go about doing your business in a total vacuum but rather under the influence of a wide range of surrounding factors. The act you are carrying out and all of these influencing factors should be considered together. This is exactly what the term actor network accomplishes. An actor network, then, is the act linked together with all of its influencing factors (which again are linked), producing a network. An actor network consists of and links together both technical and non-technical elements. Not only the car's motor capacity, but also your driving training, influence your driving. Hence, ANT talks about the heterogeneous nature of actor networks. (Hanseth and Monteiro 1998: 96–97)

As can be seen this is a very attractive model for anyone working in the information and communications technology (ICT) field including those of us working in ICT regulation or governance as it helps model the role and influence of non-human actors in the network and arguably allows for better modelling of the response of human actors to attempts to regulate their activity. ANT is in itself a subset or perhaps a development depending upon your point of view of STS. This is the rather broader study of the interrelationship between scientific discovery and advancement and external social, political, and cultural influences. This covers many fields from technological determinism to modernity and deliberative democracy. Much modern structuring of STS owes a debt to the work of Thomas Kuhn and in particular his work *The Structure of Scientific Revolutions* (1962). Kuhn posited the thesis that revolutionary changes in scientific theories may be attributed to changes in underlying intellectual paradigms. For those of us working in the ICT field, it is not Kuhn's thesis itself which is particularly appealing but the question of technological determinism which also plays a vital role in STS theory and in particular the distinction between hard and soft determinism. Hard determinists see technology as a driving force in societal development. According to this view of determinism, we organize ourselves to meet the needs of technology and the outcome of this organization is beyond our control or we do not have the freedom to make a choice regarding the outcome (Ellul 1954). This may be seen as an influencing factor in movements such as cyber-collectivism or cyberpaternalism (Lessig 2006; Goldsmith and Wu 2006; Zittrain 2008). Soft determinists still subscribe to the fact that technology is a guiding force in our evolution but would maintain that we have a chance to make decisions regarding the outcomes of a situation. This is reflected in movements such as network communitarianism (Murray 2006). A third application of STS in the ICT field is of course media determinism which was famously discussed by Marshall

McLuhan in his 1964 book *Understanding Media: The Extensions of Man* and in which he set out the famous phrase 'the medium is the message'.

The application of both ANT and STS theories to ICT regulation and governance is an area already extremely well developed with excellent work available (Knill and Lehmkuhl 2002; Gutwirth and others 2008; DeNardis 2014). Due to the already established nature of the literature in this area, we do not propose to apply ANT or STS theory in this chapter; instead, the tools to be applied in this analysis are to be found in nodal or decentred governance and transnational governance or regulation. Nodal or decentred governance is found in the work of Clifford Shearing (Shearing and Wood 2003), Peter Drahos (Burris and others 2005), and Julia Black (2001). In essence, it is the acknowledgement that the regulatory environment has many more active participants than is recognized by traditional cybernetic theory. As Black observes:

> The decentred understanding of regulation is based on slightly different diagnoses of regulatory failure, diagnoses which are based on, and give rise to, a changed understanding of the nature of society, of government, and of the relationship between them. The first aspect is complexity. Complexity refers both to causal complexity, and to the complexity of interactions between actors in society (or systems, if one signs up to systems theory). There is a recognition that social problems are the result of various interacting factors, not all of which may be known, the nature and relevance of which changes over time, and the interaction between which will be only imperfectly understood. (2001: 106–107)

The decentring analysis must also be placed within globalization and the transnational aspect of modern governance/regulation. Again, Black acknowledges this:

> Decentring is also used to describe changes occurring within government and administration: the internal fragmentation of the tasks of policy formation and implementation. Decentring is further used to express observations (and less so the normative goal) that governments are constrained in their actions, and that they are as much acted upon as they are actors. Decentring is thus part of the globalization debate on one hand, and of the debate on the developments of mezzo-levels of government (regionalism, devolution, federalism) on the other. (2001: 104)

The integration of decentred/nodal governance with ANT or STS theory gives a strong regulatory model for the regulation of emergent digital technologies (Teubner 2006; Sartor 2009; Koops and others 2010). It is the foundation of the cyber-collectivist, or cyberpaternalist, movement that took root in East Coast US institutions and which has become dominant in our understanding of cyber-governance (Lessig 2006; Goldsmith and Wu 2006; Zittrain 2008). Central to this thesis is the role of code, or to widen the analysis from merely Internet-enabled technologies, the standards and protocols employed by digital technologies of all types. Cyberpaternalists believe that the guidance of the state, or an elite, achieved through manipulation of software code or network hardware, is necessary to prevent cyberspace from becoming anarchic or simply inefficient (Lessig 2006: 120–137;

Zittrain 2008: 11–19, 101–126). This is most famously captured by Lawrence Lessig's model of regulation whereby he identified four regulatory modalities—law, social norms, architecture or design, and markets (Lessig 2006: 122–123). These modalities act as constraints on action or behaviour and within the plastic environment of the digital space where almost all aspects of the environment may be altered by human intervention. Lessig identifies architecture, or code, as the key modality (Lessig 2006: 83–119). As Wu observed in discussing Lessig's work:

> The reason that code matters for law at all is its capability to define behavior on a mass scale. This capability can mean constraints on behavior, in which case code regulates. But it can also mean shaping behavior into legally advantageous forms. (2003: 707–708)

Lessig identifies a shift in regulatory ability and power in this environment. The power and plasticity of code makes it the pre-eminent control mechanism for digital technologies as:

> [C]ode or software or architecture or protocols [which] set [the] features of the [digital space] are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. (Lessig 2006: 125)

He identifies two competing regulatory interests. The first are the East Coast codemakers:

> [T]he 'code' that Congress enacts . . . an endless array of statutes that say in words how to behave. Some statutes direct people; others direct companies; some direct bureaucrats. The technique is as old as government itself: using commands to control. In our country, it is a primarily East Coast (Washington, D.C.) activity. (Lessig 2006: 72)

The second regulatory interest come from the West Coast codemakers, which he describes as 'the code that code writers "enact"—the instructions imbedded in the software and hardware that make cyberspace work' (Lessig 2006: 72). Often they will work in concert with traditional, or East Coast, codemakers mandating technical standards from the technical community. Sometimes they work in parallel with the same values driving both East Coast and West Coast code. Occasionally they will come into conflict and in some cases East Coast code prevails, in others West Coast code survives. What Lessig identified more than anything though was the contribution of the West Coast codemaker: this was another example of the developing nodal or decentralized model of regulation, but, importantly, Lessig put considerable regulatory power into the hands of non-state actors.

1.2 Non-State Actors in the Technology Sectors

As digital technologies have moved from the lab to the home, and more recently to the world around us through mobile and wearable digital technology, non-state

actors have come out from Silicon Valley and the US West Coast to inhabit and represent almost all areas of society. In this chapter we have categorized them into four classifications: (1) business actors; (2) transnational multistate actors; (3) transnational private actors; and (4) civil society groups. Each has a particular value set and unique ability to influence key regulatory designers (East Coast and West Coast regulators). Although none of these have the ability to directly make policy, law, or to develop underlying architectures of control, each actor has the ability to access those who do have that ability and each have a particular method or means of influence.

The first group, business actors, are made up of those technology companies who have the ability to directly influence the design or code of emergent technologies including actual code developers, such as Microsoft, Google, and Apple; hardware developers, such as Sony or LG, and media and content companies such as Fox, Disney, or UMG. The tools available to business actors are varied. Those who have direct access to software or hardware design may directly manipulate design or code to their advantage. Others may find that due to their intermediary role, such as Internet service providers (ISPs) or search engines, they become proxy regulators for the interests of others (Laidlaw 2015). Developers of new platforms and technologies often find themselves quickly in a dominant position, particularly if the technology is both disruptive and widely adopted. In the last 20 years, Google has developed a dominant position in a number of technology sectors, but in particular in search, while Apple had (but may no longer have) dominance in digital music distribution. Currently Spotify seems to hold the leading position in streaming music distribution against strong competition in the form of Apple Music, Google Play Music, and Amazon Prime Music, while Netflix, Hulu, and Amazon fight for dominance in streaming video distribution. The need for content suppliers to be on these dominant platforms gives these companies considerable market power, a position that it takes competition authorities a considerable time to address, as we shall see in our discussion of the Microsoft dominance cases (see section 3.2).

Our second group, transnational multistate actors, reflect the global reach of new and emergent technologies: markets for new technologies are worldwide. As a result, and as predicted by Johnson and Post (1996), the ability of nation states to legitimately and effectively regulate emergent technologies is limited. This enhances the role of supranational organizations like the European Union (EU) and United Nations (UN). The EU is taking the lead in a number of areas of emergent technology, in particular privacy and data privacy and in abuse of dominance and more widely through its Digital Agenda for Europe. UN bodies also play a key shaping role. Most obviously through the World Summit on the Information Society, and the International Telecommunications Union Internet Policy and Governance Programme.[3] Finally there are multilateral initiatives such as the Transatlantic Trade and Investment Partnership which proposes common standards in a number of technology industries including ICTs, pharmaceuticals, engineering, and

medical devices. It is the second proposed multilateral trade treaty following on from the Anti-Counterfeiting Trade Agreement. These treaties are proving to be highly controversial with civil society groups and may be interpreted as an attempt to secure the dominance of current technology providers against possible emergent technologies.

