9 Holistic Regulation of the Interoperable Internet

In the opening chapters, we described the multistakeholder environment for Internet governance and regulation, in which user groups lobbied along with business and governments. We also described the insights of new institutionalism, with exit and competition for standards becoming increasingly critical in the information economy. In chapter 2, we went on to describe interoperability as a means of lowering entry barriers and increasing consumer welfare. We also described how highly computer literate prosumers could encrypt and otherwise creatively secure an Internet experience with more freedom in both expression and access to information goods and how control technologies were deployed to limit some of this freedom. We explained that this freedom was for at-the-margin tech geeks, not the billion-plus Facebook and Google users. We described the perils of stranded citizens with little market attractiveness: those who are digitally illiterate, follow default settings slavishly, do not understand privacy policies, let alone click-wrap software licenses, and are unable to exit the environments in which they find themselves.

In this conclusion, we explain what more is needed to square the circle of Internet regulation in the broader public interest for all Internet users, not the fortunate few or the even more fortunate and fewer dominant corporations. We argue for “prosumer law” and give an example of our proposed solution to the problems of dominant social networking services. We then examine the international governance of information, especially the apparent incompatibility of human rights and trade-related concerns exposed in such multistakeholder fora as the OECD. Finally, we argue for holistic regulation of the Internet, taking a transdisciplinary perspective to solve those hard cases we have examined.

Prosumer Boycotts and the Silk Thread of Consumer Law

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, unchecked, unmourned, useless to advertisers, and antithetical to positive network effects that alone can feed a successful business.

Let us then speak of prosumer law (Fernandez-Barrera 2011). 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 Hendersen 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. Instead, we have portrayed 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 prosumption, or continue their silken personal data capture is a key question for prosumer law.

What should such 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 interoperate 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 nonneutral 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 behavioral 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 undiscoverable 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 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 favor 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.

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 coregulation, in order to enable prosumers to maximize their potential on the broadband Internet.

Hard-Wiring Interoperability into Standards?

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 (as discussed in chapter 2), 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.

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 CONNECT 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 colorfully 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 reestablish 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 favor 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 (Yeung 2012; Palfrey and Gasser 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.

Interoperability and SNS

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/TimeWarner 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.

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 coregulation models for harmful but legal content that affects search, e-commerce, SNS, and other intermediary providers.

"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's (2008) and Boyle's (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 that the tendency toward government captured by regulated monopoly may not be the whole story.

Internet Governance Principles: Human Rights, Free Trade, or Both?

Regulators are used to acting at national scale, but effective Internet regulation requires much stronger coordination at regional and international levels. Online service providers are easier to regulate locally because they require infrastructure (Web hosting) and capital and revenues to develop (code) and operate (mainly bandwidth costs, especially with video). There are very few noncommercial cloud services; many are free to users but funded by advertising. Providers could operate outside a jurisdiction, but regulators have a nuclear option of local ISP-based blocking (e.g., Turkey commonly uses blocking against YouTube), where out-of-jurisdiction providers will not apply restrictions to local users, or more subtle options such as banning payment processing (online gambling) or purchasing of advertising space from noncompliant companies. Most of the encryption tools in use are session based (SSL/TLS) between a user and service provider, so the unencrypted data can be accessed at the provider end (Facebook messages or BlackBerry messages either at Research in Motion or corporate servers).

In standard setting, geography can still matter. Information giants can safely ignore nation-states with only a few million customers, whose national regulators impose restrictions unacceptable to those businesses. This need to build international consensus, combined with regulatory limits of technology (e.g., digital rights management), may mean that states have to compromise on some of their key policy goals (limits on hate speech, protection of scarcity-based copyright business models) and build stronger models for operational cooperation (faster takedown of child abuse images, spammers, phishing Web sites, and payment processors).

It will be critical to involve the emerging powers of the coming century (Brazil, Russia, India, China, South Africa); otherwise attempts at global cooperation will be critically undermined. However, involving more authoritarian states in negotiations can significantly harm the protection of fundamental rights and freedoms. This raises a forum-shopping conundrum: Is the Internet Governance Forum (International Telecommunication Union 2005), G20, OECD, or another body the global Internet regulation coordinator of choice? The OECD at least requires members to have market economies run by democratic institutions, but it is not a human-rights-based institution. U.S. attempts to introduce freedom of expression into the World Trade Organization (WTO) as a free trade issue may look promising, but the fate of environmental and labor standards at the WTO presages the likely outcome (Drahos and Braithwaite 2002).

