Regulating Code: Towards Prosumer Law?
Ian Brown¹ and Chris Marsden²

Abstract
In this interdisciplinary paper written by a socio-legal scholar and a computer scientist, we explain a novel holistic approach to Internet regulation in the broader public interest. We argue for ‘prosumer law’ and give an example of our proposed solution to the problems of dominant social networking sites. What should prosumer law consist of? We examine the international governance of information, especially the apparent incompatibility of human rights and trade-related concerns exposed in such multi-stakeholder fora as the OECD. Finally, we argue for holistic regulation of the Internet, taking a trans-disciplinary perspective to solve those ‘hard cases’ we have examined. Prosumer law suggests a more directed intervention, to prevent Facebook or Google+ or any other network from erecting a fence around its piece of the information commons: to ensure interoperability with open standards. It is not sufficient for it to permit data deletion as that only covers the user’s tracks. It requires some combination of interconnection and interoperability, more than transparency and the theoretical possibility to switch. It needs the ability for exiting prosumers to interoperate to permit exit.

We argue that it is untrue to state that there is so much convergence between platforms that there is no clear distinction between open commons and closed proprietary environments, though ‘voluntary forfeiture’ of IPR to permit greater innovation has always been commonplace. We base our argument on the empirical case studies presented in ‘Regulating Code’ (MIT Press, 2013), but we extend our argument from that monograph to assess the environmental preconditions for prosumer law to operate in Europe. We describe the multi-stakeholder environment for Internet governance and regulation, in which user groups lobbied along with business and governments. We also describe the insights of new institutionalism, with exit and competition for standards becoming increasingly critical in the information economy. We then describe interoperability as a means of lowering entry barriers and increasing consumer welfare. We consider United States administrative and academic arguments (Wu 2010, Zittrain 2008, Lessig 1999,2006) for self-regulation to have demonstrably failed, and focus on the European regulatory space as more fertile ground to explore prosumerism as both a market-based and citizen-oriented regulatory tool.

¹ Senior Research Fellow at the Oxford Internet Institute, Oxford University. His research focuses on public policy issues around information and the Internet, particularly privacy, copyright and e-democracy. He also works in the more technical fields of information security, networking and healthcare informatics. He has consulted for the US Department of Homeland Security, JP Morgan, Credit Suisse, Allianz, McAfee, BT, the BBC, the European Commission, the Cabinet Office, Ofcom, the National Audit Office and the Information Commissioner’s Office. Previous projects include Pilot Interactive Mobile Multimedia System (PIMMS), Control and Prediction of the Organic Solid State (CPOSS), CLEF (Integrating Information for the clinical e-Scientist), Fair Tracing, e-Curator and the Cambridge-MIT Institute’s Critical Infrastructure Protection working group.

² Professor of Law, Law School, University of Sussex. He is author of the full length monographs Regulating Code (MIT, 2013, forthcoming), Internet Co-regulation (Cambridge UP, 2011), Net Neutrality: Towards a Co-regulatory Solution (Bloomsbury, 2010), several other co-authored books, and many peer-reviewed articles. He has advised the European Commission, national governments and regulators, OSCE and Council of Europe. Formerly Professor of Law at the University of Essex, Research Fellow at Harvard’s Kennedy School (1999), Industrial Policy Fellow at Cambridge Computer Lab (2006-8), visiting fellow at law schools in US, Japan, and Australia.

Table of Contents

Regulating Code: Towards Prosumer Law? ................................................................. 1

Abstract ......................................................................................................................... 1

Conflicting Approaches to Internet Regulation ......................................................... 3

Empirical ‘Hard’ Case Studies Exploring Prosumer Law ............................................. 4

Regulating Through Code .......................................................................................... 6

Tussles in Code and Law ............................................................................................... 9

Competition Law and the Internet ............................................................................. 11

Interoperable Code and Communications Policy ...................................................... 12

Interoperability: A Code-Based Solution ................................................................... 14

Search Markets: Google .............................................................................................. 22

Social Networks: A Prosumer Problem ...................................................................... 23

Prosumer Solution to Social Networking .................................................................. 24

Conclusion: Towards Prosumer Law? ........................................................................ 27

References .................................................................................................................... 29
We are all becoming ‘prosumers,’ sharing intimate details of our personal lives online. But this ‘prosumer environment’ is currently either grossly unregulated, leaving personal information at the mercy of the multinationals who host it, sell adverts based on it, and sometimes claim to own it, or subject to knee-jerk over-regulation. This paper examines how a prosumer law interoperability framework can be applied to Internet law and policy. First, we assess the standard analyses of Internet regulation. We explain how regulation of this virtual environment is best approached by examining the protocol stack rather than geographical approaches and assessing regulatory intervention according to the code solution or solutions used. However, following Shannon (1948, 1949), we reject a technologically determinist view of code as an efficient stand-alone solution and examine the predominant justifications for various regulatory systems, classified as broadly supported by economic or rights-based regulation (Lessig 1999; Balleisen and Moss 2010). We analyse the regulatory shaping of “code”—the technological environment of the Internet comprising hardware, software and their interactions, notably in the protocols and standards used to achieve interoperability — to achieve more economically efficient and socially just regulation. In the following section, we explore a particularly promising recent approach, multistakeholder governance (Drake and Wilson 2008; DeNardis 2009). We go on to explore code-based solutions that involve both competition analysis and interoperability requirements in strategic communications sectors, before examining the case studies of search engines and social networking sites. We conclude that prosumer law is urgently needed to enable European citizens to make most effective use of the opportunities offered by broadband technologies, Web2.0 and the overall Digital Agenda.

Conflicting Approaches to Internet Regulation
There are three existing conflicting approaches to Internet regulation from a technical and legal policy perspective: continued technological and market-led self-regulation, re-introduction of state-led regulation, and multi-stakeholder co-regulation.

The first, self-regulation, holds that from technical and economic perspectives, self-regulation and minimal state involvement are most efficient in dynamic innovative industries such as the Internet. This explanation is challenged by three factors: technological, competition, and democratic. Technology is never neutral in its social impact (Reed 2007; Dommering 2006). Network and scale effects are driving massive concentration in information industries (Zittrain 2008; Wu 2010). And voters will not allow governments to ignore the social impact of this ubiquitous medium.

The second explanation holds that from the legal policy perspective, governments need to reassert their sovereignty. It states that code and other types of self-regulation critically lack constitutional checks and balances for private citizens, including appeal against corporate action to prevent access or remove materials (Frydman and Rorive 2002; Goldsmith and Wu 2006). According to this explanation, government should at least reserve statutory powers to oversee self-regulation to ensure the effective application of due process and attention to fundamental rights in the measures taken by private actors. However, government regulation has serious legitimacy deficits, with as much government as market failure in Internet regulation to date, with over-regulation evident in public and private censorship (MacKinnon
There has been widespread industry capture of regulators and legislators in, for instance, copyright law (Horten 2011). Incumbents lobby to protect and introduce new barriers to entry with regulatory or legislative approval, as in a perceived failure to enforce or approve network neutrality legislation (Marsden 2010). There has been continued exclusion of wider civil society from the formal policy discussion, where official views do not permit easy representation of new non-corporate technical or user rights lobbies (Mueller 2010).

The civil society argument leads to the third multistakeholder co-regulatory explanation: that formally inclusive multistakeholder co-regulation—reintroducing both state and citizen—is the approach that has the best chance to reconcile market failures and constitutional legitimacy failures in self-regulation (Collins 2010; Marsden 2011). Though intended to increase inclusiveness by representation beyond the government-business dialogue, there are significant questions as to the effectiveness, accountability, and legitimacy of civil society groups in representing the public interest. There is a body of work on Internet governance specifically addressing legitimacy gaps and development challenges in global institutions from an international political economy perspective (Mueller 2010; Drake and Wilson 2008).

Given the legitimacy gap in multistakeholder interaction, it is unsurprising that the approach so far has been to conduct conversations rather than make law in such fora, reflecting the “unconference” approach of Internet innovators (in which agendas are collaboratively determined by participants at the beginning of a meeting). Cynicism is at least partly justified (Morozov 2011).

Co-regulation has been extensively discussed in European law (Senden 2005; Hüpkes 2009), including in Internet regulatory debates (Lievens, Dumortier, and Ryan. 2006; Frydman, Hennebel, and Lewkowicz 2008) and in relation to data protection governance (Raab 1993). Co-regulation is even more familiar to Australian regulatory scholars since the term entered common use in about 1989 (Marsden 2011), with the term applied to codes of conduct for industry sectors (Palmera 1989; McKay 1994; Grabowsky 1995; Sinclair 1997) including the Internet (Chen 2002). Adoption of the term in the United States has been slow, with co-regulatory in legal terms referring to state-federal division of competencies (Noam 1983). However, both Balleisen (Balleisen and Eisner 2009; Balleisen 2010) and Weiser (2009, 2010) have made extensive claims for co-regulation to be adopted more frequently.