The third group are transnational private actors. These are private regulatory organizations, as distinct from business actors, which have either organically developed into a regulatory role from a technical design or self-regulatory role, such as the Internet Architecture Board and the World Wide Web Consortium, or bodies created to fill a vacuum caused by the transnational nature of new and emergent technology such as the Internet Corporation for Assigned Names and Numbers (ICANN). As with transnational multistate actors a more recent development is the design of multistakeholder principles. These bodies draw authority and capacity to regulate from a number of sources. The Internet Architecture Board and the World Wide Web Consortium are essentially technocracies supported by the engineers who develop and make use of their systems. ICANN receives formal authority from two memoranda of understanding with the US Department of Commerce and the Internet Engineering Task Force,[4] a not uncontroversial position (Hunter 2003).

Finally, we must acknowledge the role of civil society groups. One aspect of Internet-enabled technologies is that as commerce becomes global so does activism and civil society. Leading civil society groups such as the American Civil Liberties Union and the Open Rights Group (ORG), have found themselves supplemented by a number of international multi-issue and single issue civil society groups such as Privacy International, GovLab, Drones Watch, Stop the Cyborgs, and many more. Although not able to directly develop regulation or governance, these groups through steady pressure can influence the development and deployment of new and emergent technology. Privacy International has successfully, along with other international civil society groups, influenced the EU to classify some digital surveillance technologies as dual-use for the purpose of exportation,[5] while Stop the Cyborgs, through a long and vocal campaign which attracted much negative media attention undoubtedly contributed to Google's eventual decision not to fully commercialize the explorer version Google Glass.[6]

Through a series of case studies this chapter examines how each of these groups plays a role in the development of governance for new and emergent technologies, demonstrating the role and contribution of non-state nodes of governance in emergent digital technologies. The first case study looks at business actors, and in particular the role of Internet intermediaries (IIs) such as Google, Facebook, and key ISPs such as BT or Sky, in controlling access to content online. As intermediary gatekeepers (Laidlaw 2015) they have a particular role, and some may argue commensurate responsibility, in allowing for the free flow of information from one part of the network to another. Their unique gatekeeper position has also led to them being identified by states as a key regulatory node targeted by them as proxy regulators.

The second case study examines the particular role of transnational multistate public bodies such as the UN and the EU. Our examination of this area centres upon the role of the EU in competition law or antitrust. We examine the Microsoft series of cases which have seen some of the largest fines in corporate history levied. These may also be considered alongside the current EU Google investigations that include one on the Google Shopping marketplace and one on the Android operating system (OS) and app store. Our third case study examines transnational standards setting bodies and in particular the role of ICANN, in managing the generic top-level domain name space (gTLD). This is a space of considerable commercial value and some public interest. ICANN have over the years been required to manage a number of controversial programmes to expand access to the gTLD and we will examine two procedures in some detail, the .xxx space and the new top-level domain process (new gTLD). Finally, we will examine the role of civil society groups in this sphere and in particular the degree of success achieved by civil society groups in the digital privacy sphere with particular attention to the role of Digital Rights Ireland and other European privacy groups in the series of challenges brought in response to the EU Data Retention Directive (Dir. 2006/24/EC).

2. Business Actors: Intermediaries as Proxy Regulators

2.1 Gatekeepers

IIs–ISPs, hosting providers, search engines, payment platforms, and participatory platforms (such as social media platforms), exercise key functions in their role as gatekeepers in the online environment (Laidlaw 2015). While IIs provide essential tools that 'enable the Internet to drive economic, social and political development', they may also 'be misused for harmful or illegal purposes, such as the dissemination of security threats, fraud, infringement of intellectual property rights, or the distribution of illegal content' (OECD 2011: 3). Their role as gatekeeper made IIs clear targets for regulatory reform. East Coast codemakers wanted to encourage them to act in an editorial, self-regulatory role; to police and remove harmful content, while IIs wanted to remove any risk of being held liable for that same harmful content.

In the USA, this issue came to a head with the decision in *Stratton Oakmont, Inc*. v. *Prodigy Services Company* 1995 WL 323710 whereby the New York Supreme Court ruled that IIs who assumed an editorial role with regard to customer content could be held liable as publishers, potentially making ISPs legally responsible

in libel or tort for the actions of their users. This effectively discouraged IIs from self-regulating, an outcome which went against the intention of Congress. This led to the passing of s. 230 of the Communications Decency Act 1996 (47 USC) which provides immunity for IIs operating in an editorial capacity. Unlike the controversial anti-indecency provisions found in the Act that were later ruled unconstitutional, s. 230 is still in force. It allows ISPs to restrict customer actions without fear of being found legally liable for their intervention. In *Zeran* v. *America Online* 129 F 3d 327 the Fourth Circuit Court of Appeals noted Congress 'enacted s. 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision'. Fearing this spectre of liability would deter ISPs from blocking and screening offensive material, Congress enacted s. 230 'to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material' (47 USC §230(b)(4)). Thus, s. 230 was specifically passed to encourage IIs to play a regulatory role.

In Europe, regulators undertook a nuanced approach to IIs as gatekeeper regulators. The e-Commerce Directive focused energies on notice and take down, imposing liability for ISPs only with attainment of actual knowledge of illegal content or activity (Art. 14, Dir. 2000/31/EC). This approach has been fine-tuned through case law where courts have struggled to find a sense of proportionality that balances the rights of Internet users with litigants. In carrying out this unenviable task, courts have to balance not only rights of users against other rights-holders, within an acceptable framework for advocates of Internet freedoms that *also* complies with international standards.

2.2 Searching for Proportionality

Searching for 'nuance' has led to a series of cases in the UK where the courts examined various questions relating to the passivity of IIs in content moderation: for example, how involved in moderation does an II have to be before they lose their exemption from liability?[7] What actually qualifies as 'notice' under Art. 14 of the e-Commerce Directive?[8] And what is meant by the term 'intermediary' under the Directive?[9] This search for nuance has had three effects. First, it has fragmented intermediary liability into subject-specific pockets of analysis. In copyright law, UK (and European) law has responded to immunity for conduits under Art. 12 of the e-Commerce Directive by developing Art. 8(3) of the Information Society (Dir. 2001/29/EC). This was given effect in the UK by s. 97A of the Copyright, Designs and Patents Act 1988, and is a provision specifically designed to allow injunctions against IIs. Meanwhile, s. 1 of the Defamation Act 1996, ss. 5 and 10 of the Defamation Act 2013 and the Regulations for Operators of Websites, when taken together, provide a specific defence for the II if they can show that they did not post a defamatory

statement.[10] Second, there has been an additional series of cases so fact sensitive that it is hard to draw a line of authority in order to advise actors on how to structure their business.[11] Finally, agreements outside formal legal frameworks occur without the oversight and transparency that one would normally expect from traditional state actors. For example, agreements between the UK government and major ISPs allow for the restriction of access to content deemed pornographic unless a broadband user 'opts in' with their ISP to access such content. The UK government has stated its intention to extend this regime to sites hosting extremist content (Clark 2014), while companies like BT have implemented wider content filtering systems under frameworks for of parental control, whereby new users must opt in to a variety of content, ranging from obscene content, to content featuring nudity, drugs and alcohol, self-harm, and dating sites (BT 2015).

Since 2012, a series of orders pursuant to s. 97A of the Copyright, Designs, and Patents Act 1988 have been made by the English courts requiring ISPs to block or at least impede access to websites that offer infringing content. Since the initial cases of *Twentieth Century Fox Film Corp* v. *British Telecommunications plc* [2011] EWHC 1981 (Ch) and *Twentieth Century Fox Film Corp* v. *British Telecommunications plc (No. 2)* [2011] EWHC 2714 (Ch), ISPs have not opposed a single blocking order sought by rights-holders. They have instead limited themselves to negotiating the wording of orders. To date there has not been a single appeal regarding the costs of the applications or the costs of implementing the orders.[12] All section 97A orders relating to copyright have been obtained by film studios, record companies or by the FA Premier League. The courts have also allowed for an s. 97A-style order to be made under s. 37 (1) of the Supreme Courts Act 1981 against a site selling mass quantities of trademark infringing goods.[13] Injunctions issued under s. 97A (or s. 37(1)) pose a new set of challenges for the courts, in large part due to Art. 11 of the Enforcement Directive which requires that any remedies for relief be 'effective, proportionate, and dissuasive' and implemented in a way that does not create 'barriers legitimate trade' and 'safeguards against abuse'. The courts must take into account the interests of third parties, particularly those consumers and private parties acting in good faith (Recital 24, Dir. 2004/48/EC). Taken together, Recital 24 and Article 3(2) of the Enforcement Directive (Dir. 2004/48/EC), and the ruling from the European Court of Justice in *L'Oréal* v. *eBay* [2012] All ER (EC) 501 require that any injunctions must not only be 'effective, proportionate, and dissuasive and must not create barriers to legitimate trade', but also must have regard to safeguards against abuse and interests of third parties.[14]

2.3 Business Actors

Major benefactors of increased regulation over IIs are arguably those who offer legal alternatives to the now regulated copyright infringing services. This has led to

greater demand for legal services such as Spotify, Apple Music, Google Play Music, or Amazon Prime Music for accessing and/or purchasing copyrighted music and Netflix, Hulu, and Amazon Prime in the lucrative video market. The role of commerce in the governance of new and emerging technologies never has been more relevant. Companies like Dropbox, Spotify, and Netflix have developed their services in response to user frustrations with the digital environment. Dropbox, a cloud storage company, thrived by providing a user-friendly solution to secure offline access to files from multiple devices while offering a product that circumvents limitations in capacity found in personal computer hardware. By summer 2016, the music service Spotify had grown to over 100 million users and over 40 million paying subscribers[15] providing a legal streaming alternative to Apple's iTunes download service. The success of Spotify eventually forced market leaders in music downloads Apple, Google, and Amazon to begin their own streaming services in competition. At the same time video service Netflix boasted over 83 million members in over 190 countries enjoying more than 125 million hours of TV shows and movies per day.[16] With growing popularity in cloud-based, legitimate, and income-generating media providers, it is unsurprising rights-holders continue to take steps to protect their intellectual property in the online environment.