The local regulatory trend has been to co-opt ISPs as enforcers—passing on infringement warnings to users, blocking access to banned sites (Cleanfeed, Newzbin), and disconnecting accused copyright infringers (HADOPI). Without extreme care, such measures will drive up the cost of Internet access, damage freedom of expression and privacy, and retard innovation. Even worse, they are unlikely to have any significant impact on the illegal distribution of child abuse images or copyrighted work. Policymakers would be well advised instead to stick with the "mere conduit" compromise reached in the U.S. Digital Millennium Copyright Act and the Electronic Commerce Directive, whereby ISPs are not liable for the data they transport—the Internet equivalent of the common carriage protections that have worked well for centuries in other network industries such as transport and telephony (Cherry 2008).

To illustrate some of the difficulties in analyzing the Internet from both a rights- and economics-based perspective, consider the OECD high-level conference of June 2011, a follow-up to its previous Internet regulation meetings in Seoul in 2008 and Ottawa in 1998. The previous meetings were dominated by electronic commerce discussions. The 2011 meeting ended with the chair's conclusions, a communiqué, and a proposal to move toward OECD guidelines (2011) for member states on Internet governance principles. The Internet Technical Advisory Committee agreed to the final text, as did the member states, the Business Industry Advisory Council, and the trade unions. The Civil Society Information Society Advisory Council (CSISAC) did not. The biggest public discussion was about intermediary liability: an excellent updated OECD report (2011c) was declassified and distributed at the conference. The word *coregulation* was not used at all in the conference, although it was the central mechanism that might have bridged some consensus and was extensively discussed in the report.

Reasonable people can disagree about as fundamental an issue as the role of ISPs and other intermediaries. CSISAC had flagged this concern in their informal part in the Seoul meeting three years earlier, asking OECD countries to "defend freedom of expression and, in this context, oppose mandated filtering, censorship and criminalisation of content that is protected under international freedom of expression standards."

The 2008 Seoul declaration that judicial due process should be followed was deleted from the 2011 communiqué. Formal opposition to ISPs as copyright police was consistent with this conviction. There were several CSISAC statements on their opposition to the communiqué, including CSISAC as a whole (CSISAC 2011), and from Knowledge Economy International, European Digital Rights initiative, Electronic Frontier Foundation, La Quadrature du Net, and others. They made clear their view of the Internet as an information commons to be kept open to innovation. Rashmi Rangnath of Public Knowledge and Milton Mueller both shared praise for the inclusiveness of OECD's process—if some concern over timing of deliberation—but regret that the proposed private censorship model for intermediaries was proposed without due process and legitimacy, including judicial process (Marsden 2011).

So many OECD speakers used different definitions of the words *freedom* and *openness* in connection with the Internet that moderator Kevin Werbach was moved to state that we are separated by a common language and to conclude that multistakeholderism is, like democracy, the "least worst system" to discuss Internet governance (Marsden 2011).

The view of governments appears to be that a form of coregulation will arrive, whether formally agreed with appropriate judicial appeal available to injured parties (as laid out in the 2008 Seoul conclusions) or as a murkier and less well regulated quicker-fix political compromise (or quid pro quo with copyright lobbyists and others). EU commissioner Neelie Kroes signaled a move toward a compact in the direction of civic responsibility, which suggests that there is now a direction of travel, if not yet a concerted push, for more ISP activity, even if she says "it is not about regulating the Internet" (Kroes 2011).

The context is also important: the communiqué was agreed by OECD members and also the Egyptian delegation on behalf of the new government. Misunderstandings of the proposed informal private censorship model by non-OECD members are very possible, to put it mildly. The United States said that the OECD and member states must do much more to explain to non-OECD members (such as Egypt and China) that the principles do not permit the types of censorship that civil society illustrated. It is exactly that liability principle and mission creep to which CSISAC so vociferously objects.

The OECD also hosted a 2011 workshop to discuss implementation of the updated OECD Guidelines for Multinational Enterprises (OECD 2011b). Cisco, Alcatel-Lucent, Vodafone, and other Internet multinationals would be well advised to take close note of point B1 in the guidelines: "Enterprises are encouraged to: Support, as appropriate to their circumstances, cooperative efforts in the appropriate fora to promote Internet Freedom through respect of freedom of expression, assembly and association online." The June OECD meeting also discussed the U.N. Human Rights Council (2011) endorsement of Ruggie's guidelines for multinational enterprises on human rights (Ruggie 2011). Point 12 established an annual forum on business and human rights, one of whose responsibilities is to examine the operation of human rights in specific sectors, likely to include communications.