**Empirical ‘Hard’ Case Studies Exploring Prosumer Law**

Our approach takes a multidisciplinary perspective from both computer science and law, following Kahin and Abbate (1995), Berman and Weitzner (1995), and Lessig and Resnick (1998). We cover European as well as U.S. regulation and policy, and explain why a geographically specific attempt to regulate will largely fail to achieve optimal code and regulatory solutions. Previous legal work has tended to examine the Internet from a position reflecting the technology’s unregulated origins (Post 2009), even in debunking the borderless “Wild West” mythology of early libertarian paradigm (Lessig 2006; Goldsmith and Wu 2006; Zittrain 2008). They equally have tended to be U.S.-centric. This debate has been effectively ended in favour of realistic pragmatic viewpoints (Reidenberg 1993, 2005; Goldsmith & Wu 2006; Wu 2010). Regulatory and political economy work has concentrated on single issues or themes, such as the domain name system or privacy issues. There has been significant
analysis in individual issue areas, notably the Internet Corporation for Assigned Names and Numbers, or ICANN (Mueller 2002) and Internet standard setting (Camp and Vincent 2004). Holistic examinations have tended to be compendia, such as Marsden (2000), Thierer and Crews (2003), and Brown (2013), or examine the Internet from development or other political economy perspectives (Cowhey, Aronson, and Abelson, 2009). We examined empirically grounded, multidisciplinary case studies of five difficult areas—what we refer to as hard cases (Brown and Marsden 2013).

For the whole of this century, governments have been able to require crude filtering of access to content based on geography. The imposition of sanctions on U.S. Internet host Yahoo! by the French courts in 2001 could not block all French users from accessing content that was illegal in France but legal in the United States. It was intended to restrict the vast majority of ordinary non-expert users who did not have the ability or incentive to disguise their location (Reidenberg 2004, 2005; Goldsmith and Wu 2006). Expert witnesses told the French court that users could be blocked with about 70 per cent effectiveness, although one witness later retracted this opinion (Laurie 2000). The idea that one can map Internet regulation based on the location of bits is therefore superficially attractive but essentially a technologically determined attempt to reintroduce physical jurisdictional boundaries (Bender 1998). Ultimately the Internet’s highly connected nature has enabled at least sophisticated users to route around censorship, protected by encryption, which we explore in more depth in the next chapter.

If Internet transactions cannot be regulated in the same way as physical goods transactions, a second suggestion is that they be mapped using their nearest physical analog: the geography of their routing through servers. The problem here is significant and can be stated simply: the Internet remains largely a “dumb” network that routes packets without examining their contents. This lies behind the so-called end-to-end nature of the Internet: “intelligence” lies in end nodes such as PCs and smart phones, not between these nodes in network routers (Saltzer, Clark, and Reed 1984; Clark and Blumenthal 2011). Though attempts are being made to “see” inside the packets to check their compliance with the law, governments still cannot very effectively act as customs officials and stop, check, deport, or import packets (Burk 1999; Marsden 2010). Though this is a technological possibility in Internet design, it would create a significantly different environment where, for instance, the anonymity of senders was removed or at least penalized (Deibert et al. 2008, 2010; Johnson et al. 2004).

There are regulatory opportunities to shape the market in favour of interoperability if regulators choose such options. The open Internet policy coordination challenge is acknowledged by the G8 nations (2011: 14): “As we adopt more innovative Internet-based services, we face challenges in promoting interoperability and convergence among our public policies on issues such as the protection of personal data, net neutrality, transborder data flow, ICT security, and intellectual property”. These policy conclusions can be applied by the countries and regions that are both most engaged in and most able to influence the future of the fundamental policy objectives of Internet policy. Network openness is under reconsideration as never before, with increasing partitioning of the Internet, partly driven by security concerns, which is leading many ISPs to add capabilities to their routers to filter,
inspect, and prioritize network traffic to a much greater degree than previously possible. This policy field displays both a plurality of market actors (content and carriage disguises the various interests within and between those sectors, such as mobile networks and vertically integrated actors) and a profusion of formal (state and supranational) and informal (standard-setting) regulators. It exhibits advanced examples of regulatory capture, especially in the more static and matured regulatory environment of telecoms.

Early analysts viewed technical and geographical challenges to existing regulatory functions (Johnson and Post 1996) as insurmountable obstacles to regulation. Later analysis demonstrated that there was much greater interdependence between the allegedly global and un-regulable Internet and national rules (Thierer and Crews. 2003; Marsden 2000). The ability of the state to seize physical assets and interrogate evidence (such as data on servers) is at the centre of national enforcement (Brown, Edwards, and Marsden 2009), as well as traditional state censorship. Our selection of hard cases is an attempt to investigate the gaps where full state regulation is unfeasible, unwieldy, or unnecessary. A strong working assumption of our research is that many such institutions will map not to geographical boundaries but to sectoral or technical realms (Bar et al. 2000; Barnes 2000).

National law does not create effective solutions to prevent code-based problems, but a better solution may be a combination of a pooling of sovereignty to create global standards in support of effective code and protect users’ rights. There has been a growing realization that the Internet presents a complex series of challenges to existing laws, but that a nuanced and interdependent (if complex) relationship has emerged between existing nationally based legal systems and a global (or at least multipolar) Internet architecture based on code. The role of state sovereignty has been reintroduced by both the Internet’s mass adoption and by government desires to reintroduce substantial monitoring and other functions to maintain state security. These were particularly driven by the September 11, 2001, terrorist attacks in the United States and subsequent attacks in Bali, Madrid, London, and elsewhere (Ball and Webster 2003), and the growing scourge of virus writers, spammers, fraudsters, child pornographers, and paedophiles using the Internet (Brown, Edwards, and Marsden 2006).

The Internet is not a novelty in regulatory discussion (and was not at the time of much initial surveying in this field; Kahin and Nesson 1997). But its’ relatively fast and technologically dynamic development means that there is likely to remain a governance gap between what the technologists and advanced users know of the medium and political responses, as with many other advanced technologies (Brownsword 2005). Internet regulatory history is partial or incomplete, as the issue areas were either neglected by regulators for Internet-specific reasons as technically forbidding (as with many Internet security problems) or because of forbearance based on the desire to avoid harming self-regulatory mechanisms (Price and Verhulst 2004; Priest 1997) and to ensure the continued competitiveness advantages of rapid Internet deployment and development. Regulation has lagged Internet development.

Regulating Through Code
A more technical view can provide a different perspective. Engineers designed the Internet, and its content, services, and applications sit on the infrastructure. Therefore the logic of the
infrastructure’s design can provide a basis to assess what is different about the Internet for regulatory purposes: its code (Reidenberg 1998; Lessig 1999; Werbach 1997). This suggests that we explore the Internet from the perspective of those who designed its standards, whether the basic standards of the Internet Protocol (IP) itself and its end-to-end design (Clark and Blumenthal 2011), the motives and (limited) policy purposes behind the refinement of that design, or the particular applications that interact directly with the content layer (Berners-Lee and Fischetti 2000). Internet self-regulation emerges from that technical perspective.

Problems of both a regulatory and disciplinary nature remain. The lack of interaction between (most) engineers and (most) social scientists mean that the technology is often as unsuitable for wider societal goals as the law is unsuitable for many practical enforcement processes (Sola Pool 1983). A technical view of mapping begins with the classic open systems interconnect (OSI) “layers model,” which was adapted to represent the stack of Internet protocols that enable end-to-end signalling of communications traffic (Werbach 2002). There are cross-cutting issues that affect the stack as a whole, examples such as digital rights management (DRM) and security. Content and applications and their regulation sit atop the Internet’s deeper architecture, which is typically represented by the “protocol stack.” The technical infrastructure provides the underpinning of the content layer, and design choices in those layers underpinning content have a significant influence on the content itself (Reidenberg 2005; Lessig 1999). We selected case studies that have a significant material impact on the content layer, including those that may be located further from the end user’s visibility. For example, the relatively anonymous end-to-end nature of the Internet facilitates the transmission of unsolicited commercial e-mail (spam). Laws restricting this content cannot be effective for most consumers without also enlisting the support and deployment of services deployed outside the user’s own computer (Clark 2005; Brown, Edwards, and Marsden 2006) through some level of classification and filtering at other points in the network.

The hard case studies that we analyze demonstrate the links between core protocols and content regulation in the areas of data protection, network neutrality, censorship, copyright, and social networks. For instance, DRM and security affect content consumption but can also be embedded within architectures and hardware. This type of joined-up thinking between content-based laws and architectural principles runs through our logical analysis of the case studies. It explains in large measure governments’ acknowledgment of the futility of attempts to regulate using law alone. For a road traffic comparison, one cannot enforce fundamental changes in road users’ behaviour without the support of automobile manufacturers, transport planners, as well as suppliers, pedestrians, bicyclists, and environmental groups. Instrumental regulation-led description of the Internet must acknowledge the underlying architecture in the same way as road traffic rules and conventions must acknowledge the environment in which they operate (safety rules do not permit bicycling at night without lights, for instance).

