# 8 Comparative Case Study Analysis

In this book, we have examined five hard cases of code-based systems in which self-regulation has had limited effect in producing key public goods:

*Privacy and data protection* A reliance on firms' disclosure of privacy-related behavior and consumer education has done little to protect privacy. More interventionist EU data protection rules for controllers of personal data have had a significant global impact, but this regime is now being supplemented by code rules for radio frequency identifier (RFID) tags and behaviorally targeted advertising in an attempt to improve the efficacy of privacy protection.

*Copyrights and the incentivization of creativity* In contrast, rights holders since the 1990s have encouraged governments to provide statutory code regulation protecting technical protection measures and, more recently, imposing graduated response and Web blocking powers against infringers. This case illustrates the dangers of blunt code regulation imposed following government capture by concentrated industries, which has seen a distortion of the aims of copyright law, the sweeping aside of delicate social balances protecting disadvantaged groups, and forum shifting from the World Intellectual Property Organization (WIPO), to the World Trade Organization (WTO), to the Anti-Counterfeiting Trade Agreement (ACTA).

*Censors and freedom of expression* Blocking and labeling systems have been introduced mainly through pressure from governments for ISP self-regulation, often without an adequate representation of civil society groups that could promote freedom of expression. Repressive regimes have encouraged self-censorship through the use of intensive surveillance of online forums.

*Social networks and user-generated content* These newer domains of online interaction have seen a regulatory focus on privacy and child safety, with protections based on user consent to terms of service and minimal, crowd-sourced regulatory signals.

*Smart pipes* There has been some regulatory support for network neutrality, which combines elements of universal service and common carriage to support application-layer innovation and freedom of expression. Architecting a low barrier-to-entry Internet that supports fundamental rights is a key concluding policy challenge.

Our aim throughout this book has been to identify the regulatory and governance mechanisms that have enabled the production of public goods such as security and freedom of expression, while enabling the continued rapid development of the Internet, and to understand how these processes can be protected as the Internet becomes a multilingual mass market artifact. We have taken a holistic approach to capture the roles of technology and services, business models, market structure and conduct, and governance (regulation, self-, and coregulation, standards, and other nonstate forms of control).

Understanding governance contributes to a better understanding of success and failure of Internet systems more generally. Activities at one layer of the protocol stack—and one disciplinary approach—may be driven by and affect those at others. Failure may be gaps, duplication, conflict as well as solution at the wrong level, poor function, inappropriate adoption, distorted development, or poor integration between different platforms or protocols.

The critical risks of a failure to develop governance more effectively arise from two directions:

- From the technical design community, a sensitivity failure to account for user adoption practice in creating better feedback loops can lead to system design that results in suboptimal adoption. Examples might be lack of privacy by design, misalignment of user practices and design solutions, or adoption rates below optimal (especially where universality is a desired and otherwise achievable policy option).
- From the social scientific, economics, and legal community (and government policymakers whose advice is largely drawn from their ranks), a failure to create better dialogue with the engineers in the Internet com-

munity can result in a governance failure in which user groups perceive critical governance flaws in standards creation. The result of this could be ill-conceived legal mechanisms designed to control rather than develop the future Internet, or a widespread reimposition of national borders and state censorship rather than enhancing human rights and a vibrant public sphere.

More fundamental questions need to be asked about the space for regulation of code, accepting both its importance as a regulatory tool and the overarching legitimacy and efficacy concerns that it poses. Zittrain (2006, 2008) and Ohm and Grimmelman (2010) have written about the key impact on Internet innovation of the technology's open or "generative" quality, with high reconfigurability enabling user-led innovation (Von Hippel 1976) and rapid market entry thanks to high levels of standards use and interoperability and few chokepoints or gatekeepers. However, we have seen through the case studies in this book that governments' attempts to intervene after proof of dominance has been shown is invariably a second-best compromise between a desire to avoid overly hasty regulation and a failure to realize the effect of technology on neighboring policy areas.

For instance, in the two decades since the Web browser first included cookies that are left on user computers, the European authorities have failed to persuade American companies to introduce meaningful prior consent for their users. The attempt to solve the network neutrality problem through competition law and consideration of abuse by dominant actors appears bizarre in the face of the herculean technical standards efforts since 2000 to achieve a "cash register on the Internet and charge for it" (Waclawsky 2005), which has made ISP actors unsurprisingly resistant to any regulatory nudges away from this emerging business model.