Interoperability is of course linked to open data, open code, and, arguably though technologically deterministically, free speech. However, the blizzard of Internet governance principles written in the course of 2011 have their origins in law and economics or human rights, but apparently do not translate one to the other. This apparent dialogue of the deaf is also a competition policy problem (Brown and Waelde 2005; Brown 2010) and a corporate governance problem, from multinational hydrocarbon companies (Shell, BP, and others) to multimedia combines (News Corporation) (Leader 2005).

The translatability or comprehensibility of human rights language to economic law is needed more than in previous eras when the arena of international trade and competition was kept largely separate from human rights. However, the pressing need to create a dialogue between experts in the previously discrete fields is an urgent task, notably because information communication technology (ICT) brings together a fundamental growth driver and transformative technology for the global economy with its equally fundamental and transformative role in driving human communication and dialogue.

To bridge the gap between free trade and human rights standards in Internet governance, a start can be made by comparing rhetorical aims in table 9.1. We can compare the bilateral attempt by the EU and the United States to extend the WTO's Information Technology Agreement to broaden both scale and scope and eliminate nontariff barriers, which the EU has previously pushed for (IP/11/402), with the ten principles of the multistakeholder Internet Rights and Principles Coalition, which establishes at least some overlap, albeit one is written in the legal language of "trade liberalization-ese" and the other in "human rights-ese."

We have shown through our case studies that governments and companies are still not showing due regard for the rights of users, and long-overdue reform of copyright law and notice and takedown regimes in this direction is not imminent. The failure of the European institutions to reform the Electronic Commerce Directive to at least match the U.S. Digital Millennium Copyright Act in ensuring some measure of investigation and "put back" is one example. By contrast, human rights advocates have increasingly found support in the wake of the Arab Spring's demonstration of the potential of the Internet for democratic expression, and both the United Nations and regional human rights bodies have called on governments to pay more heed to private censorship and not to permit or encourage such informal censorship to take place.

In the late nineteenth and early twentieth centuries, the FTC responded to industrial trusts based on continental U.S. markets, which were replacing trade guilds at regional and local levels (Wu 2010). Internet-based informational markets are network markets of a global scale for which the WTO and World Intellectual Property Organization (WIPO) are inadequately resourced and lacking in political legitimacy (Cherry 2008). The U.S. trade representative and the European Commission's political task

Table 9.1
EU and U.S. principles versus Internet Rights and Principles Coalition

EU and U.S. Principles of ICT Trade with Third Parties	P	Internet Rights and Principles Coalition
Transparency of rules affecting trade in ICT and ICT services	1	Universality and equality: All humans are born free and equal in dignity and rights, which must be respected, protected, and fulfilled in the online environment.
Open networks for consumers to access and distribute information, applications, and services of their choice	2	Rights and social justice: The Internet is a space for the promotion, protection, and fulfillment of human rights and the advancement of social justice. Everyone has the duty to respect the human rights of all others in the online environment.
Cross-border flows of information	3	Accessibility: Everyone has an equal right to access and use a secure and open Internet.
No requirement to use local infrastructure for ICT services	4	Expression and association: Everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural, or other purposes.
Governments should allow full foreign participation in their ICT services sector, through establishment or other means	5	Privacy and data protection: Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal, and disclosure.
Efficient and maximized use of radio spectrum	6	Life, liberty, and security: The rights to life, liberty, and security must be respected, protected, and fulfilled online. These rights must not be infringed on or used to infringe other rights in the online environment.
Independence of regulatory authorities overseeing ICT services	7	Diversity: Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression.
Simple authorization of competitive telecommunications services	8	Network equality: Everyone shall have universal and open access to the Internet's content, free from discriminatory prioritization, filtering, or traffic control on commercial, political, or other grounds.

Table 9.1
(continued)

ICT service suppliers must have the right to interconnect with other service providers for access to publicly available telecommunications networks and services: cost-oriented, nondiscriminatory, and transparent rates	9	Standards and regulation: The Internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion, and equal opportunity for all.
International cooperation with a view to increasing the level of digital literacy in third countries and reducing the digital divide	10	Governance: Human rights and social justice must form the legal and normative foundations on which the Internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation, and accountability.

arguably makes them too partisan to tackle these grand challenges with legitimacy, and the International Telecommunication Union has so far been largely irrelevant.

