Marsden, Christopher T. "Conclusion: Towards a Co-regulatory Solution?." *Net Neutrality: Towards a Co-regulatory Solution*. London: Bloomsbury Academic, 2010. 211–236. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781849662192.ch-008>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 11:35 UTC.

Copyright © Christopher T. Marsden 2010. You may share this work for non-commercial purposes only, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

CHAPTER EIGHT

Conclusion: Towards a Co-regulatory Solution?

The time, it is to be hoped, is gone by when any defence would be necessary of the 'liberty of the press' as one of the securities against corrupt or tyrannical government. ... It is as noxious, or more noxious, when exerted in accordance with public opinion, than when in opposition to it.¹

J. S. Mill

We have seen in the previous chapters that 'net neutrality' is a deceptively simple phrase hiding a multitude of meanings. First, it was unpacked in the Introduction to discover that it comprises two separate non-discrimination commitments. Backward-looking 'net neutrality lite' claims that Internet users should not be disadvantaged due to opaque and invidious practices by their current ISP. Forward-looking 'positive net neutrality' describes a practice whereby higher QoS for higher prices should be offered on FRAND terms to all-comers, a modern equivalent of common carriage. It is a more debatable principle, with many content providers and carriers preferring exclusive arrangements. We saw in Chapters 1–3 how current ISP (and government) practices have been highly deceptive in places, blocking content for specific anti-competitive and non-specific traffic management purposes. We saw that there is little 'middle-mile' competition in fixed ISP markets, even in Europe where the commitment to regulation for competition remains. We also saw that we have the worst of all possible worlds: no competition and no common carriage currently. In the remaining Chapters 4–7, we saw the attempts to at least introduce transparency into the debate, as well as the rights of end-users. Co-regulation was seen to be a prevalent but awkward compromise between state and private regulation, with constitutionally uncertain protection for end-users and a worryingly large latitude for private censorship, which has been increasing throughout the last decade even as the law declares ISPs to be 'three wise monkeys', as we saw in Chapter 4. Mobile Internet in Chapter 7 was seen to be claiming the same special protections from regulation that its forerunner, mobile voice termination, claimed, to enable walled gardens to flourish. This type of asymmetrical regulation was seen to be especially dangerous for

the future of fixed ISP net neutrality. Any solution would need to be holistic, considering ISPs' roles in the round. It needs to acknowledge Mill's point: censoring the Internet is as noxious as censoring the press was 150 years ago, especially when it is claimed to silence only those society condemns, such as copyright 'pirates', suspected paedophiles and pornographers.

I have some partial solutions but no panacea. Transparency and investigation are easy wins, principles that regulators can only discount on grounds of ignorance ('net neutrality is a solution in search of a problem') or resource depletion ('we don't regulate the Internet, it is too complicated'). It improves competitive forces, such as they are, so the pro-market advocates surely have little to disagree with, especially as it is to be achieved through co-regulatory means at lowest cost to ISPs. I grapple with the dilemma that I may be giving the ISPs a free lunch, the appearance of a solution without even a partial remedy for end-users. After all, if all ISPs are using that same backhaul pipe to the incumbent's wholesale network, how can any one offer a significantly different solution? Informing end-users that 'you can have any colour as long its black' is a hundred-year-old solution, ill-serving the twenty-first century user. The popular solution amongst academics would be to proclaim the immutable if economically inconvenient truth that information wants to be free and the Internet wants to be open. I create trouble for myself by admitting to both economic and normative rationales, each pulling in different directions, and attempt unsuccessfully to square that circle. That is why I only recommend net neutrality 'lite' – the easy backward-looking solution.

This is a policy area with no perfect solutions. Of course the Internet should be open to all, but private investment is the critical component in building a faster Internet. Of course universal service should be supported, and there must be some minimum access to the open Internet for all, whether they use a mobile 3G connection or a fast IPTV-enabled premium service. If it says 'Internet service', it should do what it says on the tin, offer an open Internet (alongside walled gardens if expressly advertised as such). I am happier limiting my conclusion to emphasize the complexity of the problem than trying to claim a one-size-fits-all solution. I am no technologist or economist though I write articles and papers jointly with some of the best, and listen closely to the others. My solutions are very much grounded in current policy realities, and that is where they offer a potential route forwards, in that they are politically feasible and desirable.

In this conclusion, there are four parts: first I try to fit the Internet to other public forums, to find out what we would be losing if net neutrality was abandoned. The second section details co-regulation as an alternative way to approach net neutrality instead of state regulation. The two sections together are an attempt to make politicians understand what ‘net neutrality lite’ is for, and that it is a partial solution worth having, and which co-regulatory methods are needed to get there. I discuss the need for a users’ Internet Bill of Rights, and the very apparent global problems that private or ‘co-regulated’ filtering and censorship cause, whether for private ends such as copyright enforcement or public ends such as restricting freedom of expression, as well as the potential impact on developing countries. Finally, I sum up by looking at what evidence may be needed for regulators to address net neutrality policy discussion. As others have warned, when policy makers collude in private Internet censoring, they should be careful what they wish for.

The Open Internet and the Public Forum

Is the open public Internet ‘just’ a pub with its beers, pay-TV and gossip? Or is it a coffee house with information trading, innovative discussion and WiFi? Neither comparison rings entirely true, and the ‘Wealth of Networks’ analysis of Benkler thinks of it as a giant experiment, combining laboratory with user innovation and feedback, as well as those other things, while Boyle describes a wider movement ‘Enclosing the Commons of the Mind’ and Post extends a comparison with Jeffersonian America.² It is certainly very complex and may well have bottleneck characteristics which mean that any tinkering by regulators just moves the problem elsewhere – as Odlyzko suggests, perhaps from ISPs to Google or ESPN. The open Internet is, it is constantly said, a commons. That is the basis for claims that it should be preserved and regulation induced to prevent any more enclosure of that commons, while at the same time ensuring that the commons is not ruined by free-riders, that there is no ‘tragedy of the commons’. Net neutrality is, in its various guises, an attempt to preserve the public space for the public benefit, whether as a modern Speaker’s Corner in the many voices authoring blogs, or in common carriage rules intended to remind the carriers of this commons that they have special rights and responsibilities, as we saw in Chapter 2. Just like Speaker’s Corner, the open Internet is by no means the only, or – some might say – the

most important place for public opinion to be formed, but it has so far been more or less guaranteed free and open to those with a computer and ISP. In physical space, there are private members' clubs and working men's clubs, Methodist chapels and Friendly Societies, professional associations, country and golf clubs, Freemasons and Opus Dei all have their place, but it is the open public space that gives legitimacy to all these private or semi-private spaces: it is the guarantor of free speech for the others. That all sounds rather grand and pompous, so let us bring it down to Earth for this conclusion. Let us compare this populist but technologically enabled space, the Internet, to one of its forerunners. Let's go to the pub.