## Cross-Sectional Comparison of Case Studies

Our case studies demonstrate what is by now obvious: code and law are interdependent, and law cannot control code without unforeseen consequences. Law must therefore comprehend its effects on code, and vice versa: programmers need to understand the limits of law and its potential to affect their architectures. Smarter regulation provides nudges and tweaks to coders, users, and companies, as well as using market incentives, standards, and government procurement policies.

We asked in each case study how different levers work at different layers. In legal terms, that means examining the extent of vertical integration and bottlenecks. However, as we are dealing with human rights such as free expression, that also means compatibility with those fundamental rights—and how civil society can push governments toward regimes that have a better outcome for them.

We asked in each case if stakeholder input to policy has been meaningful or a Potemkin village square to which neither corporate nor government actors pay real attention (Marsden 2011). Our conclusions are in table 8.1. Note that *sledgehammer* refers to the use of that particular tool to crack a nut, an explicit and disproportionate use of force.

Our top-level concern, shown in table 8.2, is public policy response to code and institutional dynamics. In the absence of market failure, without detrimental social impact, there would be no need for regulation at all.

An overarching social impact of the Internet and related technologies has been to make the diffusion of information—whether personal data, copyrighted works, or banned materials—much more difficult to control. Regulation that depends on such control is therefore challenged, which gives rise to many of the problems we consider in the case studies.

Despite the speed of development of these markets, they all display significant monopolistic tendencies driven by network effects, even where corporate sunk cost is not an overwhelming factor—for example, social networking sites (SNS), in which user time is the most significant investment. The user is a prisoner of her own making. At the same time, ex post competition policy, postulated as the most economically efficient response to monopoly concerns, has been shown to be very defective in its speed of response to rapid market entrenchment (e.g., in the Microsoft browser case).

In several of our case studies, there were no agencies with responsibility for fundamental rights concerns such as censorship and freedom of expression. These concerns were left largely or entirely to markets, and regulators focused on economic impacts. Only in the most egregious cases (such as the U.S. Communications Decency Act, or European Commission proposals for mandatory ISP blocking) did courts or legislatures intervene.

In other case studies, existing regulators have been extremely slow to understand the implications of new technology and markets and to ensure effective protection of individual rights. This oversight on the part of poli-

**Table 8.1**
Best and sledgehammer practices

| Example | Reflexive best practice | Sledgehammer |
|---|---|---|
| Encryption | Incentives for adoption of Secure Socket Layer/Transport Layer Security (SSL/TLS) to protect e-commerce, stop WiFi hacking | Clipper chip; crypto software export controls; key escrow (government attempts to require individuals to deposit or otherwise reveal encryption passwords) |
| Data protection | Privacy by design: Schleswig-Holstein public procurement rules favoring EuroPrise-certified software<br>Privacy impact assessment (of legislation, government regulation, private companies) | U.S.-EU negotiated safe harbor for data protection—market entry condition—but mollified by weak enforcement |
| Copyrights | New business and legal models needed | Napster, KaZaA cases<br>DRM and anticircumvention laws<br>“Three strikes”<br>DNS rerouting/blocking<br>ACTA |
| Censors | Pre-CAIC Internet Watch Foundation<br>Banking industry response to phishing<br>Spam filtering and takedown | Golden Shield and Green Dam<br>Statutory Web blocking<br>*ACLU* v. *Reno*<br>Superinjunctions to reveal Twitter and Google users |
| Social networks | Coregulatory codes of practice<br>Enforcement action by Canadian federal privacy commissioner | Requiring real name registration, prelicensing and regulating bloggers; kill switches for social networking |
| Smart pipes | Instant messaging interoperability—AOL/TimeWarner merger<br>Essential facilities, fair reasonable and nondiscriminatory, and interoperability | Network neutrality—extreme positions on both sides<br>Google algorithm and mergers<br>IMS and DPI as used by Phorm |