What can achieve the aim of the production of public goods through the appropriate level of regulation of these markets? Progressive coalitions within intergovernmental organizations (e.g., Brazil and Chile within WIPO) can sometimes have an effect, but are strongly resisted by the G8 and are sidestepped through forum shifting (e.g., the Agreement on Trade Related Aspects of Intellectual Property Rights [TRIPS] within WTO and the Anti-Counterfeiting Trade Agreement). The enlarged economic policymaking community since 2009 in the G20 brings in a progressive coalition with India, Brazil, and others. But the Internet Governance Forum illustrates the limitations, as does the environmental movement (Drake and Wilson 2008; Mueller 2010).

A global Internet bill of rights should also form a baseline for analysis, and here the United Nations as well as the Council of Europe and others can play a role (Akdeniz 2011; Kleinwächter 2011; La Rue 2011). Nations could impose requirements of transparency and open participation on standards bodies through procurement power related to the produced standards. They can also use funding power and direct subsidy of standards bodies (e.g., European Telecommunications Standard Institute), suggested, if not yet convincingly implemented, in the EIF.

The sunk costs and network effects of the broadband Internet have grown stronger as information distribution has become more critical to more applications, such as voice and video calling, real-time interactive gaming, and video streaming. To maintain the Internet's openness, dominant actors need to be restricted in blocking rival content that threatens their commercial interests. As the fixed and mobile ISPs gain horizontal and vertical bottlenecks over distribution, those rules need to be more vigorously pursued to maintain some continued openness to innovation.

This modest junction between economics and human rights is only a start in reconciling the fundamental and often compatible goals that they target, especially given the public goods created by information networks (investigated by Stigler, 1999). That makes it especially important that censorship is kept to a democratic minimum and that anonymity and freedom of speech more generally are preserved. As John Stuart Mill observed in his great work "On Liberty" (1869), the majority has no more the right to silence a minority, even if that is only one individual, than that individual has the right to silence the majority.

Human rights and free markets have much to gain from the Internet's continued efficient functioning. First, it is evident that transparency and enhanced information flow at decreased cost are benefits to both economics—laboring under the weight of imperfect information as pointed out by Hayek, Arrow, and others—and human rights. The U.N. Broadband Commission for Digital Development (Gilhooly et al. 2011; Budde et al. 2011) noted that the Millennium Development Goals for 2015 depend on the Internet for both their achievement and the monitoring of their progress. Moreover, transparency is a market-based remedy that can reduce information privacy and user autonomy problems in, for instance, social networks and data protection more generally, alongside network neutrality and some measure of renewed copyright bargain between users and distributors, artists and authors. In connection with copyright and network neutrality, we note the particular importance of evidence-based policymaking rather than the extensive and even pervasive industry capture of the regulator that has characterized Internet policy to date.

Toward Holistic Examination of Internet Regulation

Hard-wiring interoperability is a radical enough option, but it goes only partway to achieving our aims in this study. An Internet open to innovation and denying dominant actors the means to reinforce their position through unfair means is a good start to ensuring choice for users. However, it neither ensures their fundamental rights nor the means to raise those fundamental issues at the design stage of new standards. We must therefore address some specific issues:

- How to introduce greater transparency and dialogue between consumer groups and other civil society stakeholders and standards experts
- How to ensure that the benefits of rapid standards making are maintained even with the additional scrutiny suggested in increasing multistakeholder arrangements

Our conclusions lead us to add our voices to those proposing multidisciplinary examination of code and law, incorporating sociolegal studies, economics and game theory, and interdisciplinary information studies drawing on socioeconomic and political analysis (Clark et al. 2005; Marsden et al. 2006). The investigation of governance and standard setting needs increasingly to draw on these interdisciplinary approaches. This is an ambitious long-term challenge, and we acknowledge that the pathway toward more holistic approaches is littered with obstacles. It includes process and the design of multidisciplinary methodologies for new protocols and standards. We argue that these decisions need engineers to consider human rights for both code and law.

There should be no appeal to technological determinism (Dommering 2006) in our calls for more holistic design of code, neither creating an inviolate sacred principle as with the end-to-end principle when the actual principle is a design fix, nor a theological dictate, nor a nihilistic (and self-serving commercial) claim such as “privacy is dead.”