Though one does not have to understand every element in design to implement a rule, or every protocol in the layers model, it is essential to understand the system fundamentals. The end-to-end IP-enabled Internet is by definition an interoperable and technically neutral
regime on which many open standards result in open source products or services for use without charge, protected by copyright licences (such as the General Public License, GPL) that require any derivative software to be freely available and modifiable (EC 2011a). In such a regime, anyone can design based on publicly and freely available protocols and software and interoperate with anyone else properly deploying the same protocols with the same rules. This open interoperability gives enormous practical advantages, which resulted in the development of the public Internet as it is widely experienced today. “Closed-open proprietary versus free information models” depend on code choices (Zittrain 2008; Wu 2010). The concern here is not with the openness of FSF-GPL, Apache, or Linux license models directly (Guadamuz 2009), though we note their importance as contributors to the Benkler (1998) argument that peer-produced production can help create an information commons. Our concern is with wider mass participation models and their regulation, with Lessig (2008) and Boyle (2008) commons arguments for reform to redress the extremism of intellectual property law. The difference is that we acknowledge the role that government can play as a broker for policy solutions while recognizing that government can often be captured by regulated industries. However, antitrust and open data policies can help user empowerment (Mehra 2011), and we are more confident than Wu is that the tendency toward government captured by regulated monopoly may not be the whole story.

We selected five case studies in the book from which this article derives its framework, which addressed the topics of: data protection; copyrights; censors; social networking; and smart pipes (Brown and Marsden 2013: Chapters 3-7). The first three are case studies in fundamental rights with economic implications. The final two are studies of the most innovative platforms to develop new markets and protect those fundamental rights. They are also in a period of regulatory flux, yet with significant regulatory development in the past five years such that it is possible to draw some conclusions. We deliberately omitted search, whose development was critically dependent on further antitrust activity in Brussels and Washington. Hence the final substantive part of this article considers recent developments in the regulation of search (Zittrain 2008; Deibert et al. 2010).

The mass take-up of social networking tools has heightened concerns over privacy, copyright, and child protection and created a generic centre for regulatory activity that raises new questions about the scope and focus of Internet regulation. With nearly one billion Facebook users, regulators’ concerns over ordinary citizens’ use of the Internet have led to specific regulatory instruments that address the risks of such use (Facebook 2012; Office of the Data Protection Commissioner Ireland 2011). The case study which concludes this article builds on the literature and regulatory proceedings to assess the extent to which the more conventional issues-based regulatory instruments are being supplemented by generic social networking regulation.

We address these key questions in each of the substantive case studies:

• Who were the key stakeholders (traditional and multistakeholder), and how far were they involved in policy debates, organizational design, and operational issues associated with the
regulatory processes or institutions adopted? What was the institutional political economy (Mueller 2010)?

• How far did solutions have source, process, or outcome legitimacy (Weber and Grosz 2009), including human rights compliance, in the outcome? What influence did fundamental rights have in policy design? This exploration is based on both documents relating to design and later judgments of human rights bodies (e.g., national parliamentary scrutiny committees, Council of Europe).

• How effective is the current and developing code solution? How might it have developed differently under different regulatory conditions?

In each case study, we examine whether governments have moved from sledgehammer prohibition-based, enforcement-oriented regulation, to smarter regulation that works technically, with some degree of outcome legitimacy in terms of goals. These might, for instance, support the creation of public goods and disruptive innovation in markets. A smart solution in terms of code and regulation would provide effectiveness in enforcement (whether by law or code), technical efficiency (in an engineering sense) and legitimacy, transparency, and accountability (to allay rights-based concerns). Unsurprisingly, the outcomes are likely to be trade-offs among these goals.

**Tussles in Code and Law**

Clark et al. (2005: 10) recognize that struggle or “tussle” between different interests is as important in technology evolution as in economic and political systems, suggesting that “we, as technical designers, should not try to deny the reality of the tussle, but instead recognize our power to shape it”. As Greenstein (2011) advises standards bodies, “doing the tussle” can create more robust and widely adopted industry standards. Although this is a mandate for the technical community, it can be extended to the legal regulatory communities that directly shape the various aspects of Internet development, many of which already recognize that their shaping decisions are moves in a game rather than acts of sovereign design. Design choices in code can be as normative as law—decisions have to be made on the values that code embeds (Brown, Clark, and Trossen 2011).

Code has continued to morph rapidly even as legislation has tried to adapt. Investor certainty and democratic participation in legislative processes are arguably enhanced by the leisurely speed of legislation, contrasted with the rapid—but slowing—progress of Internet standards in which only technical experts can realistically participate. Most progress has happened with technical protocol development within companies (and, arguably, open source communities), where coordination (“tussle”) problems are less complex than in legislatures. IPv6 has been slowly, even glacially, deployed, but a big switch in Facebook design to facilitate the use of Secure Socket Layer connections was possible in a few days, and Windows security updates can be automatically distributed to hundreds of millions of users overnight. Consider single-company developments as a reminder of user empowerment through code: Facebook achieved a billion user accounts in under a decade; Skype achieved 650 million user accounts in less than a decade; Google almost 2 billion users—multilingual and with functionality
largely unaffected by culture, though China and Russia have their alternatives; many millions of infected PCs have been infected and gathered into botnets —networks of computers hijacked and controlled by a single bad actor—since consumer broadband emerged (Brown, Edwards, and Marsden 2009) as a result of the actions of individuals and small groups of criminal entrepreneurs. A more dynamic social network than blogs and e-mail, a better P2P voice over Internet protocol client that could evade ISP control, and a new search algorithm and method of targeting advertising were all eagerly taken up by consumers. The development of Google, Facebook, and Skype is testimony to the ability of emergent code to respond to and keep pace with market demands.

Architecture, law, norms, and markets interplay (Lessig 1999). Regulators have only slowly woken up to regulation using technology. If regulators fail to address regulatory objects at first, then the regulatory object can grow until its technique overwhelms the regulator. Napster as a “child” could have been shaped by regulation. Once it had exerted its network effects and grown, any blunt regulatory tool simply reshaped P2P—to more powerful tools of file sharing, overwhelming regulatory defences by their architectural ingenuity, morphing to jurisdiction-hopping P2P “on steroids” (Wu 2003). Digitally locked music formats were outpaced by the overwhelming Metcalfe’s law effect of MP3 as a legitimate but untethered technology. Major rights holders were highly successful in coordinating demands for DRM from tech companies, but ultimately they were defeated when their own cartel was attacked by the dominant monster they created: iTunes. Apple used its pricing policy as a bargaining tool to push rights holders to abandon DRM (Williams and Gunn 2007). A horizon limit of Zittrain (2008) is a failure to fully incorporate the market structure limits to generativity versus stability and move beyond nudges into regulation (House of Lords 2011).

Reidenberg (2005) argues that law can use code to overcome code, as Yahoo! filters French users to prevent access to Nazi memorabilia auctions. Another example is China using Cisco routers and code to create its “Golden Shield” filter (Deibert et al. 2010). A combination of points of control (Zittrain 2008) and scale economies (Lemley and McGowan 1998) give levers for law and markets to act on architecture. Traction results from the physical presence of the Internet company on the sovereign territory of the host government. The forces of regulation can be shaped more subtly: forbearance in one dimension enables expansion in others. Where code is slow to evolve, law can assist by removing bottlenecks to innovation. Where law is designed expressly to stymie code innovation, code is likely to spill over any logjam by creating new paths to achieve user goals, as, for instance, in the P2P solution to friends sharing music files. Accusations of illegality did not serve as a veto on user adoption of P2P. Both permissive un-regulation and prohibition create pitfalls in public understanding of the effect of regulation on technologies. In simple terms, these regulatory clichés of the Internet routing around censorship as damage, or the heavy hand of the law falling on all users, do not assist public and policymaker understanding of the wider challenges of Internet regulation any more than death penalty debates assist in understanding the scope of criminology.

Regulation that succeeds or fails based on the presence or absence of specific software tools is doomed to eventual failure, while most users own open computing platforms and can
download and run the software of their choice. Despite Zittrain’s (2008) concerns over the rise of “tethered” devices, the success of the iPhone and Android software platforms (with limited oversight from Apple, and even less from Google) demonstrates that the benefits to innovation of openness will continue to give manufacturers a strong incentive to provide such a capability (Ohm and Grimmelman 2010), though we note that mandated interoperability is neither necessary in all cases nor necessarily desirable (Gasser and Palfrey 2012). Moves to hardwire regulation in all computing devices in an attempt to enforce copyright restrictions have faded away in the face of resistance from manufacturers and consumers, both by lobbying and in the marketplace.

**Competition Law and the Internet**

Are there solutions that may be effective ex ante to ensure the development of technologies that do not act against the public interest, without stifling innovation and introducing bureaucratic interventionist regulation to an area that has blossomed without it? Such a solution would avoid the economic determinism of belief in the invisible hand of the market, and the technological determinism of some (typically super-profitable multinational) technology companies that claim that progress all but inevitably results in wider choice and more desirable features, despite public policy concerns.

Two examples present themselves: one a remedy of necessity in competition law, the second a deliberate design feature increasingly being deployed by OECD governments. The first is the use of competition law to engage in predicting and designing prospective markets, and the second is the widespread adoption of interoperability policies across the European Union.