British public houses are – as we saw in the common carriage discussion in Chapter 2 – granted special rights and given special duties, primarily that to accommodate all-comers who so request. How does the Internet currently resemble a pub? It has its share of gaming³ and gambling, of queuing and noise, of public lounge and saloon, of the snug (in certain areas), of spam, of video, of music, of piracy (those smuggled CDs), and of course many people of a religious persuasion are convinced it's a den of vice – it certainly is a place to meet romantically (or otherwise). It has its private privileged alternatives – the members' club, the nightclub with its VIP room, the other more private spaces with their reserved tables and guest lists. It is related to the coffee houses which provided the first insurance (Lloyds) and stock market speculation in London. It is a place for all people and all seasons. It is also the place for debate and conflict, even violence and police response. More libel is committed in an evening's 'character assassination' in a local pub than in a year of a newspaper, hence the popularity of the widest viewed English language soap opera, 'Coronation Street' and its ubiquitous gossiping in the 'Rovers Return' pub. The pub is monitored in several ways: first the police license its hours and services; second, police make (somewhat) random visits to check on activities; third, publicans in the United Kingdom often install video cameras to film the entrance. Furthermore, popular pubs have security guards on busy evenings. You might say that the surveillance is as methodical here as on the Internet. We accept these measures of surveillance – though both cameras and security guards (who are now licensed by a regulator to ensure they are fit and proper persons) as well as some licensing authority decisions continue to grate.

Pubs, like ISPs and Internet content providers, have complex economic value chains which constantly threaten the independence of the local public

house. Parliament has continually intervened in the past twenty years to ensure that the ideal of the public house, the common carrier, as a public space, is maintained with at least some defence against the tyranny of the economics of scale and scope that tend towards the concentration of pubs with brewers in vertically integrated national or even multinational conglomerates. The idea that pubs are 'free houses' unconnected to each other and selling any beer or other service they wish is a romantic but false idea, and many pubs are parts of chains tied in one way or another to each other, or vertically integrated with beer suppliers. However, rules prevent over-monopolization of this market, and untied pubs and guest beers predominate since the abuses of competition were recognized and acted upon in the early 1990s.⁴ Radical regulatory action saved pubs: the Monopolies and Mergers Commission (MMC) investigated the market.⁵ Its report found a complex monopoly existed in favour of brewers who owned tied houses or who had tying agreements with free houses in return for loans (brewer loans) at favourable interest rates. MMC recommended barring any one brewing company owning more than 2,000 licensed pubs. Government followed this advice: the Beer Orders⁶ modified the recommendations of the MMC report. The Office of Fair Trading in 2000 concluded that there seemed to be a reasonable amount of competition nationally, even if some regional and local concentration existed, and government followed its advice and revoked most of the Beer Orders.⁷ In 2009, Parliament once again investigated pubs,⁸ and after nearly a decade of deregulation their findings were different. Parliament urged self-regulation by pub chains to be taken more seriously:

Since the British Beer & Pub Association code of practice was updated in 1997 the industry has changed and we suggest that this code of practice should be revised ... if the industry does not show signs of accepting and complying with an adequate voluntary code then the Government should not hesitate to impose a statutory code on it.

They recommended urgent government action to the industry, not relying on the previous light mixture of regulation and self-regulation. Pubs are by no means a common agora and debating house paradise lost, but the mix of law enforcement, licensing and pro-competitive changes has restored some tenuous vitality and independence to the trade.

I raise the pub issue not only because of certain similarities of economics and speech freedoms associated with both the Internet and pubs historically, but also to illustrate the specific, sustained and careful consideration which Parliament has given to maintaining some openness in the industry. If it is willing to devote such time and energy to pubs on behalf of one part of its electorate, can it not also find resources to devote to fully exploring net neutrality and the Internet? The Internet's core values of openness and democracy have been established by accident and design. Horten states:⁹

By authorizing blocking practices, the Telecoms Package puts Europe on a path to a closed series of Internets. It puts at risk innovation, trade, and any policy goals to encourage cross-border trade. It puts at risk the European Union's Information Society goals. And, it stands to chill democratic speech.

Strong arguments remain for checking closely that ISPs inform consumers when they reach caps, and for ensuring we do not return to rationed Internet use as we did in the 1990s with dial-up – Martin Cave and AOL helped start FRIACO in 2000, let us not abandon flat rate pricing now!¹⁰

Medium Law

The future of the Internet is a non-trivial issue,¹¹ in fact it is central to the future of productivity in most industries. It is an enabling technology, which means that the exchange of information on this open platform promises (and delivers) real efficiencies in the economy and society generally, as it helps collaboration and improvement.¹² It is also socially enabling – whatever your view – for all the reasons encompassed in the expression 'Web 2.0' or 'the participative web'.¹³ That is, it has become a virtual playground, classroom, laboratory and at its most basic – chatroom. The rise in the number of people using email, Facebook, MySpace, Wikipedia, Skype, Instant Messaging and other applications has extended so far into mass participation that it has truly affected society and the economy in all its facets. Children, in particular, are now 'born digital' in many locales in developed society,¹⁴ and their access to the consumer Internet is an essential part of their development, as Pew Internet surveys and others increasingly show. Moreover, small businesses and solo home-based workers depend on this tool as a vital part of their participation in the economy.¹⁵ The promise of virtual worlds and massive online collaboration

(not just the Web, but online gaming, Wikipedia-type knowledge sharing and transfer and other avatar environments including over-hyped but fascinating poster child of digital life, SecondLife) is to extend this pervasive impact of online environments even further in the coming decade.