Section 97A appears to be a powerful and symbolic tool in the East Coast code-maker's arsenal. Orders made under s. 97A provide allow rights-holders to compel ISPs into becoming *complicit* deputies in their fight, whatever that fight might be. Intermediary gatekeepers, discussed so eloquently by Laidlaw, now arguably have dual roles: the gatekeeper is not only an independent regulator, enforcing their own moral or corporate values (as allowed by s. 230), but is also a proxy—a mere tool or node in a larger regulatory matrix. In many cases the second category captures that most Lessigian act—seizing and deployment of non-state actors by the state to protect wider political or commercial interests: West Coast Code has been enrolled by East Coast Code.[17]

3. Transnational Multistate Actors: The EU DG Competition

3.1 Emerging Markets and Disruptive Innovation

Governments, of course, remain engaged in the digital governance debate. The very premise of a chapter which discusses the role of non-state actors in the governance of emergent digital technologies is that state actors are still the primary regulators

in this sphere. State actors may leverage control directly and indirectly and they play key roles in the private governance space through governmental advisory committees and policy committees. More directly governments through organizations such as the UN, the EU, or the African Union form supranational regulatory blocs. One area where the European Union has been particularly active in the field of new and emergent digital technologies is in competition abuses.

New and emergent technologies are often disruptive in nature and as such pose a threat to established market participants. The risk to established market participants has been identified and discussed extensively in economics literature, especially by Clayton Christensen of Harvard Business School whose work *The Innovator's Dilemma* (Christensen 1997) has become the foundational text in this discourse. In a contemporary attempt to modernize and give flesh to Schumpeter's now dated conceptualization of creative destruction (Schumpeter 1942: 81–87), Christensen replaces Schumpeter's macroeconomic concept of a collapse of capitalism with a microeconomic business-centred concept of disruptive innovation (Christensen 1997: 10–19). While Schumpeter is looking at the outcome of disruption, Christensen is looking at the causal mechanism. Christensen notes that while most technological innovations are sustaining innovations 'technologies . . . that [] improve the performance of established products, along the dimensions of performance that mainstream customers in major markets have historically valued' (1997: 11) disruptive technologies are quite different:

> [They] result in worse product performance, at least in the near-term . . . they bring to a market a very different value proposition than had been available previously. Generally, disruptive technologies underperform established products in mainstream markets. But they have other features that a few fringe (and generally new) customers value. (1997: 11)

In time these technologies become mainstream as more customers are attracted to the benefits the new technology offers. Meanwhile the operators of established technologies lose out as they fail to invest in the disruptive technology for three reasons:

> First, disruptive products are simpler and cheaper; they generally promise lower margins, not greater profits. Second, disruptive technologies typically are first commercialized in emerging or insignificant markets. And third, leading firms' most profitable customers generally don't want, and indeed initially can't use, products based on disruptive technologies. (Christensen 1997: 12)

As a result, established firms fail and new entrants take over. We have seen this happen frequently with digital technologies. IBM and DEC, major mainframe manufacturers lost out to smaller and more nimble desktop computer manufacturers such as Dell, Wang, and Apple in the 1980s; IBM lost out again to Microsoft in the OS market, while more recently Internet technologists such as Google, Adobe, Netflix, and Spotify have disrupted a number of markets including web browsing, file storage, applications software, mobile OSs, television and film, and music distribution.

It is unsurprising therefore that established market participants often take defensive positions vis-à-vis new and emergent technologies which display disruptive characteristics. These defensive positions vary dependent upon the market and the new entrant. Often extensive patent thickets will be employed with dominant market participants patenting all aspects of their technology as has been seen in the *Samsung* v. *Apple* series of cases fought globally over a number of patents including the Apple 381 'bounce back' patent and the Samsung 711 'music multitasking' patent.[18] An alternative strategy is to leverage market dominance in one technology market to achieve control or dominance over an emergent market. This strategy is employed usually when the dominant player in one market wishes to move into a vertically related emerging market such as Microsoft's attempts to leverage dominance in the ~~OSs~~ market to achieve dominance in the web browser market or Google's attempts to leverage dominance in web search into vertical search, online advertising and mobile platforms. Unsurprisingly, these attempts have drawn the attention of competition authorities in both the US and the EU and provide the perfect case study to analyse the regulatory activity of the EU directorate General for Competition as a multistate, supranational, public regulatory body.

3.2 Microsoft: Interoperability, Media Players, and Web Browsers

In the 1990s, the disruptive innovation for OS and applications software (AS) developers like Microsoft was web browsers. The risk was that anything which could be achieved through a personal computer could be achieved through a network computer connected to a server. The fruits of the network computer concept may be seen today in inexpensive and lightweight notebook computers such as the Google Chromebook, which operate using the Chrome OS, a variant of Linux, designed to be used with network applications such as Google's online office suite. For Microsoft, there was a dual threat: browsers could challenge their dominance in the ~~OS~~ market while online applications could undermine their dominance in office applications software. Despite this threat, as Christensen could have predicted, Microsoft as the incumbent in the wider OS/AS markets was a slow adopter to web-browsing technology. The first commercial web browser was the Netscape or Mosaic browser which in January 1994 was used by 97 per cent of Internet users.[19] Microsoft would not debut its browser, called Internet Explorer, until August 1995 by which time Netscape Navigator, the replacement for Mosaic, was on its way to controlling nearly 90 per cent of the browser market.[20] Remarkably though by October 1998 Internet Explorer would overtake Netscape Navigator to become the most popular web browser: in a little over three years Microsoft had gone from less than 4 per cent of the browser market to 49.1 per cent[21] and in time Internet Explorer would go

on to hold nearly 97 per cent of the browser market.[22] The story of how Microsoft achieved this is of course well known and is recorded by the findings of facts in *United States* v. *Microsoft* (253 F.3d 34):

> In early 1995, personnel developing Internet Explorer at Microsoft contemplated charging Original Equipment Manufacturers and others for the product when it was released. Internet Explorer would have been included in a bundle of software that would have been sold as an add-on, or 'frosting', to Windows 95. Indeed, Microsoft knew by the middle of 1995, if not earlier, that Netscape charged customers to license Navigator, and that Netscape derived a significant portion of its revenue from selling browser licenses. Despite the opportunity to make a substantial amount of revenue from the sale of Internet Explorer, and with the knowledge that the dominant browser product on the market, Navigator, was being licensed at a price, senior executives at Microsoft decided that Microsoft needed to give its *browser* away in furtherance of the larger strategic goal of accelerating Internet Explorer's acquisition of browser usage share. Consequently, Microsoft decided not to charge an increment in price when it included Internet Explorer in Windows for the first time, and it has continued this policy ever since. In addition, Microsoft has never charged for an Internet Explorer license when it is distributed separately from Windows. (*US* v. *Microsoft*: [137])

As District Judge Jackson notes:

> over the months and years that followed the release of Internet Explorer 1.0 in July 1995, senior executives at Microsoft remained engrossed with maximizing Internet Explorer's share of browser usage. Whenever competing priorities threatened to intervene, decision-makers at Microsoft reminded those reporting to them that browser usage share remained, as Microsoft senior vice president Paul Maritz put it, 'job #1'. (*US* v. *Microsoft*: [138])

Applying this ethos Microsoft leveraged a 3.7 per cent market share into a 96.6 per cent market share in six and a half years. The infamous case of *United States* v. *Microsoft* examined both the bundling of Internet Explorer and Windows Media Player in the Windows OS. The outcome of this case, which took six years to final disposal (*Massachusetts* v. *Microsoft Corp*, 373 F. 3d 1199), was roundly criticized for not doing enough to prevent future abuses of dominance in the OS market by Microsoft (Chin 2005; Jenkins and Bing 2007).