Institutions that apply the consumer interest in the case of mergers and other market concentrations differ markedly by country (Weiser 2010; Coates 2011). Agencies follow enabling legislation, and therefore the breadth of definition of competition problems should reflect and adapt from that original legislative intent, despite much of its age. For instance the United States applies the Sherman Act (1890) and Clayton Act (1914), and the EC applies the Treaty of Rome (1957, articles 101–102 as amended), based on updated Guidelines to enforcement agencies (European Commission 2011b). In some nations, there is only a general consumer and competition agency, which has oversight of communications market mergers. In others, such as the United States, there is cooperation between two competition agencies and one communications regulator: the Department of Justice, FTC, and Federal Communications Commission. In yet others, there is a single competition agency assisted by a communications regulator with some competition powers (in the United Kingdom, incorporating two appeals bodies that oversee regulator decisions). A growing European trend is toward the communications regulator forming part of a larger network utilities regulator as with BNetZ in Germany and the Dutch networks regulator OPTA. These institutional differences are obviously vital for our consideration of the regulation of code, as the proficiency of regulators will differ enormously based on institutional preferences as well as the vagaries and happenstance of personal skills. Thus one expects communications regulators to have greater code expertise than general competition agencies, though this may not always be the case, particularly where the communications regulator is poorly adapted to digital networks and relies on telecoms and broadcasting analysts with a paucity of software
skills. The recognition of particular code problems and application of specialist staff and advisers is greatly to be desired in such cases. A particular example is the FTC creation of a post of chief technologist, filled by an academic visitor (Ed Felten), and a special advisor also taken from academia (Tim Wu), in 2010–2011 as the agency actively pursued solutions to code issues.

The recent literature on competition policy has tended toward substituting economic judgments of consumer harm for political judgments and the apparent triumph of the Chicago school of microeconomics and associated economic doctrines regarding the perfectability of competition (Lessig 1998). The notion of creative destruction, whereby a lazy monopolist is overwhelmed by an innovative flexible competitor, has gained much ground, following the work of Joseph Schumpeter and the Austrian school (Mehra 2011). The Internet had appeared secure ground for Schumpeter’s hypothesis, and social networks even more so, given News Corporation–owned MySpace’s dominance that was replaced rapidly by that of start-up Facebook between 2007 and 2009. Against this must be placed two rival readings of this case study. The first is that social networks were an immature medium, and the growth of the market floated all ships in enabling all rivals to grow while consumers experimented. Consumer preference led to a maturing of the market, which itself tilted toward the eventual winner, Facebook, whose monopoly is now arguably durable. The second reading is more structural: that social networking had relatively low entry barriers in the past, as did, for instance, search engines, but that the advertising-dominated mass market model that currently applies is inimical to the successful overturning of Facebook’s dominance. Internet markets are not in continuous “Schumpeterian emergency” (Bresnahan, Greenstein, and Hendersen 2011).

The fertile testing ground of social networks can be once more employed as Google+ challenges Facebook, just as Microsoft’s Bing search engine challenges Google’s main search engine business. Net neutrality deals with a century-old monopoly over copper telephone wiring into the home that has been leveraged by state-sanctioned monopolies as it became possible to attach modems and other appliances to the copper telephone network. Schumpeterian creative destruction theory in such a durable and high-entry-cost environment is arguably a misapplication. One could date concern over closed walled garden social networks—closed areas of moderated content and services intended to encourage users to stay within affiliated Web pages and thus attract advertising—further back to the time of the MCI investment in News Corporation, leveraging its ISP access business into content (Noam 1994).

**Interoperable Code and Communications Policy**

An extensive legislative and regulatory history of public communications occupies a special place in regulatory policy far predating modern competition law. This has always justified an ex ante regulatory policy. The loss of the ability to license does not of itself entirely negate ex ante regulation—standards define the architecture of code, and standards are heavily government influenced even when not government funded. The government imprimatur on standards enables significant, which is arguably as true in the twenty-first century as it was for Marconi.
The notion that communications policy introduces certain rights and duties is as old as electrical and electronic communications media, with the 1844 Railways Act in the United Kingdom introducing the right for government to take control of the telegraph for the national interest—this only seven years after electric telegraph technology was standardized. Cannon (2003) suggests that the fundamental regulatory constraint imposed on U.S. telecoms firms in the 1980s was open network architecture (ONA) under the 1985 Computer III inquiry by the U.S. Federal Communications Commission (FCC). (The Computer II and III inquiries refer to investigations by the FCC into the regulation of data transfer and the conditions necessary to achieve an increasingly competitive market for that data.) This constraint had its European equivalent and amounted to interoperability plus physical interconnection between networks (Coates 2011). This was a rare early example of full technical harmonization, which allowed the Internet to flourish across borders without being stymied by pre-existing telephony regulation.

ONA had its legacy in the FCC championing regulatory forbearance (Oxman 1999) in the late 1990s, notably in the “Digital Tornado” working paper (Werbach 1997), which further institutionalized the policy of preventing telecoms companies from foreclosing Internet access and was widely admired and copied by European and other regulators racing to catch up with the phenomenal growth of the Internet. U.S. readers should note that mass consumer adoption of the Internet in Europe dates to 1998, as earlier per-minute charging for local telephone calls had chilled the market. In fact, the subtle interoperability pressures of Computer III were much criticized by innovators in the 1980s as they removed the structural remedies against incumbent telephony players (which Computer II had instituted in 1975, finalized in 1980), replacing them with a behavioural solution. As it emerged, this type of control may have had its legacy in the failure to fully ensure unbundling in telecoms in the early 2000s (Frieden 2010a), but for our purposes, it more pertinently leaves a legacy in the interoperability imposed on AOL’s Instant Messenger in the merger conditions for its takeover of Time Warner in 2000 (Faulhaber 2002). ONA and its forerunner, comparatively efficient interconnection, were still used in orders against U.S. incumbent telephony operators (the “Baby Bells”) until 1999. More recent examples of using interoperability, the ONA legacy, include the conditions imposed on Microsoft by the EC in settling its competition lawsuit (EC 2010c).

The AOL–Time Warner merger of 2000 introduced the notion of regulation for interoperability in the case of vertically integrated ISP social networks, even though interoperability was not eventually enforced. It also reflected a trend toward using merger proceedings to raise public policy concerns including privacy and interoperability, if not always to address them successfully. Thus, as detailed in chapter 7, the beginnings of the modern network neutrality debate date to cable TV mergers with ISPs in the late 1990s and the concern surrounding ISP control over access to information, recognized as an international human right since the Universal Declaration of 1948.

The use of competition proceedings to introduce human rights concerns in communications raises two threshold issues, the second of which (the special case of communications) we consider in the next section. The first is whether human rights concerns are ultra vires as not
relevant to the consumer interest in mergers. Note that this can depend on the width of the definition of consumer interest. That in itself can be unpacked to consider two issues: how much the consumer interest is subsumed into its proxy, competition policy, and whether the institutional governance of consumer welfare permits human rights considerations, dependent on whether the specialized agency (or agencies) has any such competence and expertise. In permitting the consumer interest to prevail over the private property rights of a corporation, we are of course balancing rights in the U.S. context, where corporations are granted more substantial legal personality, though fewer such considerations appear to apply in the European human rights context.

A warning against overenthusiasm for rights discourse as a partner to competition policy is that in the Google purchase of DoubleClick, the Department of Justice and EC Directorate-General for Competition both refused to take privacy concerns into account in scrutiny (Coates 2011). Future cases or legislation would need to overturn this precedent if competition regulation were to be an effective mechanism for protecting fundamental rights as well as economic efficiency. It has taken many years for Internet access to become recognized as a right (Murray and Klang 2005). In 2010, Finland was the first of several countries introduced a universal right of access to the broadband Internet. This continues a universal service obligation on communications that dates to radio broadcasts, telephone service (the Kingsbury Commitment, made by the chairman of AT&T to the FCC, dates to 1913), and common carriage, which predates all these, as a common law duty and privilege imposed on certain activities, typically in transport (ferries, haulage, and stagecoaches; Cherry 2006).

**Interoperability: A Code-Based Solution**

There is an extensive history of competition policy in favour of open technology standards that long predates the Internet (Kahin and Abbate 1995, but the evidence of extensive network effects and innovation that can rapidly tip markets has helped focus policymakers’ attention on the potential for using interoperability as a solution to the online competition and innovation problems that have emerged. As competition policy provides for interoperable remedies, governments have set great store by the success of open standards as solutions for the well-known entrenchment of dominant Internet commercial actors using network effects (Pitofsky 1998; Lemley and McGowan 1998). Bar et al. (1995) observed that “interconnection is binary—you are either connected or not—but interoperability comes in degrees [and] presupposes a higher level of logical compatibility”: the higher the compatibility, the greater the interoperability.

Understanding code and legal regulation leads to a better understanding of how regulation can work toward better code rather than simply avoiding the worst of code. That conjunction of code and regulation will lead to better outcomes than a Chinese wall designed to keep out code. We therefore explain how innovative regulatory and policy responses to the increasingly controlled Internet user experience can harness the power of code to create opportunities for innovation rather than erect entry barriers to new applications. That leads to consideration of the code remedies imposed on Microsoft in the European Commission (EC) final settlement of its antitrust case in 2009 and Intel in its Federal Trade Commission (FTC)
antitrust settlement of 2010 (Coates 2011). We argue that interoperability is the key to regulating dominant actors’ uses of code. Such checks to encourage competition do not ensure fundamental rights that must be respected in communications industries, and we argue that improved competition law enforcement to shape more interoperable code must be accompanied by human rights audits to create greater commercial and state respect for fundamental rights.