The Internet matters far more than television or radio or the simple telephone, whatever technology debunkers may continue to claim. Of course it is true that many collaborators and innovators use very powerful Internet connections at school, university and in office environments. However, much of their out-of-work collaboration, and creativity and innovation, take place using consumer Internet connections via desktop computers, laptops, netbooks and smart 3G mobile phones. Therefore, the question of what happens to their 'domestic' Internet connection is vital. Yes, it should be faster, but should this speed increase be entirely to guarantee the existing ISPs' phone quality and video service? How much of the increase should be 'open' to all Internet traffic, and how much a toll lane for reserved high-speed signals? Note that this open question is posed in terms of proportion, not absolutes. I state immediately that I do not believe in social or economic justifications either for barring any proprietary high-speed traffic at all, or for strict versions of net neutrality that would not allow any traffic prioritization. It appears to me that there is too much at stake to either expect government to supplant the market in providing higher-speed connections or for the market to continue to deliver openness without the most basic of policy and regulatory backstops to ensure some growth.

The legal policy and regulatory implications of rapidly standardizing innovation on the communications ecology were well understood by Benkler who was concerned with the need to maintain interoperability and openness to ensure a 'commons' in which unaffiliated and non-commercial innovation could flourish (building on de Sola Pool).¹⁶ So this is important, it is not just another industry and it is becoming more important, not less. That also means it is infusing our society and polity as well as the economic relationships we have.¹⁷ Therefore, we are not simply considering economic analysis of bottlenecks in another transport-based industry, or a convergence of regulation between television and the Internet, but regulating the global Information Society. I moved on from competition analysis of bottlenecks a decade ago to the wider, you might say meta-narrative, and if it was impossible then to separate the economic and wider policy considerations of the consumer Internet, how much more so is that the case today? That is

not to say that much good work is not being done in economic analysis of networks, when it so clearly is, but to attempt to partition net neutrality – which is to say, the future of content on the Internet – as simply an economic issue just won't wash. Noam states:

There is nothing especially new about [media law's] recent round net-neutrality as a conceptual issue, or in terms of its policy options, except for the terminology.¹⁸

This is a debate about media law as much as telecoms law, and given that the Internet can carry almost previous forms of media with great efficiency, making its regulation 'Medium Law'.¹⁹

There used to be separation between telecommunications and e-commerce law: no longer. Where content providers – newspapers, TV companies, search and e-commerce providers, and those making user generated content – formerly paid a flat rate to access the Internet based on the same service, that may no longer be the case on the next generation of Internet services. As a result, those most able and willing to pay may receive first-class service, while other content travels in the slow lane, where ISPs can track the incoming traffic. This trend is not just a telecoms dispute, but affects all online content and e-commerce providers. As that effectively is every major provider of content and commerce, it means medium law (i.e. mass market content online that formerly used several media) is intimately tied into telecoms law. Furthermore, security and anti-terrorist measures are also driving ISPs towards filtering all incoming traffic. This may change the entire architecture of the Internet, its business model and freedom of speech. It is happening beyond the analysis of the discrete fields of information security, e-commerce law, media law and telecoms law. It could overwhelm all those areas. It could be a 'perfect storm'.

Regulatory analysts often 'don't get it' because they focus on narrow questions of telecoms regulation. There are at least two other critical factors at play: concern over illegal and inappropriate content (such as child pornography, music protected by copyright and latterly video files being inappropriately shared, and malware including spam), and the security agenda which aims to enforce QoS to separate 'good' or preferred from 'bad' or discriminated-against packets. There is a legitimate concern that this represents a division between the rich and powerful senders of packets and the lesser content types. These three policy areas, telecoms, content and security regulation,

have come together. Policies made in their respective arenas tend to the same result in terms of incentives to deploy NGNs which could change the Internet forever, to become faster and safer but more closed.

As the law and practice stands today, it seems most customers do not know when they have been targeted as over-strenuous users of the Internet. Once targeted, customers generally cannot prove their ‘innocence’ – they have to accept the terms of use of the ISP without appeal (except theoretically via courts for breach of contract, or regulator for infringement of their consumer rights). The number of alternative ISPs is small and shrinking – not only is the ISP business expensive, leading to concentration in the industry, but the costs of renting backhaul from dominant operators is – as we saw in the UK case in Chapter 3 – sufficiently high that no-one would want to offer service to a suspected ‘bandwidth hog’. We may expect to see more protest behaviour by ‘netizens’ who do not agree with a law or policy, especially where ISPs are seen to have failed to fully inform end-users about the implications of policy changes. Regulators (and their political equivalents) will not be able to ignore such problems.²⁰ The Pirate Party MEPs in the European Parliament 2009–14 will make sure of that.

Globalization and Net Neutrality

The book of that conference a decade ago which I discussed in the opening chapter, was called ‘Regulating the Global Information Society’ – ten years on, the problems of development and the global Digital Divide have become yet more pressing. Net neutrality is very definitely a global issue as two examples indicate.²¹ Internet connectivity is still very expensive for most developing countries, despite attempts to ensure local Internet-peering points (exchanges) and new undersea cables. To flood the existing and then new links with an exaflood of traffic, much of which came from major video production countries such as India, Nigeria and of course Hollywood, could place the local ISPs in serious financial peril. Casualties in such undertakings include for instance countries blacklisted by major ISPs for producing large amounts of spam: imagine as a Nigerian consumer how you would feel if your ISP was blacklisted in your relatives’ country, blocking your email, simply because the ISP you use is also used by spammers.