It is arguable that the outcome of the *United States* v. *Microsoft* case represents a failure by the state to regulate one of its own citizens. However, in addition to the US antitrust investigation, the Commission of the EU undertook a separate investigation. This investigation was begun in 1993 and related to the licensing of Windows OS, access to Windows OS application program interfaces (APIs) and the bundling of Windows Media Player (WMP). The initial investigation in Europe did not involve Internet Explorer but a later investigation did involve Internet Explorer bundling. The initial case was brought in 1998 and was an investigation of two breaches of Art. 82 of the EC Treaty (now Art. 102 TFEU), and Art. 54 of the EEA Agreement: (1) refusing to supply interoperability information and allow its use for the purpose of developing and distributing work group server OS products (the interoperability investigation); and (2) making the availability of the Windows

Client PC OS conditional on the simultaneous acquisition of WMP from May 1999 until the date of this decision (the bundling investigation).[23] The case is, of course, extremely well known. Following a five-year investigation, the Commission found that Microsoft had a dominant position in both the group server OS market and the PC OS market. They further found Microsoft had abused both market dominances to leverage control into related markets, eventually fining Microsoft over €497 million although over time this fine has increased considerably due to Microsoft failing to comply in good time, with an additional fine of €899 million (reduced on appeal to €860 million) added in 2008.[24] With a clear, and for Microsoft costly, precedent set that, for the purposes of former Art. 82 of the EC Treaty bundling was unlawful the Commission opened up the entire market for software which operated on the Windows platform. When soon after the Commission announced that it was turning its attention to Internet Explorer bundling Microsoft immediately took action to ensure that it complied with EU competition law by offering an 'E' version of Windows 7 which would unbundle Internet Explorer for distribution within the EU (Heiner 2009), although in 2013 Microsoft were fined an additional €561 million for failure to implement correctly and in good time the settlement agreed to in 2009.[25]

The actions of the European Commission have generally been viewed as being much more successful than the intervention of the US federal government into Microsoft's activities. While the US antitrust case is viewed as being less effective in regulating Microsoft's leverage of its dominant position in the OS market, the collected EU competition actions are seen as effective interventions into especially the emergent streaming video and browser markets. Market share data seems to demonstrate that given a free choice the consumer chose not be tied to the Microsoft product. The global market share for Internet Explorer has fallen from nearly 97 per cent in April 2002 to 9.5 per cent today. In addition the market is much more open with no browser holding a clearly dominant position, the market leader Google Chrome holds 58.1 per cent, Apple Safari 12.7 per cent, Firefox 12.4 per cent, Internet Explorer/Edge 9.5 per cent and Opera 2.8 per cent.[26] While much of this change in market share can be tracked to the emergence of new browsing technologies such as smartphones and tablets which make extensive use of Google and Apple ~~OSs~~ (and hence a pre-eminence for Chrome and Safari on these products), there is no doubt the actions of the EU Commission helped create an environment where new (and existing) technologies such as Chrome and Safari could develop their product in the PC market before phone and tablet versions were developed. Accurate figures for just desktop market share are harder to find but online site 'Net Market Share' suggests that Internet Explorer/Edge holds a stronger position in the desktop browser market, with Chrome being the dominant browser on 43.4 per cent of desktops, Internet Explorer/Edge on 26.1 per cent, Firefox on 5.4 per cent, Safari on 3.3 per cent and Opera on 1 per cent. Internet Explorer's greater desktop application seems to be a legacy issue with Internet Explorer 8, still being

used by 4.2 per cent of users (almost the same as Safari and Opera combined). This was the version released in 2009 which was bundled with Windows 7 outside the EU, and which according to the Commission was bundled to 15 million EU citizens in error.[27] There is little doubt that the browser market is much healthier today than in 2009. Equally data shows that the market for streaming video players is much healthier post the intervention of the Commission.[28] The Commission's interactions with Microsoft may have been critiqued by some free market thinkers (Ahlborn and Evans 2009; Economides and Lianos 2009) but there seems little doubt that by cutting back the leveraged vertical dominance of Microsoft they have allowed new entrants and new technologies to flourish in what may not be sexy but are important everyday markets.

4. Transnational Standards and Private Actors: ICANN

4.1 ICANN

When one thinks of a transnational private actor in the digital environment, one invariably thinks of ICANN. ICANN is a high-profile private regulator with global reach. It was formed in 1998 to take over management of the root domain name space which meant ICANN became responsible for the allocation of Internet Protocol (IP) address spaces to regional registrars and for the management of generic top-level domains (gTLDs) such as .com, .net and .org. This was all achieved by the signing of a memorandum of understanding with the US government which transferred to ICANN the so-called IANA function of assigning Internet address blocks previously under the management of the Information Sciences Institute at the University of Southern California (Mueller 1999). ICANN was the conscious creation of a private multistakeholder regulator to replace the old system of public/private governance (NTIA 1998). In the years since ICANN's creation, it has grown to be an effective, although controversial, multistakeholder regulator. Despite initial criticism that it was unrepresentative (Mueller 1999; Froomkin 2001) and lacked legitimacy (Froomkin 2000), ICANN has withstood a number of challenges, including a sustained challenge to its role at the 2005 WSIS summit in Tunis (Pickard 2007), and today despite ongoing challenges seems to be secure in its role as the established global regulator not only of the IANA function and the root domain name system (DNS), but of domain name policy more generally (Take 2012).

4.2 Generic gTLDs and the .xxx Controversy

One policy area continually debated by ICANN and stakeholders is the creation of New gTLDs. These are thought to be necessary due to a paucity of available addressing options in the domain name structure. The limited number of gTLDs (in 1998 when ICANN was formed there were only three open gTLds .com, .org and.net) meant that once someone had registered say apple.com it was unavailable for anyone else. This meant once Apple, Inc. had registered this address it was no longer available for Apple Records or Apple Bank (Murray 1998). The scarcity of available domain name space meant the push for a greater number of gTLDs to alleviate pressure on the ever expanding use of the DNS is older than ICANN. In 1997, the International Ad-Hoc Committee (part of IANA the forerunner to ICANN) proposed seven New gTLDs including .firm, .store and .web as 'the DNS was lacking when it comes to representing the full scope of the organizations and individuals on the internet' (Gibbs 1997). These proposals were abandoned when ICANN took over management of the DNS but in November 2000, following a short public consultation, it announced seven New gTLDs of its own: .aero, .biz, .coop, .info, .museum, .name and .pro. They were quickly criticized for being, with the exception of .biz, too narrow in reach (Levine 2005; Nicholls 2013) and ten years later an analysis of the .biz gTLD found it too had failed to meet its policy objectives (Halvorson and others 2012). Despite this, ICANN continued to introduce a drip of gTLDs including six more between 2004 and 2007 and another in 2012. During this time, the major controversy was over the .xxx proposal. This was a proposal for an adult space on the Internet delineated by a .xxx gTLD, proposed by ICM Registry in 2004. Initially, ICANN approved the application but in the aftermath of this decision national governments became engaged through ICANN's Government Advisory Committee (GAC), an advisory committee formed of representatives of all UN member states and a number of supranational organizations including the African Union and the European Commission, supplemented by a number of observers from multinational organizations including the European Broadcasting Union and the International Telecommunications Union.

Initially, it appeared members of the GAC had no objections to the .xxx proposal. A letter from GAC chair Mohamed Sharil Tarmizi in April 2005 had stated '[n]o GAC members have expressed specific reservations or comments in the GAC, about the applications for sTLDs in the current round'.[29] This quickly changed, though. Under pressure from groups like the Family Research Council and Focus on the Family, the US government hardened its stance against .xxx. This was quickly followed by objections from Australia, the UK, Brazil, Canada, Sweden, the European Commission, and many others. As a result, in May 2006 ICANN withdrew its approval. There are many ways to view this. It can be seen as a success for the multistakeholder model in that an initial decision of the ICANN Board taken following limited consultation was reversed following action from civil society groups and

discourse by representatives of democratic governance in the GAC. In the alternative, it could be viewed as a failure by ICANN to represent the wider community and the variety of stakeholders with an interest in liberalization of the gTLD space. In the first major challenge to the ICANN multistakeholder model, national governments had flexed their muscles and had won the day. As Jonathan Weinberg states: 'National governments had become involved with the issue late in the day, but their objections were powerful . . . empowered by that experience, GAC members sought to make their views known more broadly' (Weinberg 2011: 203); certainly there was a prevailing view that ICANN had allowed themselves to be dominated by the GAC in this exchange (Berkman Centre 2010; Mueller 2010: 71–73; Weinberg 2011). Perhaps fortuitously, ICANN had previously agreed to arbitration should there be any challenges to their decisions and ICM took advantage of this to challenge the decision. The eventual decision of the International Center for Dispute Resolution in February 2010 found that ICANN had been wrong to reverse their decision (*ICM* v. *ICANN*, ICDR Case No. 50 117 T 00224 08, 19 February 2010). They found that ICANN had a duty to 'operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law', that 'the Board of ICANN in adopting its resolutions of June 1, 2005, found that the application of ICM Registry for the .XXX sTLD met the required sponsorship criteria' and vitally that 'the Board's reconsideration of that finding was not consistent with the application of neutral, objective, and fair documented policy' (*ICM* v. *ICANN*: [152]). They also tacitly supported ICM's contention that '[ICANN] rejected ICM's application on grounds that were not applied neutrally and objectively, which were suggestive of a pretextual basis to 'cover' the real reason for rejecting .XXX, i.e., that the U.S. government and several other powerful governments objected to its proposed content' (*ICM* v. *ICANN*: [89]). As a result of this, ICANN reviewed the decision, and in March 2011 ICANN approved the .xxx domain.