The outcome of the two decades of Microsoft competition litigation, beginning with U.S. antitrust investigation in 1991 prior to the dawn of mass Internet adoption, was to enforce interoperability and application programming interface disclosure (EC 2010c), with Intel settling a similar long-standing investigation into interoperability and anticompetitive practices. The interoperable code solution was extended and adapted by the complainants in both Google and Facebook investigations by the EC opened in 2010 (IP/10/1624). Apple’s iTunes faced similar calls in its price discrimination settlement by the EC in 2007–2008 (IP/08/22) and its preliminary antitrust investigation into Apple’s App Store policies (IP/10/1175).

The market and information failures of the network effects pervading the Internet were noted by the chair of the FTC as early as 1996 and have been in evidence throughout its development (Bar, Borrus, and Steinberg 1995; Lemley and McGowan 1998; Cowie and Marsden 1999). As the technology stabilizes and matures, it may be that less radical innovation lies ahead, but we see no reason for policymakers to surrender entirely to a cable television model (Lemley and Lessig 1999) for the Internet in copyright or carriage or convergence on social networking. Therefore, solutions that maintain interoperability and open standards, which drove Internet, World Wide Web, mobile, and computer innovation in the 1990s and 2000s, should be maintained against the Janus-faced comfort of a largely walled-garden, passive Internet future.

Most merger decisions throughout the period 1996 to 2011 supported interoperability and open standards, including European media mergers in the mid-1990s, the AOL-TimeWarner and Baby Bell mergers subject to Computer III requirements, and European Commission abuse of dominance decisions against Intel, Microsoft, and Apple. It is our contention that similar remedies should be pursued against the new information monopolists of Google and Facebook, where abuse of dominance is found. Google and Facebook negotiated consent decrees after user privacy breaches, which commits both to agreeing to privacy audits of all products and applications every two years until 2030.

Agencies regulating antitrust and competition issues have a deep cleft between their competition economists and their consumer advocates (Mehra 2011), a division that at the Federal Trade Commission had traditionally been physical as well as intellectual. Even as innovative arguments are made for intervention in high-technology networked markets, intellectual resistance runs deep (Verizon v. Trinko 2004; Meisel 2010; Barnett 2011; Manne and Wright 2011). Communications regulators have similar silos, even the yawning chasm between telecoms and broadcast regulators, the former concerned largely with network economics and technical proficiency (Laffont and Tirole 2001; Cave 2004). For instance,
Spulber and Yoo (2009) introduce network theory to the study of the economics and law of telecommunications and in so doing adopt a minimalist view of the application of the essential facilities doctrine to the Internet’s plumbing. Pro-consumer arguments (Reding 2007) to the contrary in Europe are viewed as European exceptionalism by the isolated United States. The broadcast regulators should be concerned with the rights of the citizen and consumer to receive balanced information on that ubiquitous and pervasive medium (Cowie and Marsden 1999). We argue that little has been done to support prosumers as opposed to passive viewers (Directive 2007/65/EC Articles 1–2).

Essential facilities law is a very poor substitute for the active role of prosumer law that we advocate, especially in its Chicago school minimalist phase (Lessig 1998). In the late 1990s, as the Web was developing and Microsoft was crushing Netscape in what is elegantly described as its moment of “Schumpeterian emergency” (Bresnahan, Greenstein, and Henderson 2011), it was still possible to agree with Schumpeter, Scalia, and Easterbrook (Mehra 2011) that innovative upstarts could outwit clumsier behemoths (Cowie and Marsden 1999; Lemley and McGowan 1998). This was not the real lesson of IBM and Microsoft in our view.

This is a less radical proposal than the separations principle of Wu (2010), who proposes a rigid separation between carriers and content and applications providers, based on historical analysis of previous communications industries—including the FCC’s 1970 Financial Interest and Syndication (“fin-syn”) Rules in cinematic production and distribution, as well as the concentration in the telecommunications industry resulting from the 1996 Telecommunications Act. Our analysis is similar but has shown that effective enforcement of interoperability is possible even in the face of vertical integration by incumbents. This in part reflects the view from Brussels, where less obvious regulatory capture of the political process of communications regulation takes place. National policy may be entirely captured, but even its harshest critics must admit the European Commission is more insulated by its supranational character.

Paradoxically, this may be due to a political contaminant in competition policy. European competition policy is less captured by the minutiae of price-based abuse of dominance than the United States, even though this is the direction of travel (Coates 2011). As a result, the more interesting interoperable solution in such cases as Microsoft is possible, whereas the Microsoft case was settled rapidly in the United States after the George W. Bush administration took power. It might be argued that the European targets were American firms with homes of convenience in Ireland or Luxembourg for European legal purposes, which of course and undoubtedly defuses much political pressure for leniency.

Competition policy is also not the only European or U.S. initiative. The EIF 2.0 emphasis on interoperability as a priority in both government procurement and in research and development offers a broader toolkit than competition policy alone can provide, in part a function of the fortunate placement of the former competition commissioner in the Directorate General Information Society responsible for the EIF. We argue that a separations principle to break up monopolies across the information field is neither feasible nor entirely
necessary in the European context (Cave 2004, 2011). Examples of industries switching under competitive pressures that create new market models will prevent radical separations policies from being adopted, as Facebook’s success over MySpace and Apple’s success in creating a music store free of digital rights management argue for interoperability, not separation. Moreover, the fight to establish interoperable electronic book standards will not be answered by structural separation, as Apple, Amazon, and others tussle to offer standards to the market.

Moreover, the interoperability approach does prevent a further regulatory arm wrestle of the type that Wu so colourfully chronicles and has pervaded the history of pre-Internet communications policy. It does depend on effective enforcement, and in this it suggests a heroic commitment to such policies at national as well as European levels, which critics suggest is beyond the European Commission’s appetite for implementation (Moody 2010). Critics may argue that an approach founded largely on the relatively puny market impact of the Microsoft decision is grasping at the shortest of straws. The alternative, trench warfare based on regulatory attempts to re-establish rigid separation of functions (Kroes 2010a), is in our view both an excessive intervention given the continuing flow of innovation in the Internet ecosystem and likely to favour the politically skilled incumbents more than scrappy entrants, as we have seen in our case studies.

A comparable example is the attempt to separate retail from investment banking. This has been a far higher political priority in the wake of the vast regulatory failures in bank regulation since 1980 but shows little real progress since 2007’s calamitous revelation of the extent of the larceny in the banking system in the United States and Europe (Davies 2010). We accept that a complex and interlocking EIF will depend on coordination between member states and the European Commission, a coordination shown to be spectacularly lacking in the altogether more important matter of the governance of the single European currency in 2010 through 2012. However, interoperability is technical enough, and its problems and potential hostages lie far enough away from Brussels (mainly in Silicon Valley, San Diego, and Seattle) that a heroic policy signal is possible.

The FTC may have shown the way in its treatment and settlement of the Intel case, with its emphasis on interoperability requirements as a remedy with a six-year period stated and conditions affecting interoperability and patent policy in the case of change of control, a spectacularly invasive example of interoperability being hard-wired (FTC 2010). It is coincidental and fortuitous that interoperability can also mean free software in principle (however expensive its implementation and integration with legacy systems). Politicians who (perhaps mistakenly) assume that interoperability is a free and leisurely European lunch are more likely to support that policy. However, we recognize that interoperability is neither a simple nor a cost-free option (Gasser and Palfrey 2012), nor that it should be imposed without prima facie evidence of dominant actors’ refusing to provide interface information that permits interoperability. Commissioner Kroes (2010a) referred to the arduous attempts made by antitrust authorities on both sides of the Atlantic to ensure interoperability in the Microsoft and Intel cases. The outcome was to deny those actors the tools to exclude
innovative competitors from the market. Hard-wired interoperability is the most promising solution to achieve those ends, however tortuous the task.

It has been suggested that open participatory standards are themselves better for the development of fundamental rights in terms of participation (Drahos and Braithwaite 2002) and more equal access to information (La Rue 2011). This raises normative questions such as: Is an open source operating system such as Linux ultimately a better foundation for the information society (Van Oranje et al 2005) than a proprietary operating system such as Windows? Is Android better for wireless innovation than Apple’s iOs? Is Firefox a better Web browser for developing countries than Microsoft’s Internet Explorer? Is the non-hierarchical Internet Engineering Task Force better for participation and designing standards for human rights than the nation-state-dominated International Telecommunications Union? We test a profound claim of those who favour open standards: information standards that are more open and participatory are more just in terms of both competition and human rights (Clinton 2011). That has been sloganized in terms of a basic norm as “information wants to be free” (Brand 1985), “information communism” (Benkler 1998, 2011; Lessig 2008), and even “dot communism” (Moglen 2003). These claims have been variously adopted by such entities as the Free Software Foundation, the Pirate Party, the Creative Commons movement, and the Access to Knowledge movement. There is no objective right answer to such normative claims, simply assertions of short-versus long-term efficiency or social welfare maximization. However, a solution that closes off the choice for innovators in how to develop their own products in such a contingent environment is gambling with the future.