The second development problem that net neutrality debate centres on is the wireless Internet. Most developing countries’ citizens have much lower bandwidth than the West, and most of their connectivity is mobile: India is

probably the poster child for a country with at least ten times more mobile than fixed phone subscribers. There is a straight race ongoing here between free WiFi and WiMAX projects that are accompanying initiatives such as local variants of the \$100 Laptop, and the type of walled garden, low-speed Internet access that mobile providers have until now been providing. In the next several years, the developing world Internet user is going to try to test the limits of mobile networks to their maximum, and capacity as well as price might determine the extent to which they can expect a rapidly developing or a Third World Internet experience.

In this conclusion, I flag up development issues because they are critical. Universal service is still a pipedream for many in the developing world, and when that arrives, the definition it is given will determine the minimum threshold that ISPs have to achieve. As Mueller states, net neutrality ‘must also encompass a positive assertion of the broader social, economic and political value of universal and non-discriminatory access to Internet resources among those connected to the Internet.’²² The types of non-net neutrality employed in China and Iran in June 2009 were not economically motivated, but political censorship designed to prevent citizens’ access to foreign discussion of the twentieth anniversary of the Tiananmen Square massacre, and the closely contested Presidential elections, respectively. Mueller claims that the tendency of governments in both repressive and traditionally democratic regimes to impose liability on ISPs to censor content for the plethora of reasons we discussed in the last three chapters argues for a policy of robust non-interference:

The flip side of an NN policy that valorizes the right of Internet users to access each other without interference from intermediaries is the belief that network users wronged by other users must hold the wrongdoer responsible – not the intermediary network operator.²³

This is especially valuable in countries where there is much less discussion of how ISPs being used as censors can create unambiguous dangers to user privacy and freedom of expression. Mueller suggests that the net neutrality metaphor could be used to hold all filtering and censorship practices up to the light, as well as governance in other areas of Internet regulation, such as domain name governance. As this issue has globalized and attracted activists, it has become an important policy issue discussed at the United Nations IGF. The IGF discussions of net neutrality and other issues are expected to substantially increase in its

forthcoming meeting in Egypt in November 2009,²⁴ and it highlighted the issue in its December 2008 meeting.²⁵

Taking Co- and Self-regulation Seriously

The general trend we saw in Chapters 4–6 is towards an expansion of scope of co-regulation, often at the expense of statutory regulation. NRAs such as Ofcom in the United Kingdom are exploring the possibility of ‘sunsetting’ particular regulations in the event that co-regulatory alternatives can be found. Where there is a clear industry interest in co-regulation to improve market penetration, or to head off threats of statutory regulation, there are adequate market incentives for resources to be allocated to co-regulatory activities. However the calculation of enlightened self-interest required is vulnerable to changing personnel and market structures such that co-regulatory institutions, where they do not have access to compulsory funding, will not enjoy the funding necessary to meet standard requirements of transparency, accountability and due process. A wide variety of models of co-regulatory tools exist. Some of these are based on adequate standards of transparency, inclusion, due process, resources, and some clearly are not. There is some concern that insufficient standards apply to both law enforcement and protection of freedom of expression rights. Public harm can result.

Co-regulation expresses a form of regulation which is neither state or NRA regulation with specialized functions,²⁶ nor ‘pure’ self-regulation as observed in industry-led standard setting. The state and stakeholder groups including consumers are stated to explicitly form part of the institutional setting for regulation. Co-regulation constitutes multiple stakeholders, and this inclusiveness results in greater legitimacy claims. However, direct government involvement including sanctioning powers may result in the gains of reflexive regulation – speed of response, dynamism, international cooperation between ISPs and others – being lost. Ayres and Braithwaite stated:²⁷ ‘Practical people who are concerned with outcomes seek to understand the intricacies of interplays between state regulation and private orderings.’ Responsive or reflexive regulation reflects a more complex dynamic interaction of state and market, a break with more stable previous arrangements.²⁸ This applies to other globalizing phenomena, for instance, financial and environmental law.²⁹

Co-regulation is a vitally important concept to define, refine and examine against a rigorous methodological template. Price and Verhulst assert that there is little purity in self-regulation without at least a lurking government

threat to intervene.³⁰ The term ‘co-regulation’ encompasses a range of different regulatory phenomena, which have in common that the regulatory regime is made up of a complex interaction of general legislation and a self-regulatory body. The varying interests of actors result in different incentives to cooperate or attempt unilateral actions at the various points of the value chain.³¹ Without regulation responsive to both the single European market and the need for constitutional protection of freedom of expression at national levels, co- and self-regulatory measures cannot be self-sustaining. In the media sector since Boddewyn’s pioneering 1988 study of advertising,³² there have been many studies of co-regulation, including Tambini et al.,³³ Larouche³⁴ and those for the Council of Europe.³⁵

Schulz and Held³⁶ view self-regulation in Anglo-American debate as concerned with ‘reconciliation of private interests’ whereas their formulation – regulated self-regulation³⁷ – is indirect state regulation based on constitutional principles. It is the combination of ‘intentional self-regulation’ – the actions of market actors, whether in social or economic settings – with the state sanction in reserve which results in self-regulation ‘regulated’ by the possibility of state intervention. Schulz and Held suggest that ‘regulated self-regulation’ can be any of these categories: co-regulation, self-regulation or a third category – ‘audited self-regulation’. In the case of ISPs, audited self-regulation might involve at least a standard being set that an audit firm could certify organizations against (or at least that organizations could self-certify with reporting requirements), but could involve the setting of an international standard. At a minimum, dedicated budgetary and personnel resources, with activity reports, would be required to demonstrate regulatory commitment. The German concept of regulated self-regulation gives the state a role when basic constitutional rights need to be upheld.

A legal approach to co- and self-regulation extends from the definitions in the 2003 EU Inter-institutional Agreement.³⁹

- Co-regulation: ‘The mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field.’
- Self-regulation: ‘The possibility for economic operators, the social partners, NGOs or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practices or sectoral agreements).’