4.3 The New gTLD Process

The fallout from the .xxx case was felt acutely in the next stage of domain name liberalization, the creation of 'New gTLDs' a process formally begun in 2008. It reached fruition in 2011 when the ICANN Board agreed to allow applications for New gTLDs from any interested party upon payment of a substantial management fee.[30] To date, over ~~500~~ New gTLDs have been approved,[31] and they fall mostly into four categories: trademarks such as .cartier, .toshiba, and .barclays; geographical such as .vegas, .london, and .sydney; vocational such as .pharmacy, .realtor, and .attorney and speculative such as ~~.~~ beer, .porn, and .poker.[32] Learning from their experience in the .xxx controversy, ICANN approached the New gTLD process

differently. First, an attempt by some members of the GAC to regain control over the approval process was met head on. An attempt by the Obama administration to secure for the US and other GAC members a veto right against New gTLD applications (McCullagh 2011) was deflected by ICANN who refused to act on the proposal. Instead, ICANN reaffirmed the process which had been previously agreed; a proposal which ultimately met with agreement of most members of the GAC.[33] To meet both the concerns of allowing an open registration process, which allows any string of letters or characters to be registered, and the .xxx concern, the New gTLD registration process has two safeguards. The first is that once an application is made there is a period during which objections against grant may be lodged on one of four grounds: string confusion (where the applied for name is confusingly similar to an already in use or applied for string, such as .bom or .cam); legal rights objections (where the name is confusingly similar to a legal trademark or right in a name, such as .coach or .merck); community objections (where a challenge may be brought by representatives of a community to whom the name is impliedly or implicitly addressed, such as .amazon or .patagonia); and finally and vitally for our analysis a limited public interest challenge which may be brought where the gTLD string is contrary to generally accepted legal norms of morality and public order that are recognized under principles of international law. Each objection gives rise to an arbitration process with the WIPO Arbitration and Mediation Centre dealing with legal rights objections; the International Center for Dispute Resolution dealing with string confusion objections and the International Center of Expertise of the International Chamber of Commerce dealing with both community and public interest challenges. New gTLDs cannot be awarded until they have either passed the period for objection without any objection being lodged or the applicant has been successful at arbitration. Any interested party with standing, including GAC members, can bring challenges. As with the .xxx case, arbitration was seen as the best way to settle disputes, and as with the longstanding dispute resolution procedure, independent arbiters are preferred. The second safeguard was the creation and appointment of an 'Independent Objector'. This was an office created solely to serve the best interests of global Internet users. The Independent Objector could lodge objections in cases where no other objection has been filed but only on limited public interest and community grounds. The appointed Objector was Professor Alain Pellett and he lodged 23 such objections ranging from .amazon to .health. He prevailed in five claims, lost in 14 and four claims were withdrawn.

The New gTLD process is clearly a refinement of the processes used in previous rounds of gTLD creation. There have been a number of critiques of ICANN that have drawn into question its legitimacy. Many of these have focused upon its processes for renewing and reforming the DNS. Claims made by critics include that ICANN, despite being set up as a multistakeholder regulator, has been too narrow in approach, unresponsive to criticism and undemocratic in action (Mueller 1999; Froomkin 2000; Froomkin 2001; Koppell 2005; Pickard 2007). Fears about undue

influence of GAC members remain to this day (Mueller and Kuerbis 2014), but the New gTLD process, although not without flaws (Froomkin 2013), is clearly more inclusive of the wider Internet community and stakeholders outside of the usual closed group of ICANN board members, GAC members, and trademark holders. Objections have come from diverse interest groups such as the International Lesbian Gay Bisexual Trans and Intersex Association and the Union of Orthodox Jewish Congregations of Americas, member associations such as the Universal Postal Union and the International Union of Architects, political associations including the Republican National Committee and local interest groups including the Hong Kong Committee on Children's Rights. All these challenges are in addition to the challenges brought by the Independent Objector and the large number of challenges brought by commercial entities as well as the limited number brought by national governments and public authorities. As noted at the outset of this section, the importance and value of domain names as a tool for identity as well as addressing mean they play a vital role in emergent online offerings. All too often, we think of new and emergent technologies in terms of hardware or innovative services. The development of the DNS from 1998 onwards has been a vital component of the development of the Web and mobile content and ICANN have played a vital role in this. The importance and value of the DNS is exactly why they are such a controversial regulator. Much improvement is still clearly required of them but the New gLTD process is arguably a move in the right direction.

5. Civil Society Groups: Data Retention

5.1 Data Retention, Proportionality, and Civil Society

The EU Data Retention Directive (Dir. 2006/24/EC) sought to harmonize EU Member States' provisions 'concerning the obligations of the providers of publicly available electronic communications services or of public communications networks' with regard to data retention for the *purpose of the investigation, detection and prosecution of serious crime* (Data Retention Directive. Art. 1 (1)). Under Art. 10 of the Directive, Member States ~~are~~ required to provide statistics relating to the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. These statistics include: the cases in which information was provided to the competent authorities in accordance with applicable national law; the time elapsed

between the date on which the data were retained and the date on which the competent authority requested the transmission of the data; and the cases where requests for data could not be met.[34]

Given the rapid advance in technology, concerns for what amounted to sufficient legal safeguards remained unclear. After an advocacy group called Access to Information Program (AIP) initiated an action, the Bulgarian Supreme Administrative Court (SAC) annulled Art. 5 of the Bulgarian Regulation No. 40 which provided for a 'passive access through a computer terminal' by the Ministry of Interior, as well as access without court permission by security services and other law enforcement bodies, to all retained data by Internet and mobile communication providers. The SAC annulled the article, considering that the provision did not set any limitations with regard to the data access by a computer terminal and did not provide for any guarantees for the protection of the right to privacy stipulated by Art. 32(1) of the Bulgarian Constitution. In Romania a challenge to Law 298/2008, the Romanian implementing provision, found that

> [T]he provisions of Law no. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as the modification of law 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area are not constitutional.[35]

After over 30,000 German citizens brought a class action suit, Germany's highest court suspended its implementation of the Directive by ruling that it violated citizens' rights to privacy.[36] Finally, a constitutional challenge was raised in the Irish courts, brought by another advocacy group, Digital Rights Ireland, challenging the entire European legal basis for data retention (*Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* (C-293/12) [2014] All ER (EC) 775).

The EU responded with data retention reform plans to reduce and harmonize the data retention period: It noted '[a]pproximately, 67% of data is requested within three months and 89% within six months' (EU Commission 2013: 7). Additionally, there was an increase in the types and scope of data to be retained, minimum standards for access and use of data, stronger data protection, and a consistent approach to reimbursing operators' costs.[37] Meanwhile, the Irish government attempted to discontinue the Irish action by seeking security for costs requiring payment into court to cover the costs of the state should they lose. Because of the high cost of High Court actions requiring such a payment at the outset could have effectively prevented the case from being heard. The Court rejected the state's application:

> [G]iven the rapid advance of current technology it is of great importance to define the legitimate legal limits of modern surveillance techniques used by governments . . . without sufficient legal safeguards the potential for abuse and unwarranted invasion of privacy is obvious . . . That is not to say that this is the case here, but the potential is in my opinion so great that

a greater scrutiny of the proposed legislation is certainly merited. (*Digital Rights Ireland Ltd* v. *Minister for Communication & Ors* [2010] IEHC 221: [108])

5.2 Transparency and Civil Society

In the fallout from the Snowden revelations, regulation of intelligence and surveillance agencies is slowly being increased, albeit not necessarily at the pace that privacy advocates would like. A right to privacy may not yet have the same bite as normally associated with other fundamental rights, but pressure to respond to civil society's bark has played an increasingly important role in checking the abuse of runaway state power (United Nations 2013, United Nations 2014). There have been a number of legal challenges at the European Court of Human Rights by civil society groups ranging from surveillance challenges to demands to the release documents detailing the spying agreements between the 'Five Eyes' partners (*Big Brother Watch & Or*. v. *UK* ECtHR App. 58170/13; *Bernh Larson Holdings* v. *Norway*, ECtHR App. 24117/08; *Liberty & Ors* v. *The Secretary of State for Foreign and Commonwealth Affairs & Ors* [2015] 1 Cr App R 24). At the Court of Justice of the European Union (CJEU) civil society have successfully challenged the legal regime governing data retention (*Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* (C-293/12) [2014] All ER (EC) 775) and, as seen have had considerable influence over domestic, implementing, legislation. The ORG along other European societies has led domestic campaigns forcing governments to rethink their approaches to domestic surveillance or programmes that do not embrace or understand how they may compromise fundamental rights. The German Constitutional Court partially upheld a complaint that the police authorities' audio surveillance of a home (a large-scale eavesdropping attack) breached fundamental rights; finding that any breach of a constitutional right on the basis of IT security requires factual evidence indicating a specific threat to an outstanding and overriding legal interest and judicial authorization.[38]

Civil society has also played a role in moderating legitimate actions by the state to regulate content. In 2014, the British government demanded that ISPs and mobile phone companies made a change in their choice architecture to restrict access to adult content. Access to content that is pornographic would be blocked unless a broadband user 'opts in' with its provider to access such sites. Major ISPs implemented a filtering programme, marketing the programme as 'parental controls', whereby users must opt-in to a variety of content, ranging from obscene content, to content featuring nudity, drugs and alcohol, self-harm, and dating sites. However, blocking systems tend not to work quite as well as was intended; filters designed to stop pornography also block sex education, sexual health, and advice sites. Parental reliance on blocking can result in derogation of parental responsibility. Overreliance

on a web-filtering programme often assumes that nothing is going to get through resulting in the misguided assumption by a parent that their child is safe. Civil society engaged in petitions to moderate the government's stance and to help ISPs engage with users who may be affected by their decision to change the default rule. Groups like 451 Unavailable and Blocked.org.uk have helped to highlight the problem of web blocking, and have encouraged courts to publish blocking orders to increase transparency. As a result of this type of advocacy, the UK courts adopted ORG's recommendations that any blocking orders should be required to have safeguards against abuse, and as a consequence adopted ORG's proposals about landing pages and 'sunset clauses' as safeguards against abuse.