Support for an open environment to stimulate innovation does suggest less corporate control of the value chain and possibilities for state censorship (Zittrain 2003) but does not in itself guarantee fundamental rights. The wider the choice of code available to users, the higher their ability is to choose code that respects their speech freedoms and personal data, but that is by no means a given. Creating conditions for interoperability does not enable governments or corporations (or civil society) to shirk the responsibility to ensure Internet architectures respect fundamental rights. For example, communications equipment that can help repressive states monitor users and ultimately punish dissidents creates an obligation on manufacturers and democratic governments to prevent export of such technology to such states (Brown and Marsden 2013, MacKinnon 2012). While that is not yet a regulatory aim that has been enforced, a fundamental rights argument (and Google’s mission statement, “Don’t Be Evil”) argues that such a regulation would need to be placed on top of any innovation or competition arguments in such a specialized sector (Brown and Korff 2012).

Dolmans (2010) suggests that an established common standard that is truly open allows the best-of-breed components from different manufacturers to be combined, with maximum efficiency. To qualify as “open,” he argues that a standard must meet a number of open conditions: access to the decision-making process; transparent and undistorted procedures; published, pro-competitive goals; published, objective, relevant criteria for technology selection; and no over-standardization. Most critical is access to the standard, which he argues includes open information on blocking patents (the cause of much patent thicket litigation in smart phones and tablet computing), no unjustified refusal to license, and fair
reasonable and non-discriminatory (FRAND) pricing (Coates 2011; EC 2011a). Dolmans suggests that royalty-free licensing is advisable in the software arena, allowing both open source and proprietary software to compete on quality and functionality. However, the telecommunications sector should use FRAND licensing, given the price and complexity of standard-setting efforts. He states: “Mandating royalty-free licensing would likely recreate a tragedy of commons and discourage innovation, while allowing IPR owners to charge at will could create a tragedy of anti-commons. To strike the right balance, therefore, a contract of mutual restraint is necessary” (Dolmans 2010, 126). This argues for a mixed market and against uniform royalty-free pricing.

Unfortunately, open interoperable solutions have not entirely solved the market entry problem. The flexibility, or fungibility, of code and the degree to which default settings can adjust user behaviour give rise to one of the more interesting experiments we can conduct using Internet policy. Given the claim by behavioural economists and their supporters (Thaler and Sunstein 2009 that signalling and “nudging” by government can adjust consumer and market behaviours, we also examine in our case studies to what extent government actions can be characterized not as a nudge but as a much more complicit association with private actors (Yeung 2012). We could characterize that as two types: “nudge” where neither corporate nor government actions are carried out without mutual reinforcement, or at least joint dialogue, or “wink” where non-legislative solutions are adopted by corporate developers, but users decide whether to follow these more subtle nudge signals (e.g., including abandoning copyright enforcement by digital locks altogether using P2P software).

Internet regulation appears to be a particularly promising arena in which to explore the types of weak signalling and their effect, if any.

The EC’s thinking on interoperability and code has developed through the course of the Microsoft, Intel, and Rambus cases (Coates 2011). Neelie Kroes was competition commissioner from 2005 to 2009 and signalled more intervention on interoperability: “I will seriously explore all options to ensure that significant market players cannot just choose to deny interoperability with their product” (Kroes 2010). She argues that the lengthy Microsoft case has lessons for action: “Complex anti-trust investigations followed by court proceedings are perhaps not the only way to increase interoperability. The Commission should not need to run an epic antitrust case every time software lacks interoperability.” Eighteen years of transatlantic competition proceedings against Microsoft resulted only in a choice of browsers, a very large but proportional fine, and some old code being released.

Kroes’ solution to the Microsoft dilemma—solving the antitrust problem long after the competitors have died—is to require ex ante interoperability evidence, which had not previously been available except through antitrust suits: “Whereas in ex-post investigations we have all sorts of case-specific evidence and economic analysis on which to base our decisions, we are forced to look at more general data and arguments when assessing the impact of ex-ante legislation.” She argues for a potential future legislative proposal, which would impose an ex ante requirement to publish interoperability information.
Microsoft and Intel’s settlements illustrate a general point about smart structural remedies under competition policy: network effects demand very effective transatlantic cooperation plus policy formed from research into global information technology. This applies the Lessig “code is law” analysis but with Braithwaite and Drahos’ international coordination regulatory approach applied to the overall information environment (Braithwaite and Drahos 2000; Drahos and Braithwaite 2002). Note that the forerunners of the suggested policy direction are 1980s data protection and 1990s cryptography cooperation.

If free and open source software has not proved a significant competitive check on information monopolists, that raises a significant regulatory challenge that governments must meet to create interoperability in those dominant actors’ own software. Kroes (2010) set out a radical agenda to ensure interoperability in European ICT procurement and regulation, drawing on procedural frustrations in the Microsoft case. It is in five parts:

1. A new standard-setting framework
2. New horizontal agreement guidelines to establish more transparency in licensing standards (EC 2011a: chapter 7)
3. A common framework for ICT procurement
4. A new European interoperability framework (EIF)
5. Intervention in competition cases to establish a principle of interoperability, including through ex ante requirements.

The EIF is a second version of a much less ambitious 2003–2004 first version of the framework. EIF Version 2.0 was adopted by the College of Commissioners “as of a higher status and importance than EIF version 1,” which was more guidance than instruction. EIF 2.0 has been severely criticized by open source advocates, with the EC accused of regulatory capture by large software companies and the interoperability requirements substantially watered down (Moody 2010).

The new standard-setting framework was established before the end of 2010, intended to result in a widening of participation from the European telecoms standards body, European Telecommunications Standards Institute (ETSI), to more Internet-based standards bodies, W3C and Internet Engineering Task Force in particular, arguably about twenty years too late (International Telecommunications Union 2010). Kroes explains that her proposal benefits these “truly open” standards with two paths to approval: “via a fast-track approval of their standards through a process hosted by a traditional European standards body such as ETSI, or through the assessment of these bodies’ compliance with certain criteria regarding notably openness, consensus, balance and transparency.” On licensing standards, she notes the commission drafted horizontal agreements guidelines in 2009, which came into force in January 2011 (European Commission 2011b), and aid in allocating FRAND pricing for accessing essential technologies (EC 2011a). Kroes does not argue for uniformity: “Standard-setting for software interoperability is not the same as setting a new standard for, say, digital television or mobile telephony.” She continues to suggest strategic action to encourage open standards. This suggests an additional legislative requirement that government support for standards must rely on best practice in licensing including royalty terms.
Kroes’ agenda embraces research funding and government information technology procurement. European law requires governments to ensure they open public procurement contracts above a minimum size to all European firms to encourage the development of the single European market (Directive 2004/18/EC). As government spending is about half of European GDP, this opens the largest single information technology market to interoperability. Member states that fail to register procurement contracts with the EC are subject to infringement actions and ultimately court proceedings, though implementation has not been as rigorous as it might be. Market-setting procurement EC policy can be used to pursue EIF 2.0. On IT procurement by European governments, Kroes (2010) suggests “detailed guidance on how to analyse a technology buyer’s requirements in order to make best use of ICT standards in tender specifications.” Governments became unintentionally locked into proprietary technology for decades. An IT vendor “cartel” was alleged by government buyers on both sides of the Atlantic in 2011, publicly voicing their frustration at the limited choices available. EIF 2.0 contains a “comply or explain” requirement if government buyers do not adopt an available open standard, which follows the practice in the Netherlands, Kroes’ own country.

In the first phase, the EC (2010a) adopted the communication to “establish a common approach for Member States public administrations, to help citizens and businesses to profit fully from the EU’s Single Market.” The EC has a four-prong strategy: common frameworks in support of interoperability, “reusable generic tools,” “common services” (operational applications and infrastructures of a generic nature to meet user requirements across policy areas), and “analysis of the ICT side in the implementation of new EU legislation.” As Ganslandt (2010) argues, the four prongs are not likely to be sufficient without a more effective enforcement strategy. The European Parliament (COD/2011/0150) responded to the standards strategy by proposing direct funding for small and medium-sized enterprises and civil society to participate in the standards that underpin the entire strategy, confirming a multi-stakeholder approach to be adopted, though substantial disagreement ensured in committee over whether “balanced,” “relevant,” or “appropriate” representation should be established and financially supported. These proposals are promising, but no conclusions can be drawn, as they are both ambitious and yet to be implemented in practice.

In response to the dominance of commercial code sellers, notably Microsoft but also other infractors of competition rules, antitrust and regulatory authorities have adopted comprehensive interoperability strategies including EIF 2.0. Among them are standardization strategies that extend to the entire organization of standards bodies themselves and establish class monitoring of standards. They also include procurement requirements for interoperability on government contracts of more than about $200,000 (Regulations 1177/2009 and EU/1251/2011). This strategy is intended to ensure a fundamentally open approach to information technology standards.

In terms of code outcomes, we also need to ask whether there are alternate ways to consider solutions rather than those adopted: forks in the path or alternate dependencies? An example might be using legislation rather than code (or vice versa) or industry or consumer-led solutions where the opposite actually occurred (Bresnahan, Greenstein, and Hendersen 2011).
Institutional examination needs to account for alternative histories, as previous Internet policy studies have concluded following North (1990; Mueller 2010; Benkler 2006). Our framework and conclusions can be applied to two recent developments, based on our continued examination of the issues in 2012-13. These are the continued competition investigations into Google’s dominance of search advertising, and the privacy law reforms specifically applied to social networks, notably Facebook. We note as background that net neutrality, state censorship and copyright reform all remain mired in exactly the public goods failures that we have extensively documented.