- Co-regulation and self-regulation ‘will not be applicable where fundamental rights or important political options are at stake or in situations where the rules must be applied in a uniform fashion in all Member States’.³⁹

Co-regulation in the European context must also be proportional to the aims of the legal instrument, as well as conforming to the competition law of the European Union. Enforcement is the ultimate responsibility (‘the safety net’) of the state. Also note the 2006 Recommendation⁴⁰ and Directive 2007/65/EC at Recital 36:⁴¹

self-regulation constitutes a type of voluntary initiative, which enables the economic operators, social partners, non-governmental organizations or associations to adopt common guidelines amongst themselves and for themselves ... Co-regulation gives, in its minimal form, a legal link between self-regulation and the national legislator in accordance with the legal traditions of the Member States. Co-regulation should allow for the possibility for State intervention in the event of its objectives not being met.

Four elements reinforce the role of EU institutions in addressing issues arising from the practice and assessment of self- and co-regulation:

- the European Union has particular competence in specific policy areas where alternatives to regulation can be of particular importance, deriving directly from the legal (treaty) base;⁴²
- the European Union has established already a lead role in articulating the ‘Better Regulation Agenda’, laying out an implementation framework through the Inter-institutional Agreement on Better Regulation;⁴³
- many of the issues raised, in terms of regulatory competence and objectives, and of evidence collection, are inherently cross-border or even trans-European; and
- in recognition of subsidiarity, the most common EU instrument of regulatory policy is the Directive, rather than the European Regulation. The use of this instrument in areas where self- and co-regulatory alternatives are likely to be relevant requires concrete and consistent guidance to implementing Member States, to avoid regulatory and market barriers and fragmentation. Formal mechanisms for harmonizing and reconciling

formal regulation in different Member States prove to be less effective in relation to self-regulatory institutions.

Net neutrality regulatory solutions can be classified by the ‘degree of self-regulation’ involved, from basic informal communication through to formal regulation. Table 8.1 describes the extent of government involvement by analogy with the Beaufort Scale of wind strengths, in a continuum from complete calm (no involvement) to the strongest intervention (hurricane).

Specifically, levels 9–11 represent co-regulation (i.e. government legislative force behind the regulatory forum), while 0–8 represent the evolution of self-regulation from its first beginnings towards the onset of co-regulation. This broad classification by policy involvement is not perfectly aligned with direct or indirect government funding. Such support includes aid to self-regulation by soft law and other policy interventions, including financial assistance. For instance, governments or the European Union may choose to support self-regulatory standard setting as a genuinely non-regulatory policy, as in scales 2 and 6 above, which may include financial support. Examples in the table are drawn from a recent EC study, and more explanation is offered there.⁴⁴

A Bill of Internet User Rights?

If co- and self-regulation are unsuitable mechanisms for fundamental rights to be arbitrated over, am I – and is the EC – ‘doing a Lessig’? Are we suggesting watered-down, market-oriented forms of regulation where the State should be stepping in with all its majesty to prevent abuses of its citizens’ rights? My colleague Steve Peers recently published a report for the European Parliament explaining how cybercrime detection threatened to strike too hard at individual liberties without appeal.⁴⁵ He suggests we need a non-binding Internet Bill of Rights:

The drafting and promotion of an ‘Internet Bill of Rights’ could summarize these rights and draw them to the attention of Internet users, industry actors, the public sector (regulators, police officers, teachers, et al), relevant NGOs and the media. The Bill of Rights could be drawn up initially by the European Parliament, but could be open for signature and/or support by industry actors, NGOs, Member States, other EU institutions, media bodies and others. It could be endorsed and promoted on the websites of companies, NGOs, EU institutions and

Table 8.1 A 'Beaufort Scale' of Self-Regulation

Scale	Regulatory scheme	Self-Co	Government involvement
0*	'Pure' unenforced self-regulation	Creative Commons SecondLife	Informal interchange only – evolving partial industry forum building on players' own terms
1	Acknowledged self-regulation	ATVOD	Discussion but no formal recognition/ approval
2	Post-facto standardized self-regulation	W3C#	Later approval of standards
3	Standardized self-regulation	Internet Engineering Task Force (IETF)	Formal approval of standards
4	Discussed self-regulation	IMCB	Prior principled informal discussion – but no sanction/approval/process audit
5	Recognized self-regulation	ISPA	Recognition of body – informal policy role
6	Co-founded self-regulation	FOSI#	Prior negotiation of body; no outcome role
7	Sanctioned self-regulation	PEGI# Euro mobile	Recognition of body – formal policy role (contact committee/process)
8	Approved self-regulation	Hotline#	Prior principled less formal discussion with government – with recognition/ approval
9	Approved compulsory co-regulatory	KJM# ICANN	Prior principled discussion with government – with sanction/approval/ process audit
10	Scrutinized co-regulatory	NICAM#	As 9, with annual budget/process approval
11	Independent body (with stakeholder forum)	ICSTIS#	Government imposed and co-regulated with taxation/compulsory levy

Denotes the presence of government/EU funding.

* Option 0 is infrequently found – a pure self-regulatory body with no prior or later approval is close to invisible in practice; it is certainly the case that only the very 'early stage' hybrid of self-regulation can be viewed in this space.

national public sector bodies. The suggestion is not for a list of new rights or a legally binding instrument, but for a 'showcase' of relevant rights to inform the public about the application of human rights principles to the Internet.

This suggests rightly that the vast majority of politicians, and even more so telecoms analysts, company executives and others, too often overlook the fundamental nature of the Internet: it is people's primary means of freedom of expression. Peers models his Bill of Rights on the European Union's Charter of Fundamental Rights, but including a final Article 14 on how to interpret the Bill. I reproduce Article 14 in full given its importance for my conclusion. Article 14 is of particular importance as it establishes the application of the general rights outlined above.