In consequence, the methodologies and techniques developed by regulatory communities should be structurally consistent with the new interdisciplinary scientific perspective called for by Clark et al. (2002). An integrated approach has not yet developed; the disciplines remain somewhat stove-piped in different silos. What is missing is bringing together these many solutions and approaches into a holistic and coherent scientific framework and associated evaluative and design methodologies. We can examine the effects of code on law via "Wiki government" (Noveck 2009), and WikiLeaks (Benkler 2011a), where the power of code to create a more open system of governance was at least promised. This holistic approach can be used to understand Internet development and to harness the creatively destructive force of the tussles of Internet development to stimulate the productive consequences of the Internet, improve its resilience and robustness, and use the combined technological and human systems of the extended Internet to address wider objectives in a holistic manner.

Developing a multidisciplinary catalogue of methodologies can improve comprehension of challenges to better participative decision making, including consideration of code governance approaches, such as the efforts to establish open source standards for hardware as well as software. The objective is not only to present and understand the various methodologies, but also to clarify their standing and the specific policy needs they address, and better understand the growing legitimacy problems and their potential solution or bypass. This may lead to the definition of a regulatory governance taxonomy under which the various methodologies can be classified and understood.

There is a need for the development of tools that help the wider multidisciplinary community to design legitimate holistic governance solutions. Development of these tools moves beyond traditional "dialogue of the deaf" interaction between nation-states, civil society, and expert standards bodies—including the Internet Engineering Task Force (IETF), ETSI, World Wide Web Consortium (W3C), and ITU-T — toward a better understanding of the needs and requirements for future Internet design based on broad sociopolitical buy-in (or at least better informed acquiescence) in the design process and outcomes. These are very difficult questions, not least because of the dynamic coalition forming and dissolving that takes place, as well as the opacity of links in the information ecology. Much pioneering work has been done in matching the challenges of Internet regulation to complexity theory by, for instance, Longstaff (2003), Cherry (2008), and Schneider and Bauer (2007), which promises to make these research questions easier to answer.

There is also an urgent academic mission to better explain Internet technology to legislators and regulators—to help prevent more "spoonfeeding of disinformation" to politicians by lobbyists. (Examples include copyright policy, data protection, and network neutrality.) The U.K. Hargreaves (2011a) copyright report may be a start in that direction, as is open government data standards policy (Marsden and Cave 2006), but examples of bad-faith lobbying have far outweighed good-faith impartial expert advice in the case studies.

In order to measure the success of governance design for future Internet standards, a living catalogue of standards bodies and their functions should encompass both telecoms and Internet standards but also the complex interplays and trade-offs between the various institutions and their design choices relating to software and hardware, privacy, security, and extensibility. Thus, an immediate contrast is evident between the IETF, ETSI and W3C models, for example.

The stakeholders who are influenced by standards setting go beyond those who necessarily actively participate in formal standards-setting activities. Who are the unrepresented stakeholders, such as the army of prosumers, in governance processes, and how can their interests be better represented? What impacts do approaches such as open source have on governance processes? Policy research needs to identify potential new participants in standards making and success and failure factors of differing governance approaches, including alternative or similar examples (Morris and Wong 2009). This would build on the well-known U.S. examples of Creative Commons, the Electronic Frontier Foundation, Free Software Foundation, Center for Democracy and Technology, and Free Press, and consider how such civil society groups could be better represented in the European standards sphere.

Governance policies involve a variety of actors operating at different layers, from physical infrastructure to content and behavior, including protocols and standards definition, as well as services and applications. Cross-mapping governance methodologies and policies can be carried out by crossing them with, on the one hand, the categories of human and nonhuman actors defining and executing them and, on the other hand, the layer at which they operate. Each element of the resulting three-dimensional matrix can then be analyzed and assessed with respect to its compliance (or lack thereof) with democratic values, such as transparency, legitimacy, accountability, and fundamental rights. The case studies we have presented demonstrate the approach.

We argue that transdisciplinary research following the type of methodology we have outlined can make a better effort at solving the following agendas:

- Assessing the impact of different market structures and their dynamics
- Developing the pioneering international political economy work of the 1970s for the Internet, compared to energy, transport, health care, and pharmaceutical sectors that Drahos and Braithwaite (2002) began
- Predicting how new minnows and gorillas (e.g., Facebook) are likely to affect regulation such as the Data Protection Directive and its 2009 revision, to be implemented in 2015–2016
- Helping governments in effective impact assessments for policy and legislation in the ICT field.

The answer to these research grand challenges is essential not only to the future study of regulation of the Internet but also to good policymaking under the U.S. and European requirements for impact assessment and better regulation. It is therefore critical to all future regulation of code.