**Search Markets: Google**

Google has faced competition investigations on both sides of the Atlantic since 2010. It settled with the US authorities on 3 January 2013 (FTC 2013), and sent a settlement proposal to the European Commission on 1 February 2013 (Brunsden and White 2013). Experts have severely criticized both the timing and content of the Obama Administration’s settlement, which they portray as extremely favourable to Google due to the composition of the outgoing Federal Trade Commission (FTC) board, and the decision not to proceed against the company on the main issues raised. Grimmelman (2013) argued: “If the final FTC statement had been any more favourable to Google, I’d be checking the file metadata to see whether Google wrote it.” The European Commission investigation continues as we write, with the same four principal complaints raised against Google as in the US:

1. **Search bias** – that Google favours its own products in search results over competitors;
2. **Vertical Search Opt-Out** – Google protocols don’t let websites opt out of particular uses that Google might make of the pages it indexes. A complete opt-out means giving up all Google traffic, a significant driver of traffic – especially in Europe where Google has almost 90% of the search market in the UK, and over 90% in Netherlands, France and Germany;
3. **Restrictions on third party use of AdWords** in one crucial respect: “The AdWords API Client may not offer a functionality that copies data between Google and a Third Party.” Companies can advertise on Google and Bing, but cannot use a program to copy Google AdWords campaigns over to Bing. This was dropped by Google as their token interoperability sop to the FTC’s investigation;
4. **Injunctions against standards-essential patents**, including those by Google-acquired Motorola Mobility (and see the Posner (2012) now–famous judgment). The FTC concluded (4-1) that the practice is unfair competition, and Google agreed not to engage in it in the future. This fires a shot not just at Google, but also at all its rivals – a clever concession by Google.

While it would be dangerous to speculate whether the European Commission can wring any concessions on the first two points, it is worth noting that on points 3 and 4, it is Google that had claimed the right to regulate others’ use of code, to use the AdWords API or to use Motorola Mobility’s patents. Google and its competitors routinely privately regulate each other’s code.
What we suggest is a “prosumer law” approach where interoperability and content neutrality are taken more seriously by European regulators, as the former Commissioner has continually threatened ever since the brutally extended Microsoft European competition litigation ground to a conclusion (Coates 2011, Kroes 2010). The first objection can be resolved through forcing Google to reinforce its search neutrality rather than bias results using its search algorithms (Bracha and Pasquale 2008), and the second by a relatively trivial (by Google standards) amendment to its code to allow other websites more flexibility in future listing, rather than the ‘nuclear option’ of a complete opt-out via the existing robots.txt convention.

We do not adopt a strong normative claim that Google should adopt an entirely neutral perspective (nor do we adopt such an approach to network neutrality), but we do advocate enforcement of truth-in-advertising, that any search engine (or ISP using search) claiming verifiably neutral results produce the same, or else be made to prominently advertise its product as a commercially driven, affiliate-biased selective search engine. Search neutrality would require that any Internet search engine provide search results that correspond to its mission to search the Internet for relevant products, with any ‘promoted’ products advertised as such and separated from the search results requested by the user. Note that this is exactly the solution that leading search engines claim to provide, with ‘sponsored links’ boxes separated from the overall results in either a side-bar or more intrusive text box above the main results (Bracha and Pasquale 2008). That would not prevent linking to an affiliated maps provider, or shopping engine, as long as these links are not in the main results. Such a requirement does not impose a significant regulatory burden on a search provider, rather it reinforces the brands of search providers of integrity. It would not apply to selective search providers if labelled as such: ‘a search engine which selectively provides you with search results according in part to its commercial affiliations’ (or equivalent wording) would need to be prominently displayed above search results if that were the case. In the book, we suggest a similar approach to network neutrality violators, who could not advertise their services as allowing end-users’ choice in accessing the ‘Internet’ when in fact it is a commercial Intranet to which full access is provided (Brown and Marsden 2013).

These code-based solutions are lighter touch than multi-billion Euro fines or structural separation of businesses (Wu 2010). This is an illustration of what we mean by a smarter ‘prosumer law’ approach. Prosumers enjoy using Google products, and would like to trust Google more by seeing transparency rather than bias. Google is not evil, but it is a stockholder company, and its directors’ duties since it was floated publicly in 2003 are to maximise returns. Regulated capitalism demands a response that works with markets and prosumers.

Social Networks: A Prosumer Problem

We give an example of our proposed solution to the problems of dominant social networking services. Descriptions of personal data as the metaphorical oil in the digital economy are wide of the mark, even for data of the deceased (Edwards 2013), unless they have seeped into the sediment. Personal data accumulate with the individual’s treks into cyberspace, and therefore a better metaphor is silk, woven into the tapestry of the user’s online personality. Moreover, user is a poor description of the potential creativity of the individual user (Von
Hippel 1976; Morrison, Roberts, and von Hippel 2000) in cyberspace. The hideous ugliness of the term prosumer (the online creator, after Toffler 1980) should not hide the potential for the individual to move far beyond a caterpillar-like role as a producer of raw silk and encompass their ability to regenerate into a butterfly or moth. The verb to surf indicates the user-generated agenda of the prosumer, as does the weaving of a web by billions of prosumer-created sites. The silk has created tapestries as rich as Wikipedia, as well as Facebook and MySpace (Benkler 2006). It is arguably the loss of the sense of ownership of “your space” that led to the latter’s decline. The silkworms that turned created a death spiral (Mehra 2011), even though it was at first only a prosumer boycott (led by those who preferred to control their data cocooned in their own personal form: chrysalis or pupae). The problem is that such boycotts rapidly create a landscape of zombie users: many readers will have ancient Hotmail and MySpace accounts that are undead, uncheckd, unmourned, useless to advertisers, and antithetical to positive network effects that alone can feed a successful business. We portray an information landscape with a billion captured moths creating silk for ever fewer merchants, notably Google, Facebook, Amazon, and Apple. Allowing those moths to evolve and choose whether to exit, control their own prosussion, or continue their silken personal data capture is a key question for prosumer law.

If Google’s flotation took some time to wipe away an idealistic founders’ myth of anti-evil cartoon-book coding, Facebook’s 2012 flotation required no such adjustment. Facebook’s buccaneering attitude to ‘monetizing’ your personal intimate data, and those of your children and grandchildren, was recognised long ago as requiring greater regulatory action. The European home of half of its users has 27 state regulators of personal data, and Facebook chose one that relocated in 2006 from Dublin to Station Road, Portarlington, Co. Laois, Ireland (Department of Justice and Equality 2006), resulting in wholesale removal or resignation of its expert staff. Google is also regulated from Portarlington. While German state and federal regulators and others may rattle sabres at Facebook, it is the Irish regulator that took action in auditing Facebook in spring 2012 and insisting on remedial action on at least nine counts (Brown and Marsden 2013: 134, Office of the Data Protection Regulator 2011).

Prosumer Solution to Social Networking
What should prosumer law consist of? It is not sufficient for it to permit data deletion because that only covers users’ tracks; it does not entitle them to pursue new adventures, particularly where all their friends (real and imagined) are cocooned inside the Schumpeterian victor’s web. It requires some combination of interconnection and interoperability more than transparency and the theoretical possibility to switch (Werbach 2010; Weiser 2009). It needs the ability for exiting prosumers to spread their wings, take their silk away from the former exploiter, cover their traces, and interoperare their old chrysalis with their new moth life. That suggests interoperability to permit exit (Burk 1999).

Consider the problem with two hard examples: network neutrality and social networking systems (SNS). In the former case, users can exit an ISP that is breaching network neutrality, subject to two as-yet-unfulfilled conditions: that full, meaningful consumer transparency is offered and that switching is trivial, in particular that consumers can leave their minimum-
term contract (typically two years) because the ISP has breached its side of the bargain by introducing non-neutral practices. Because consumers keep control of their data (except for law enforcement data retention purposes) and can delete cookies, extract files hosted, and so on, then absent behavioural advertising of the deeply invasive Phorm type (using Deep Packet Inspection to track the prosumer’s Web browsing), they are free to leave. Moreover, they can take their telephone number with them to their new ISP. That does presuppose there remains a neutral ISP in the environment, which is not by any means certain for the Skype-active mobile user (Sahel 2011). Regulatory action in transparency, switching, and contract exit is needed.

In the case of SNS, such a relatively easy transition is not assured. First, there is the extraction of the user’s proprietary data. While the Irish regulator decision ensures that data can be returned (Office of the Data Protection Commissioner, Ireland 2011), it does not cover all the data cocooned in one piece. First, Facebook removed data to the United States without valid consent, as, for instance, in the Like button dispute in Schleswig-Holstein in 2011. Second, data were leaked promiscuously to third-party application providers, as the Federal Trade Commission (FTC) discovered. Third, the formatting of the data and the need to access friends’ data (e.g., wedding and baby photos), which are indiscernible using a search engine, mean that the user is in the position of: “You can leave Facebook, but Facebook never leaves you.”