Article 14: General provisions

1. The content of these rights, including their field of application, their scope and interpretation (including any derogations and limitations on the rights), the level of protection guaranteed by these rights and the prohibition on abuse of these rights, shall be governed by the rules on the protection of human rights guaranteed by the constitutions of the Member States, international human rights treaties, including the European Convention on Human Rights, the general principles of Community law and the EU Charter of Fundamental Rights, or by other relevant rules of national, international, Community and Union law, in their respective fields of application.
2. This Bill of Rights is without prejudice to other rights applicable to the Internet, or rights applicable in other fields, guaranteed by the constitutions of the Member States, international human rights treaties, including the European Convention on Human Rights, the general principles of Community law and the EU Charter of Fundamental Rights, or by other relevant rules of national, international, Community and Union law, in their respective fields of application.

There are a plethora of rights-based treaties and other international legal instruments, in addition to the entire legal canon in each nation on, for instance, copyright or freedom of expression. The driving force behind this

non-binding further declaration should be educative, not only of consumers, but also of governments and corporations. Whether that effect is produced depends on large part on individual and collective policy drive by national governments, for which the first requirement is transparency for users, based on evidence-driven intervention. The following final section explains the types of evidence that NRAs and governments should be collecting to ensure well-informed policy.

The Future: Evidence-Based Regulation

As we have seen, market evolution is dynamic and complex. The availability and design of a suitable regulatory response must reflect this dynamism, and also the responsiveness of regulators and market players to each other. Therefore, if any legislation is required it should be future-proof and avoid being overly prescriptive, to avoid a premature response to the emerging environment. Instead, I propose that regulators equip themselves with the skills and evidence base to rapidly investigate potential problems of unjustified discrimination. The European legal basis for regulatory intervention, especially the Access Directive, potentially provides for a wider and better variety of regulatory tools to intervene than the current US situation.

Two specific issues in this ‘watchlist’ are detection of any discrimination, and the standing of the content providers complaining of such discrimination. Should QoS be introduced, the types of harmful discrimination that can result may be undetectable. Blocking, as discussed in Chapter 2, is relatively easy to spot. ‘Throttling’ or choking bandwidth, even where unjustified, may be harder to spot and even harder to efficiently regulate. It is a moot point whether unjustified discrimination short of blocking is useful to an ISP, as discrimination against a particular content type may be overcome by sophisticated content providers via encryption in a technological ‘arms race’,⁴⁶ and in order for discrimination to create a business case, it needs to be effective in creating substantial incentives for content providers to pay a premium. Though it may not be possible technically to identify all discrimination, the most egregious types of discrimination may only provide a marketing advantage if obvious enough for customers to identify the benefits. Paradigmatically, only clear discrimination may be really worthwhile for network operators – such that the cost–benefit is at least in theory obvious to content suppliers, network operators and end-users. A solution may be to

require network operators to provide their service-level agreements on QoS to content providers and more transparently to the end-user via a regulatory or co-regulatory reporting requirement.

Regulators expecting a ‘smoking gun’ to present itself as in the Chapter 1 example of *Madison River* should be advised against such a reactive approach. A more proactive approach to monitoring and researching non-neutral behaviours will make network operators much more cognizant of their duties and obligations. Regulators can monitor both commercial transactions and traffic shaping by ISPs to detect potentially abusive discrimination. No matter what theoretical powers may exist, their usage in practice and the issue of forensic gathering of evidence may ultimately be more important. An *ex ante* requirement to demonstrate internal network QoS metrics to content provider customers and consumers may therefore be a more practical solution.

Currently, not only is it not a requirement for ISPs to notify customers when they block vital P2P-distributed applications, the security reasons given are outside the remit of typical economic telecoms regulators. Where the security reason given by ISPs for blocking traffic (which they claim carries malware and other harmful content) is typically the concern of the Ministry of the Interior (in the United Kingdom, the Home Office) and occasionally the Ministry of Trade and Industry, the regulator defers to these senior agencies and has little technically specific knowledge of data security.⁴⁷ In Ec Directorate General Information Society and Media (DG INFSO), the unit that covers information security is at least in the same DG as the enforcement and policy units.

Net neutrality is politically controversial in Canada,⁴⁸ where a celebrated breach took place in 2005, when an ISP allegedly censored communications within its own employees’ union.⁴⁹ Since then, the argument has grown in scale and scope, not least because incumbent Bell Canada’s wholesale operation was found to have throttled traffic for all its retail ISP customers. CRTC, the Canadian regulator, made a simple but entirely unsatisfactory ruling – Bell discriminated against everyone, including themselves. That meant they were not in breach of competition law, but breached net neutrality and rode over customer rights. This situation could not be maintained; therefore, on the same day that the CRTC announced Bell Canada’s decision, it also announced that it would be making an evidence-based inquiry into net neutrality.⁵⁰ The CRTC has decided to hold open hearings on network neutrality and traffic management. A CRTC hearing was held at the University of Ottawa on 6 July 2009, following

a call for comments which states: 'The Commission invites parties to comment on Internet traffic management practices of ISPs.' As well as several empirical questions regarding traffic shaping and user traffic profiles over the past three years, it asks the vital questions of law and technology.

First, the law. It asks simply 'How should congestion be defined in an ISP's network?' This is a question that the European Commission and NRAs will also have to address in order to implement the new Package before 2011. CRTC explains that in Telecom Decision 2008-108, CRTC directed Bell Canada to file proposed notification requirements with the Commission, to address future QoS changes at wholesale level. It asks whether these requirements should be extended to other wholesale ISPs such as cable ISPs. Further, it addresses the question of whether all ISPs have incentives to discriminate against traffic types and whether they should be so permitted:

Are similar requirements necessary and appropriate in relation to the provision of retail Internet services? If so, what kinds of practices, and/or changes to practices, should trigger these requirements and what information and how much notice should be provided to end-users?

It asks what types of traffic management represent the ISP controlling content rather than simply passing it over the network, and how the obligations not to discriminate can be squared off against specific practices. Further, it notes that it is required to operate in as pro-competitive and light-touch regulatory manner as possible. European and United States regulators should watch these proceedings carefully for best practice and the attempt to make evidence-based rulemaking.