6. Conclusions

This chapter elucidates roles and relationships of non-state actors in governance of the online environment. In doing so, it examines reasons for that role and discusses the utility and legitimacy of the relationship with traditional Westphalian forms of governance. The chapter also pays some attention to the equivalent role of law, charting its interaction with non-state actors. Its basic premise is that non-state actors play such a key part in regulation of cyberspace that the latter cannot be properly understood without explaining the frameworks in which they reside. At the same time, we have attempted to contribute to the legal and regulatory discussion about the legitimacy of regulatory roles non-state actors play. Accordingly, there is increasing awareness of the power embedded within non-state actors and the need for ongoing assessment of the balance of power between private and public bodies generally.

On another level the chapter also seeks to address the non-state actor's role in 'meta-regulation'—their coordination in networks with markets and governments. The extent of the role of the non-state actors attracts critical analysis; accordingly, there is growing awareness that the regulatory regimes for Internet regulation have an inherent complexity that is difficult to comprehend. This poses significant challenges for regulators and engenders legal uncertainty, but also creates opportunities for abuses of power by non-state actors. For Teubner, privatized rulemaking continues to exert 'massive and unfiltered influence of private interests in law making', and is characterized as 'structural corruption' (Teubner 2004: 3, 21). For others private ordering remains the most legitimate and effective means of regulating the online environment (Easterbrook 1996; Johnson and Post 1996: 1390–1391). The role of the non-state actor will continue for the foreseeable future to remain the subject of critique.

The ascendency of non-state actors is a hallmark of the online environment. The largesse of the non-state actor's conquest is perhaps most strikingly demonstrated by its invasion of cyberspace. Legal scholars will continue to examine the relationships prevalent in cyberspace, not only relationships between private corporations, but also relationships that govern relationships between government agencies and non-state actors. These apply particularly to relationships between private sector actors (in the form of business-to-business or business-to-consumers relationships, and secondarily, to relationships between private actors and government bodies (in the form of business-to-government). Taken together they help to embed the emergence of recent macro-regulatory terms like 'nodal governance', 'Internet governance' and 'transnational private regulation' (Braithwaite 2008; Abbott and Sindal 2009; Calliess and Zumbansen 2010; Cafaggi 2011).

As we have attempted to show, ICANN is an illustration par excellence of the complexity and dynamics of a transnational private regulator. The organization of ICANN is also intricate and difficult to decipher (Bygrave and Michaelsen 2009: 106–110). This reflects the cornucopia of stakeholders that make up ICANN's raison d'être and its commitment to policymaking through broad consensus. An enduring criticism of ICANN is the lack of appeal processes to another body with the power to overturn them. Although a policy proposal may emerge with broad agreement from the constituencies concerned, it is the ICANN Board's decision alone to adopt or reject the proposal.[39] Although several mechanisms exist for reviewing Board decisions, none of these create legally binding outcomes (Weber and Gunnarson 2013: 11–12). Non-commercial user constituencies at ICANN exist solely to curb the influence of those stakeholders at ICANN that maintain considerable economic and political clout. Their function is to carve out a space for individual rights and individual registrants against excessive claims by rights-owners and governments. For example, the Non-commercial Stakeholder Group (NCSG) spent seven weeks in negotiations with other stakeholder groups to try to balance the rights of intellectual property owners with those of new and small businesses, other non-commercial entities, various users, and the registry/registrar communities.

The NCSG is only one example of civil society's role in 'checking' more traditional power structures. Civil society is no longer just a term used to aggregate non-governmental and non-commercial entities together. Groups like Privacy International, the ORG, and the Electronic Frontier Foundation exist to ensure accountability exists on two levels: organizational accountability to the stated purpose and function of the actor and procedural accountability to the behaviour and actions of internal management. Arguably, the increased role of civil society has come about in response to an increasing number of legal agreements falling under the 'soft law' umbrella, away from traditional statutory instruments. As a result, there is an inherent difficulty in establishing clear legal lines as to what legal instrument regulates what actor in the online environment. Soft law measures have incredible influence in changing established revenue streams (consider our earlier discussion

on the financial consequences for a site blocked by an S97A order) or basic human rights (consider legislation on data privacy). The fluidity of political constellations can also force a change to the way civil society interacts with other actors in the online environment (for example, the replacement of the Joint Project Agreement between the US government and ICANN by the Affirmation of Commitments).

Sometimes civil society will be instrumental in pushing back against 'soft law' measures deployed by and over non-state actors. Sometimes soft law helps to shape the continuing nuances of online communication. While the Internet is said by some to be the great facilitator of freedom of expression, governments are constantly seeking to limit this right in line with the demands of their citizens; for example, passing measures to combat Internet facilitated crime unique to the modern era like cyberbullying, trolling, and revenge porn. However, we find ourselves concluding that whenever regulators needed 'hard law' to exercise fine-grained control tailored to the needs of a particular platform, service, or online community, contract law is most often deployed. Statutory forms of control over non-state actors remains largely an option of 'last resort', used mostly in an indirect fashion and designed to leverage control through the structural features of either the network or the market. This is seen in our study through the activities of the EU Directorate-General for Competition in regulating the market for media players and Internet browsers, and represented currently by the DG-COMP investigations into Google. Such interventions remain rare and given their complexity and costs are only exercised where all other solutions have run out. Non-state, decentred, and intermediary control are likely to remain at the heart of online regulation and governance for some time to come.

Notes

1. A suitable definition of regulation is difficult given the wide range of understandings about what the term 'regulation' means. The editors of this volume suggest contributors adopt the definition offered by Philip Selznick, and subsequently refined by Julia Black as 'the intentional use of authority to affect behaviour of a different party according to set standards, involving instruments of information-gathering and behaviour modification' (Black 2002). On this understanding of regulation, law is but one means by which purposive attempts may be made to shape behaviour and social outcomes, but there may be many others, including the market, social norms and through technology itself. The term governance is if anything less well established. Again the editors suggest the adoption of governance (alongside government) as concerned with the provision and distribution of goods and services, as well as their regulation. Hence regulation is conceived as that large subset of governance that is primarily concerned with the purposive steering of the flow of events and behaviour, as opposed to providing and distributing (Braithwaite et al. 2007). The authors of this chapter are happy to adopt these definitions.

2. The importance of the actor in an actor–network is acknowledged elsewhere by the authors. Andrew Murray, *The Regulation of Cyberspace* (Routledge-Cavendish 2006); Andrew D Murray, 'Nodes and Gravity in Virtual Space' (2011) 5 Legisprudence 195; Mark Leiser, 'The Problem with "Dots": Questioning the Role of Rationality in the Online Environment', (2016) 30 International Rev L Computers and Technology 1.
3. ITU, 'Internet Policy and Governance' <http://www.itu.int/en/action/internet/Pages/default.aspx>accessed 19 September 2016
4. ICANN, 'Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers' (1998) <https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en> accessed 19 September 2016; the Internet Society, 'Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority' (2000) <https://tools.ietf.org/html/rfc2860>accessed 19 September 2016
5. Dual-use technologies can be applied to both civilian and military use. Export licences are required for the international trade in such items. Annex to the Commission Delegated Regulation amending Council Regulation (EC) No. 428/2009 setting up a Community regime for the control of exports, transfer, brokering, and transit of dual-use items C(2014) 7567 final.
6. It should be acknowledged that Google report that the Google Glass project is ongoing but details of product development or release dates for a new version of Glass are limited. What reports have come out suggest the new version will be an optimized version for use in the workplace by for example doctors, builders, or warehouse workers rather than for general sale.
7. *Kaschke* v. *Gray and Hilton* [2010] EWHC 690 (QB).
8. *Tamiz* v. *Google* [2013] EWCA Civ 68; *Davison* v. *Habeeb* [2011] EWHC 3031 (QB); *L'Oréal* v. *eBay* [2012] All ER (EC) 501.
9. Compare *Metropolitan International Schools Ltd* v. *Designtechnica Corp* [2009] EWHC 1765 (QB) where Eady J commented *obiter* that Google did not qualify as a mere conduit, cache, or host of content under the Regulations with *Google France, Google, Inc*. v. *Louis Vuitton Malletier* [2011] All ER (EC) 411 where the ECJ held that Google is an IISP to whom the limitation of liability provisions apply.
10. This defence is defeated if the claimant shows: (a) the person who posted the statement is anonymous; (b) the claimant gave the operator a notice of complaint in relation to the statement; and (c) the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations.
11. *Delfi AS* v. *Estonia* [2013] ECHR 941.
12. *Twentieth Century Fox Film Corp* v. *British Telecommunications plc* [2011] EWHC 1981 (Ch); *Twentieth Century Fox Film Corp* v. *British Telecommunications plc (No. 2)* [2011] EWHC 2714 (Ch); *Dramatico Entertainment Ltd* v. *British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch); *Dramatico Entertainment Ltd* v. *British Sky Broadcasting Ltd (No. 2)* [2012] EWHC 1152 (Ch); *EMI Records Ltd* v. *British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch); *Football Association Premier League Ltd* v. *British Sky Broadcasting Ltd* [2013] EWHC 2058 (Ch); *Paramount Home Entertainment International Ltd* v. *British Sky Broadcasting Ltd* [2013] EWHC 3479 (Ch); and *Twentieth Century Fox Film Corporation & Ors* v. *Sky UK Ltd & Ors* [2015] EWHC 1082 (Ch).
13. In a test case, *Cartier International AG and others* v. *British Sky Broadcasting and others* [2016] EWCA Civ 658 the Court of Appeal upheld the decision of the High Court