Prosumer law suggests a more directed intervention to prevent Facebook or Google+ or any other network from erecting a fence around its piece of the information commons: to ensure interoperability with open standards (Lemley 1999). We argue that it is untrue to state that there is so much convergence between platforms that there is no clear distinction between open commons and closed proprietary environments (Barnett 2011), though voluntary forfeiture of intellectual property rights to permit greater innovation has always been commonplace (Bresnahan, Greenstein, and Henderson 2011; Barton 1997). It also suggests that Google’s attempts to adjust search in favour of its products, if proven to extend beyond preferential puffery for Google+, are inimical to prosumer law.

Prosumerism should be a declared policy of the European Commission alongside the European interoperability framework (EIF). European electronic commerce consumer law is a marked departure from freedom of contract in European law. It is therefore not difficult to extend the EIF and the legal protection for prosumers in this direction in law, though implementation requires all member states to commit to such a step in practice as well as theory.

One promising solution to the otherwise patchy nature of regulation is that of SNS interoperability. In earlier work we have identified high sunk costs and network effects as barriers to entry protecting dominant SNS: “The behemoth SNS can influence negotiation with ISPs absent net neutrality regulation, leading to a vertical value chain of dominance” (Brown and Marsden 2008). We proposed that “competition authorities should impose ex ante interoperability requirements upon dominant social utilities . . . to minimise network barriers” and identified three models of information regulation from case law:
• Must-carry obligations, which are imposed on broadcasters and electronic program guides

• Application programming interfaces (API) disclosure requirements, which were placed on Microsoft by the European Commission ruling upheld by the European Court of Justice

• Interconnection requirements on telecommunications providers, especially those with dominance—already echoed in the AOL/Time Warner merger requirement for instant messaging interoperability.

We also recommended that “API disclosure requirements are necessary but not sufficient—the ability to program platform apps is of little use if they cannot run” (Beydogan 2010). Must-carry obligations enable one platform to “break in” to another (e.g. Flickr’s app on Facebook). Interconnect requirements [are] most likely to lead to seamless user experience that will create real competition.” This would impose telecoms interoperability and switching requirements on SNS.

Historically, broadcasters and cable operators did not necessarily enjoy good bilateral relations, viewing each other as competition—in the same way ISPs such as AOL/TimeWarner saw emerging SNS as competition. The success of both Facebook and the AppStore gives pause to those who champion an entirely open model, as consumers appear to prefer low-walled gardens, a debate endlessly reiterated since the AOL walled-garden service. Nevertheless, SNS are another example of some user preference for a relatively closed-walled-garden model.

Facebook in January 2013 enforced its ban on exporting data for use in social networks, by blocking Russian search engine Yandex’s new social search mobile app API calls within three hours of launch. It also cut off two apps from ‘Find Friends’ (Facebook’s API): Twitter’s photo app Vine and messaging app Voxer. This sounds remarkably like many recent reports of blocking of APIs and content by telecoms companies in breach of net neutrality law. As Constine (2013) argues, Facebook could find its actions backfiring for its platform supporters: “Facebook is playing with fire. It could use policy enforcement to cook competitors and shine a light on its dominance of social networking. But if this enforcement scares off developers whose apps might otherwise provide content that could be shown next to ads in the news feed and piped into Graph Search, Facebook could get burned badly.” We emphasise that it will be more badly burnt if – like Microsoft, Apple and Intel before it - it is found in abuse of a dominant position. It should be required to remedy its failure to follow our prosumer law principles, to permit interoperability rather than harming smaller competitors.

United States lobbyists constantly complain that the proposed new EU Data Protection Regulation will raise their costs of doing business. But separate the rhetoric from reality: it is the US federal and state authorities – and litigants in court - which have far more vigorously pursued Facebook, Google and others for their failures to guarantee users’ privacy. In November 2012, Google settled for $22.5million a case brought by the FTC in the case of tracking cookies for Safari browser users (US v. Google Inc. 2012, Devine 2012), on top of a 2011 $8.5million settlement for privacy breaches involving Google Buzz. In January 2013,
Facebook settled a class action with a $20 million payment into a compensation fund that—as with the Google Buzz settlement—will likely end up in privacy advocacy and education groups receiving a substantial part of the settlement (Fraley v. Facebook 2013, Marsden 2013). In 2012, both companies agreed to settle privacy complaints by agreeing to FTC privacy audit of their products for a twenty-year period (Brown and Marsden 2013: 134, 188). Sector-specific regulation of social networking already exists de facto in the United States, while Europeans wring their hands on the sidelines. The proposed new European Regulation, for instance, is unlikely to be implemented before 2016-17.

The final outcome of such an approach continues to be uncertain even as Facebook announced its intention to become an “entertainment hub” with news, video, and music embedded in the site from 2012. This is a similar approach to that adopted by AOL, the mobile Vodafone 360, and MySpace and has previously failed. MySpace, for instance, rewrote its code to prevent the embedding of YouTube videos in 2008, causing significant user unrest. The experience of Facebook as a destination site will prove an excellent case study as its strategy develops.

The profound implications of extensions of broadcast or other regulation onto SNS would create a very different regulatory space within which SNS operate. If one views innovation as perpetual and endemic to such networks, one may oppose such regulation on those grounds. If, however, the view is that social networking growth has plateaued with the constrained environment of Facebook now dominating, then the use of competition law on the Microsoft precedent, and its extension in EIF 2.0, may suggest that interoperability is forced on that dominant network.

It is important to note that the drive by government, most pronounced in the European Commission’s approach, toward more SNS regulation to conform to European legal norms as well as concerns for child protection and privacy, is conducted in an informal soft law manner (Senden 2005; Marsden 2011). Civic responsibility and the Internet is the leitmotif, from the graduated-response legislation that places enforcement in the hands of ISPs and co-regulation models for harmful but legal content that affects search, e-commerce, SNS, cloud services (Cowen 2013) and other intermediary providers.

**Conclusion: Towards Prosumer Law?**

Governments, users, and better functioning markets need a smarter “prosumer law” approach to Internet regulation. Prosumer law would be designed to enhance the competitive production of public goods, including innovation, public safety, and fundamental democratic rights. Prosumer law suggests a more directed intervention to prevent Facebook or Google or any other network from erecting a fence around its piece of the information commons: to ensure interoperability with open standards.

The European prosumer has already dealt significant creative destruction to many pre-Internet industries through such services as Linux, Skype, BitTorrent, and the VLC Media Player. It would be fitting for Europe to lead the United States in adapting Von Hippel’s ideas to the case studies that we have presented here. We do not have great confidence that the
United States will match rhetoric with reality in enforcing such an agenda, preferring talk of “Internet freedoms” and “bills of privacy rights” without actual regulations to achieve those outcomes. We are convinced that fudging with nudges (Yeung 2012) needs to be reinforced with the reality of regulation and co-regulation, in order to enable prosumers to maximize their potential on the broadband Internet.

Prosumerism should be a declared policy of the European Commission alongside the European interoperability framework (EIF). In fact, the Commission on 17 December 2012 launched its Code of European Union Online Rights for European citizens using the Internet (EC 2012). The UK government has made a giant rhetorical stride towards embracing interoperability in its open data purchasing principles of November 2012, a surprisingly strong statement of belief in interoperability as sound economics as well as normative policy (Cabinet Office 2012) - although this will not be trivial to put into practice (Moody 2013).

European electronic commerce consumer law is a marked departure from consumer protection in European contract law. It would therefore not be difficult to extend the European interoperability framework and legal protection for prosumers in this direction in law, though implementation requires all member states to commit to such a step in practice as well as theory.

Strengthened data protection rules and a “right to be forgotten” are an important step towards prosumer law. But interoperability is needed as well as data portability, to permit exit to more prosumer-friendly products than Google and Facebook, should prosumers wish to switch. It requires a combination of interconnection and interoperability more than transparency and the theoretical possibility to move data. Only then will information markets become more competitive, and prosumers have the luxury of real choice between very different standards offered by their hosts.
References


Cabinet Office, Government bodies must comply with Open Standards Principles, 1 Nov. 2012.


European Commission, IP/11/402. 2011a. Digital Agenda/Trade: EU and US agree trade-related information and communication technology principles to be promoted world-wide date


Federal Trade Commission, Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search, 1 Mar. 2013.

Fraley v. Facebook, Case No. CV-11-01726 RS.


International Telecommunications Union. 2010. FG-FN Output Document 77. Focus Group on Future Networks. 8th FG-FN meeting, November 28–December 3

IP/07/139. 2007. Mobile operators agree on how to safeguard children using mobile phones.

IP/08/22 Brussels, 9th January 2008 Antitrust: European Commission welcomes Apple’s announcement to equalise prices for music downloads from iTunes in Europe

IP/10/1175 Brussels, 25 September 2010 Antitrust: Statement on Apple's iPhone policy changes

IP/10/1624 Brussels, 30 November 2010 Antitrust: Commission probes allegations of antitrust violations by Google


Ohm, Paul, and James Grimmelmann. 2010. Dr. Generative or: How I learned to stop worrying and love the iPhone. Maryland Law Review 69:910–953


Sola Pool –see de Sola Pool


Treaty of Rome: establishing the European Economic Community (EEC) 25.3.1957 entry into force 1.1.1958


Williams, Martyn, and Angela Gunn. 2007. EMI to ditch DRM, offer improved sound on iTunes. Computerworld, April 2. http://www.computerworld.com/s/article/9015282/EMI_to_ditch_DRM_offer_improved_sound_on_iTunes