The technology questions are more future-oriented. They include:

- What developments are under way with respect to traffic protocol (such as modifications to transmission control protocols) and/or application changes (such as changes to P2P file exchange) which could assist in addressing network congestion?
- What are the specific capabilities offered by the technical solutions? For example, would these technologies allow for throttling of individual users or groups of users; would they allow for the collection of information about persons and to what extent?
- How effective would these solutions be in addressing network congestion in the ISP networks?

- What impact could the implementation of technical solutions have on the standards upon which the operation of the Internet is based? Could these solutions create interoperability challenges for application developers?
- What, if any, Internet traffic management practices employed by ISPs would result in unjust discrimination, undue or unreasonable preference or advantage?
- What, if any, Internet traffic management practices employed by ISPs would result in controlling the content, or influencing the meaning or purpose of telecommunications?
- For any Internet traffic management practice identified as controlling content, what criteria should the Commission apply in determining whether to authorize such practice?

It states ‘The issue of Internet traffic management practices is increasingly a global issue that is being raised in other jurisdictions’ and asks for information on ‘initiatives being examined or undertaken in other jurisdictions’.

As an early submission to the CRTC inquiry due for July, Canadian ISPs responded on the extent of their DPI deployment.⁵¹ Not surprisingly given the various billing, cybercrime and anti-terrorist legislation requirements already imposed on ISPs in developed countries, the big incumbents have made the investment decision to deploy DPI. How much that reflects a business case based on charging priority traffic or deflecting Skype and other VoIP services, as discussed in Chapter 1, we will discover.

An interesting dialogue opportunity has recently arisen with the Internet Society (ISOC) announcement of the formation of the Internet Technical Advisory Committee.⁵² This is an advisory group to an advisory group (OECD) to governments, so one should note that it is far removed from legislation, but its membership is extremely eminent in Internet standard setting and its recommendations therefore likely to be taken seriously as technocratic standards of excellence. It states: ‘Through its commitment to the Internet’s ethos of community, collaboration, and industry self-regulation, ITAC will provide counsel and the expertise of technically focused organizations to aid the OECD in its work on the Internet economy.’ It is a Technical Stakeholder Forum, which:

stressed the role of the open, collaborative, inclusive ‘Internet Model’ of development, and called upon the ministers to preserve and promote

the conditions that enable innovation and positive development on the Internet.

To summarize, for timely and evidence-based intervention, regulators will need to ensure that the network operators report more fully and publicly the levels of QoS that they provide between themselves, as well as to end-users. Internet architecture experts have explained that discrimination is most likely to occur at this level as it is close to undetectable by those not in the two networks concerned in the handover of content. It is very difficult (if not impossible) to monitor the former for any one other than the two network operators themselves, and therefore shedding light on QoS in this area will require a reporting requirement to be imposed. As this information is routinely collected by the network operators for internal purposes, this should not impose a substantial burden.

Regulator Training and Technological Research

The pace of change in the relation between architecture and content on the Internet requires continuous improvement in the regulator's research and technological training. This is in part a reflection of the complexity of the issue set, including security and Internet-peering issues, as well as more traditional telecoms and content issues. Dominant and entrenched market actors in regulated 'bottlenecks' play games with regulators in order to increase the sunk costs of market entry for other actors, and pass through costs to consumers and innovators.

Net neutrality has a rich influence – it distorts content competition, encourages certain applications while discourages others, etc. I have categorized net neutrality into positive (QoS) and negative (content discrimination) net neutrality, indicating the former as potentially beneficial while the latter as harmful. However, this categorization can be problematic, as the three major players involved in the net neutrality context – content suppliers, network operators and end-users – have different, often conflicting, interests and economic incentives.⁵³ Those incentives can either align or be at odds with the regulators' objective.

Very high entry barrier co-regulation and self-regulation can be as effective in curbing market entry as direct content regulation, especially where ISPs are incentivized to tier and charge for QoS, which raises doubts as to their desire to implement self-regulation. By and large, the greater the levels of

regulation, the more the market develops towards closed and concentrated structures, for three reasons:

1. larger companies are able to bear compliance costs much more easily than SMEs, and therefore it is important that such entry barriers – where necessary – are minimized;
2. larger companies have the resources and lobbying power to seek to influence regulation in a positive direction;
3. large ISPs in a concentrated market may offload costs upstream onto content providers and developers, or downstream onto consumers.

Therefore any solution needs to take note of the potential for larger companies to ‘game’ a co-regulatory scheme and create additional compliance costs for smaller companies (whether content or network operators), and the combination of sectors makes this a particularly complex regulatory ‘game’.

The need for greater research towards understanding the nature of congestion problems on the Internet and their effect on content and innovation is clear.⁵⁴ Research that can inform net neutrality can be listed, from the particular to the general:

1. Internet-peering and distribution costs: Intensive and focused research is needed into the costs of local IPTV, VOD and multicast distribution. Further research on an ongoing basis is needed into user generated content creation and self-regulation.
2. Price discrimination and content regulation: The interplay between content regulation and pricing is an essential area for future research. Net neutrality policy needs to ascertain the investment options that can drive content and network investment in Web 2.0 and NGN futures.
3. QoS and NGNs: Data, voice, video and other applications have different ‘legacy’ QoS standards – at least implicitly in their technologies and consumer preference. The economics of these technical interactions require further clarification.
4. Venture capital flow analysis: Exploring the fluctuations in financing more accurately would help in real option analysis of the choices made by investors depending on policy choices made by regulators and telcos.
5. Switching costs, regulation and innovation: The impact of regulation on churn and the ‘turbulent’ impact of subscriber churn on market growth need to be considered. Regulation may, for instance, encourage price/feature competition or reduce firm survival.