([2014] EWHC3354 (CH)) to award an injunction under s. 37(1) of the Supreme Courts Act 1981 against a group of websites which advertise and sell counterfeit goods indicating that, in certain circumstances, the courts would implement s. 97A-style blocking orders under the general powers given to the court under the Supreme Court Act to protect trademark owners.

14. Art. 11 of the Enforcement Directive has to be read subject to Art. 3(2).
15. Spotify, 'Information' <https://press.spotify.com/uk/about/>(information correct on 19 September 2016) accessed 19 September 2016
16. Netflix, 'Overview' <https://ir.netflix.com/> (correct on 19 September 2016) accessed 19 September 2016
17. The term enrolled, as opposed to captured, represents the enrolment of West Coast codemakers in the regulatory ambitions of East Coast codemakers. This concept draws upon Julia Black's helpful notion of enrolment as outlined in Black (2003).
18. Litigation in this series of cases encompasses South Korea, Japan, Germany, France, Italy, the Netherlands, Australia, England, and Wales (*Samsung Electronics (UK) Ltd* v. *Apple Inc*. [2012] EWHC 1882 (Pat)) and the United States (*Apple Inc*. v. *Samsung Electronics Co. Ltd* et al. C 11-1846 and C 12-0630, ND Calif. (2012)).
19. GA Tech, 'GVU's First WWW User Survey Results' (1 January 1994) http://www.cc.gatech.edu/gvu/user_surveys/survey-01-1994/ accessed 19 September 2016
20. GA Tech, 'GVU's Fifth WWW User Survey Results: Browser Expected to Use in 12 Months' (10 April 1996) <http://www.cc.gatech.edu/gvu/user_surveys/survey-04-1996/graphs/use/intend_browser.html> accessed 19 September 2016
21. Ed Kubaitis, 'Browser Statistics for October 1998' (*EWS Web Archive*) <http://web.archive.org/web/20010507151253/http://www.ews.uiuc.edu/bstats/months/9810-month.html> accessed 19 September 2016
22. OneStat.com, 'Microsoft's IE 6.0 is the most popular browser on the web' (29 April 2002) <http://www.onestat.com/html/aboutus_pressbox4.html> accessed 19 September 2016
23. Commission Decision of 24 May 2004 relating to a proceeding pursuant to Article 82 of the EC Treaty and Article 54 of the EEA Agreement against Microsoft Corporation (Case COMP/C-3/37.792—Microsoft) (2007/53/EC).
24. Commission of the European Union, 'Antitrust: Commission imposes €899 million penalty on Microsoft for non-compliance with March 2004 Decision' (27 February 2008) <http://europa.eu/rapid/press-release_IP-08-318_en.htm> accessed 25 October 2015; T-167/08 *Microsoft Corp* v. *European Commission* [2012] 5 CMLR 15
25. Commission of the European Union, 'Antitrust: Commission fines Microsoft for non-compliance with browser choice commitments' (6 March 2013) <http://europa.eu/rapid/press-release_IP-13-196_en.htm> accessed 19 September 2016
26. W3C, 'August 2016 Market Share' (31 August 2016) <https://www.w3counter.com/globalstats.php?year=2016&month=8> accessed 19 September 2016
27. Net Market Share (19 September 2016) <https://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=0> accessed 19 September 2016
28. Website Optimization, 'Apple iTunes Penetration Closing Gap with Microsoft—April 2011 Bandwidth Report' (April 2011) <http://www.websiteoptimization.com/bw/1104/> accessed 19 September 2016
29. sTLDs was shorthand for sponsored TLDs, gTLDs with a sponsor applicant. ICANN, 'Correspondence from GAC Chairman to the ICANN CEO' (3 April 2005) <https://

www.icann.org/en/system/files/files/tarmizi-to-twomey-03apr05-en.pdf.> accessed 19 September 2016

30. ICANN, 'Approved Board Resolutions—Singapore' (20 June 2011) <https://www.icann.org/resources/board-material/resolutions-2011-06-20-en> accessed 19 September 2016
31. ICANN, '~~500+ New gTLDs Introduced into the Internet~~' ~~(6 February 2015) <https://www.icann.org/news/announcement-2-2015-02-06-en~~> accessed ~~19 September 2016~~
32. The full list is at ICANN, 'Delegated Strings' (2016) <http://newgtlds.icann.org/en/program-status/delegated-strings> accessed 19 September 2016
33. ICANN, 'GAC indicative scorecard on new gTLD outstanding issues listed in the GAC Cartagena Communiqué' (23 February 2011) <https://archive.icann.org/en/topics/new-gtlds/gac-scorecard-23feb11-en.pdf> accessed 19 September 2016; ICANN, 'ICANN Board Notes on the GAC New gTLDs Scorecard' (4 March 2011) <https://archive.icann.org/en/topics/new-gtlds/board-notes-gac-scorecard-04mar11-en.pdf> accessed 19 September 2016
34. European Commission, 'Evidence for necessity of data retention in the EU' (2 March 2013) <http://www.statewatch.org/news/2013/aug/eu-com-mand-ret-briefing.pdf> accessed 19 September 2016
35. Romanian Constitutional Court Decision no. 1258 (18 October 2009)
36. Bundesverfassungsgericht, 'Leitsätze' <http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html> accessed 19 September 2016
37. European Parliament News, 'MEPs cast doubt on controversial rules for keeping data on phone and Internet use' (*European Parliament*, 25 October 2015) <http://www.europarl.europa.eu/news/en/news-room/content/20121019STO53997/html/MEPs-cast-doubt-on-controversial-rules-to-keep-data-on-phone-and-internet-use> accessed 19 September 2016
38. BvR 370/07 and 1 BvR 595/07.
39. For example, a review may occur through a 'Request for Reconsideration' directed to the Board Governance Committee (Bylaws Art IX(2)) or lodging a complaint with the ICANN Ombudsman (Bylaws Art V).

References

Abbott K and D Sindal, 'Strengthening International Regulation through Transnational New Governance: Overcoming the Orchestration Deficit' (2009) 42 Vanderbilt J Transnational L 501

Ahlborn C and D Evans, 'The Microsoft Judgment and Its Implications for Competition Policy towards Dominant Firms in Europe' (2009) 76 Antitrust LJ 887

Ayres I and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992)

Baldwin R and J Black, 'Really Responsive Regulation' (2008) 71 MLR 59

Berkman Centre for Internet & Society, 'Accountability and Transparency at ICANN: An Independent Review, Appendix D: The.xxx Domain Case and ICANN Decision-Making

Processes' (20 October 2010) <http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixD_xxx.pdf> accessed 19 September 2016

Black J, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 Current Legal Problems 103

Black J, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1

Black J, 'Enrolling Actors in Regulatory Systems: Examples from the UK Financial Services Regulation' (2003) Public Law SPR 63

Black J, 'Risk-based Regulation: Choices, Practices and Lessons Learnt' in Organisation for Economic Co-operation and Development (ed), *Risk and Regulatory Policy: Improving the Governance of Risk* (OECD 2010)

Braithwaite J, G Coglianese, and D Levi-Faur, 'Can Regulation and Governance make a Difference' (2007) 1 Regulation and Governance 7

Braithwaite J, *Regulatory Capitalism: How It works, Ideas for Making It Work Better* (Edward Elgar Publishing 2008)

BT, *Blocking categories on Parental Controls* (2015) <http://bt.custhelp.com/app/answers/detail/a_id/46809/~/blocking-categories-on-parental-controls> accessed 19 September 2016

Burris S, P Drahos, and C Shearing, 'Nodal Governance' (2005) 30 Australian Journal of Legal Philosophy 30

Bygrave L and T Michaelsen, 'Governors of Internet' in Lee Bygrave and Jon Bing (eds), *Internet Governance: Infrastructure and Institutions* (OUP 2009)

Cafaggi F, 'New foundations of Transnational Private Regulation' (2011) 38 JLS 20

Calliess G and P Zumbansen, *Rough Consensus and Running Code: A Theory of Transnational Private Law* (Hart Publishing 2010)

Chin A, 'Decoding Microsoft: A First Principles Approach' (2005) 40 Wake Forest L Rev 1

Christensen C, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Harvard Business School Press 1997)

Clark L, 'UK Gov wants "unsavoury" web content censored' (*Wired*, 15 March 2014) <www.wired.co.uk/news/archive/2014-03/15/government-web-censorship> accessed 19 September 2016

DeNardis L, *The Global War for Internet Governance* (Yale UP 2014)

Easterbrook F, 'Cyberspace and the Law of the Horse' (1996) University of Chicago Legal Forum 207

Economides N and I Lianos, 'The Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases' (2009) 76 Antitrust Law Journal 483

Ellul J, *La technique, ou, L'enjeu du siècle* (Armand Colin 1954)

European Commission, 'Evidence for necessity of data retention in the EU' (2013) <http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf> accessed 19 September 2016

Froomkin M, 'Wrong Turn in Cyberspace: Using ICANN to Route around the APA and the Constitution' (2000) 50 Duke Law Journal 17

Froomkin M, 'ICANN Governance' (Senate Commerce, Science and Transportation Committee Communications Subcommittee, 14 February 2001) <https://w2.eff.org/Infrastructure/DNS_control/ICANN_IANA_IAHC/20010214_icann_sen_hearing/0214fro.pdf> accessed 19 September 2016

Froomkin M, 'ICANN and the Domain Name System after the "Affirmation of Commitments"' in Ian Brown (ed) *Research Handbook on Governance of the Internet* (Edward Elgar Publishing 2013)

Gibbs M (1997), 'New gTLDs: Compromise and Confusion on the Internet' *Network World* (17 February 1997) 50

Goldsmith J and T Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006)

Gunningham N, P Grabosky, and D Sinclair, *Smart Regulation: Designing Environmental Policy* (OUP 1998)

Gutwirth S, P De Hert, and L De Sutter, 'The Trouble with Technology Regulation from a Legal Perspective: Why Lessig's "Optimal Mix" Will Not Work' in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008)

Halvorson T and others, 'The BIZ Top Level Domain: Ten Years Later', (2012) 7192 Passive and Active Measurement: Lecture Notes in Computer Science 221

Hanseth O and E Monteiro, *Understanding Information Infrastructure* (1998) <www.researchgate.net/publication/265066841_Understanding_Information_Infrastructure> 19 September 2016

Heiner D, 'Working to Fulfill our Legal Obligations in Europe for Windows 7' (*Microsoft Blogs*, 11 June 2009) <http://blogs.microsoft.com/on-the-issues/2009/06/11/working-to-fulfill-our-legal-obligations-in-europe-for-windows-7/> 19 September 2016

Hunter D, 'ICANN and the Concept of Democratic Deficit' (2003) 36 Loyola of Los Angeles Law Review 1149

Jenkins G and R Bing, 'Microsoft's Monopoly: Anti-Competitive Behavior, Predatory Tactics, and the Failure of Governmental Will' (2007) 5 Journal of Business & Economic Research 11

Johnson D and D Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367

Knill C and D Lehmkuhl, 'Private Actors and the State: Internationalization and Changing Patterns of Governance' (2002) 15 Governance 41

Koops B, M Hildebrandt, and D Jaquet-Chiffelle, 'Bridging the Accountability Gap: Rights for New Entities in the Information Society?' (2010) 11 Minnesota Journal of Law Science & Technology 497

Koppell J, 'Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder"' (2005) 65 Public Administration Review 94

Kuhn T, *The Structure of Scientific Revolutions* (University of Chicago Press 1962)

Laidlaw E, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (CUP 2015)

Latour B, 'On Actor-Network Theory: A Few Clarifications' (1996) 47 Soziale Welt 369

Latour B, *Reassembling the Social: An Introduction to Actor-Network-Theory* (OUP 2005)

Lessig L, *Code Ver 2.0* (rev edn, Basic Books 2006)

Levine J, 'Time to Renew.coop,.museum, and.aero ICANN' (*Circle ID: Internet Infrastructure*, December 31, 2005) <www.circleid.com/posts/time_to_renew_coop_museum_and_aero_icann/> accessed 19 September 2016

McCullagh D, 'U.S. seeks veto powers over new domain names' (*CNET*, 7 February 2011) <www.cnet.com/news/u-s-seeks-veto-powers-over-new-domain-names/> accessed 19 September 2016

Morgan B and K Yeung, *An Introduction to Law and Regulation: Text & Materials* (CUP 2007)

Mueller M, 'ICANN and Internet Governance Sorting through the Debris of "Self-Regulation"', (1999) 1 Info, the Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media 497

Mueller M, *Networks and States: The Global Politics of Internet Governance* (MIT Press 2010)

Mueller M and B Kuerbis, 'Towards Global Internet Governance: How to End U.S. Control of ICANN without Sacrificing Stability, Freedom or Accountability' (TPRC Conference Paper, 27 August 2014) <http://ssrn.com/abstract=2408226> accessed 19 September 2016

Murray A, 'Internet Domain Names: The Trade Mark Challenge' (1998) 6 International J L Info Technology 285

Murray A, *The Regulation of Cyberspace* (Routledge-Cavendish 2006)

Nicholls T, 'An Empirical Analysis of Internet Top-level Domain Policy' (2013) 3 J Information Policy 464

NTIA, 'A Proposal to Improve Technical Management of Internet Names and Addresses' (Discussion Draft, 13 January 1998) <www.ntia.doc.gov/legacy/ntiahome/domainname/dnsdrft.htm> 19 September 2016

Organisation for Economic Co-operation and Development, 'The Role of Internet Intermediaries in Advancing Public Policy Objectives: Forging Partnerships for Advancing Policy Objectives for the Internet Economy, Part II' (DSTI/ICCP (2010)11/FINAL, 2011) <http://www.oecd.org/internet/ieconomy/48685066.pdf > accessed 19 September 2016

Pickard V, 'Neoliberal Visions and Revisions in Global Communications Policy: From NWICO to WSIS' (2007) 31 Journal of Communication Inquiry 118

Sartor G, 'Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents' (2009) 17 Artificial Intelligence and Law 253

Schumpeter J, *Capitalism, Socialism and Democracy* (Harper & Brothers 1942)

Shearing C and J Wood, 'Nodal Governance, Democracy, and the New "Denizens"' (2003) 30 JLS 400

Sunstein C, 'Empirically Informed Regulation' (2011) 78 University of Chicago L Rev 1349

Sunstein C and R Thaler, 'Libertarian Paternalism is Not an Oxymoron' (2003) 70 University of Chicago L Rev 1159

Take I, 'Regulating the Internet Infrastructure: A Comparative Appraisal of the Legitimacy of ICANN, ITU, and the WSIS' (2012) 6 Regulation & Governance 499

Teubner G, 'Societal Constitutionalism: Alternatives to the State-Centred Constitutional Theory?' in Christian Joerges, Inge-Johanne Sand and Gunther Teubner (eds), *Transnational Governance and Constitutionalism* (Hart Publishing 2004)

Teubner G, 'Rights of Non-Humans? Electronic Agents and Animals as New Actors in Politics and Law' (2006) 33 JLS 497

United Nations, 'Resolution of the General Assembly, 18 December 2013: The Right to Privacy in the Digital Age' A/RES/68/167 <www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167> accessed 19 September 2016

United Nations, 'The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights' 2014 A/HRC/27/37 <www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf> accessed 19 September 2016

Weber R and S Gunnarson, 'A Constitutional Solution for Internet Governance' (2013) 14 Columbia Science & Technology Law Review 1

Weinberg J, 'Governments, Privatization, and Privatization: ICANN and the GAC' (2011) 18 Michigan Telecommunications and Technology Law Review 189
Wu T, 'When Code Isn't Law', (2003) 89 Virginia Law Review 679
Zittrain J, *The Future of the Internet and How to Stop It?* (Yale UP and Penguin UK 2008)

Further Reading

Bernstein S, 'Legitimacy in Intergovernmental and Non-State Global Governance' (2011) 18 Review of International Political Economy 17
Drezner D, 'The Global Governance of the Internet: Bringing the State Back in' (2004) 119 Political Science Quarterly 477
Grabosky P, 'Beyond Responsive Regulation: The Expanding Role of Non-State Actors in the Regulatory Process' (2013) 7 Regulation & Governance 114
Laidlaw E, 'A Framework for Identifying Internet Information Gatekeepers' (2010) 24 International Review of Law Computers & Technology 263
Perritt H, 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance' 5 Indiana Journal of Global Law Studies 423
Wu T, 'Cyberspace Sovereignty—The Internet and the International System' (1997) 10 Harvard Journal of Law and Technology 647