6. Drivers for broadband penetration: Differences in broadband penetration and capacity utilization are explained by speed of deployment and pricing differences. Further research is necessary in this area, benefiting from discrete choice modelling using stated preference data.
7. Stated preference analysis: User demand for access and services is not wholly driven by current offerings, but reflects as well a 'real option' decision based on potential future goods, services and types of interaction (especially with regard to user generated content). This has powerful implications both for uptake and utilization.⁵⁵
8. Quantitative assessment of harmonization and enforcement: Research is needed to model in quantitative rather than qualitative terms, and to shed light on the possible future shape and consequences of regulatory competition both within the European Union and between the European Union and other global regimes.
9. Game theory and regulatory impact assessment: Supposed 'unanticipated consequences' of network neutrality regulation can be estimated, and regulators can become more aware of these consequences by using regulatory games to simulate real market behaviour.
10. Fundamental rights and freedom of expression: The role of ISPs in Notice and Take Down, as we saw in Chapter 4, remains a 'black box' for regulators and users. There is a pressing need to assess current levels of filtering and censorship in order to shape regulation and align it with consumer and producer interests, though acknowledging that the former must prevail, as the regulator's statutory primary duty.

This book has been a partial attempt to remedy some of the issues, but in expressing the need to employ more technologists, financial analysts and game theorists, I am aware that these are gaps that traditional economics and legal analysis of communications can only point to. When writing with economists or technologists, I am reminded of the old African story about the elephant that crosses a rickety bridge over a riverbed with a mouse perched on his head. The mouse scampers down to the elephant's ear as he turns to survey the precariously swinging bridge after the successful crossing, and shouts: 'Woo, boy, we sure swung that bridge!' Law can only analyse with the benefit of the tools of these other specialisms, standing on the shoulder of giants – and indeed elephants.

Regulating For Net Neutrality ‘Lite’

To summarize the argument, there are incentives for network providers to police the traffic by type, if not by content. It enables the network providers, many of whom also operate their own proprietary applications, to charge a different price to non-affiliated content owners than affiliated owners. This differential pricing could make the profitable operation of non-affiliated providers more difficult. On that basis, a ‘walled garden’ of ISP services and those of its ‘preferred content partners’ might become the more successful business model. That model makes regulation much easier to enforce, but also prevents some of the interoperability and open access for users that is held to lead to much ‘Web 2.0’ innovation for businesses. It is not the aim of this book to provide the ‘right’ answer in the complex trade-off between, on the one hand, regulated ‘walled garden’ networks and affiliated content providers, and on the other, open interoperable and self-regulated Internet access, as the answer must be contingent on political, market and technical developments.

In Chapter 2, I raised the issue of business cases for broadband filtering technologies to illustrate the main conclusion: it is not the speed of broadband which is a challenge, but the cost and quality of the applications and content provided over that broadband network. The issue of uncontrolled Internet flows versus engineered QoS solutions is central to the question of a ‘free’ versus regulated Internet.

I have been suggesting a consumer- and citizen-orientated intervention. Economic orthodoxy holds that consumers are in general better off, if they can get access to a product at a lower price, and have more product variety and better quality products. Lower price is a rather short-term welfare goal that can be achieved by more intensive competition, while variety and quality are long-term welfare enhancements dependent in this case on a step-change in technology. From a general economic perspective, long-term should weight more in regulation, also because it entails short-term enhancement in the future. This in itself suggests that ISPs be allowed to raise prices short-term to pay for improvements that led to greater innovation later. There are three absolutely critical conditions to this:

1. All benefits are passed through to consumers from the short-term price rises, via investment in new networks.
2. Greater bandwidth offers a greater innovation benefit than the lost openness of the network in the meantime.

3. The third, rather obviously, is that having moved away from net neutrality, the regulator can later wave a magic wand and rediscover the 'paradise lost' (if that's what it is).

That depends on passing regulations to undo the controls exerted over traffic via DPI equipment and the like – and that in the face of the entire burgeoning DPI 'espionage-industrial complex' that will have grown up around the issue.⁵⁶ End-user generated innovation often occurs as a result of intrinsic motivations (like democracy or game play) and non-monetary motivations (e.g. cooperative or own use benefit) of content developers. In the presence of economies of scale in NGNs for incumbents, 'positive' net neutrality (or price) discrimination is an economic argument for investment incentives. So reducing the 'fun' innovations in favour of the scale economies is the trade-off proposed. That's Disney, not Google.

These conclusions support a light-touch regulatory regime involving reporting requirements and co-regulation with, as far as is possible, market-based solutions. Regulatory monitoring of potential abuses, including strengthening investigatory capacity and transparency for end-users, is a solution that maintains maximum flexibility and policy choice, while ensuring that any abuses can be quickly detected and dealt with appropriately. Solutions may be international as well as local, and international coordination of best practice and knowledge through fora such as the OECD will enable national regulators to keep up with the technology 'arms race'.

In the 2009 discussions in the new E-Communications Framework, large well-resourced European incumbents saw the opportunity to make common cause with mobile operators, public service broadcasters and commercial television companies in an unholy alliance to prevent the open Internet video model emerging. The regulation of the Internet that is rapidly taking place is being driven – unquestionably – in Europe by politicians for public safety reasons. They are erecting entry barriers with the connivance of the incumbent players, with potentially enormous consequences for free speech, free competition and individual expression. This may be the correct policy option for a safer Internet policy, though it signals an abrupt change from the 'Generative Internet'. Claims by the European Commissioner that regulating the Internet is not the intention do not flatter the intelligence of the audience. That may be the intention of the paternalistic and oligopolistic interests represented in the new regulated Internet. It is therefore vital that regulators

address the question of the proper ‘lite’ approach to net neutrality to prevent harm to the current Internet, as well as beginning to address the heavier questions of positive – or tiered – breaches of network neutrality.

A simple truth lies behind the quotation from President (then-Senator) Obama which opened the first chapter. We should not entrench ‘Lex Monopolium’ at the expense of an open Internet, nor is the choice that drastic: innovation and investment can be encouraged by relatively light-touch co-regulatory transparency principles, backed up by a regulator with sufficient comprehension and research into the issues and sharp teeth to make a real political commitment to intervene where economic or social interests dictate. Network neutrality may be a slogan that covers many concerns about the future of the Internet, but it certainly provides an excellent platform to create this wider and better informed discussion. That was my aim in this provocation.