**Table 8.2**
Public policy and market failure

| | Data Protection | Copyright | Censors | Social networking | Smart pipes |
|---|---|---|---|---|---|
| Social impact of technology | Bandwidth, storage, processing capacity all doubling every 12–24 months, making it much easier for organizations to process and share personal data.<br>E-government drives for personalization and savings; law enforcement and intelligence agency surveillance further impetus. | Perfect digital reproduction at almost zero marginal cost on user equipment has rendered copyright ineffective. Massive infringement over peer-to-peer nets, cyberlocker sites. | Ubiquitous use of broadband gives rise to call for parental controls.<br>Widespread use of blogs and other types of political expression cause state concern leading to censorship. Both have increased since 2000, with users split between those opposed to private censorship mediated by state, and others' apparent preference for walled-garden safety environment. | Mass diffusion of social networks creates need for child protection and exclusion from adult networks. Other critical concerns over privacy. | Use of monitoring of traffic still largely hidden from fixed end users, except some early adopters with peer-to-peer and gaming applications.<br>Mobile broadband and streaming video growth likely to increase user concerns. |
| Policy drivers: barriers to entry network and scale effects<br>Competition | EU promotion of single market in data flows<br>Personal data hoarding by information giants. | Incentivizing creativity. Grant of exclusive rights plus high returns to scale has created highly concentrated markets in music, film, software (latter with added network effects). | Censorship imposes entry costs through technology choice for blocking. DPI equipment for traffic monitoring a dual-use technology, also capable of surveillance and blocking. | Costs of providing safer environment nontrivial. Bebo decline relative to Facebook reveals tipping effect of dominant network. | Quality-of-service technology imposes nontrivial network costs that increase with scale, though deployment expertise offers scale economies.<br>Security dual use reduces costs. |

**Table 8.2**
(continued)

| | | | | | |
|---|---|---|---|---|---|
| Fundamental rights in policy design | European Convention on Human Rights and EU Charter of Fundamental Rights key policy drivers. | Rights to remuneration, moral rights in Universal Declaration of Human Rights and Berne Convention. | Appeal and due process almost entirely lacking. Overall frameworks subject to little democratic scrutiny. Few institutional champions of free speech ex ante. | Little effective government policy but significant private actor business model with little or no privacy. | Notable by their absence from early deployment; rights-based discussion growing with regulatory oversight. |
| Lessons | Privacy is a key human right that may need significant government intervention to protect. | Policy focus has largely been on protecting rights of creators at the expense of freedom of expression and privacy. | Privatization of censorship endemic (even in China coregulation is the claimed model). Greater regional and international transparency standards needed (La Rue 2011). Focus on content producers would have longer-term impact and greater sensitivity to freedom of expression. | Nudge toward self-regulation became audited public demand by EC in 2008–2009. Still apparent that regulation is the most likely result of failure to achieve adequate privacy standards. | Technology development without privacy or expression input can lead to spectacularly invasive systems. Telecoms regulators inadequate to discuss rights-based policies. |

cymakers has resulted in the subordination of user rights to both corporate and security interests, in privacy and data protection, network neutrality, social networks, and copyright. Remedying this failure to protect the fundamental rights of citizens is both an engineering and a broader regulatory challenge.

Regulation by code can increase the efficacy of regulation but should not be seen as a panacea. Copyright holders' hopes that "the answer to the machine is in the machine" led them to waste almost twenty years attempting to enforce scarcity-based business models rather than innovate toward the "celestial jukebox" that is finally emerging in products such as Spotify. Code is fundamentally a non-state-designed response that can lead to more effective solutions but will tend to undervalue the public interest and lack democratic legitimacy.

Nudges from regulators can encourage more legitimate private responses, but fundamental rights concerns often need stronger intervention, especially when business interests point firmly in the other direction or social benefits impose high private costs on corporate actors. Ideally it should be possible to design better code solutions that take into account the legitimate aspirations of users as citizens by incorporating social scientific and other nontechnical methodologies at the design stage. We return to this theme at the end of the chapter.

In table 8.3, the institutional political economy of Internet regulation shows a familiar dialogue between property right holders and governments, with multinational actors adding to their leverage through expertise and influence in technical standards bodies. There is a consequent legitimacy and transparency gap, and a struggle for civil society to raise any effective voice in the policy debates at an early enough stage to make meaningful design contributions in terms of due process in the deployment of technologies.

Effective, scalable state regulation often depends on the recruitment of intermediaries as enforcers (e.g., ISPs) in the few durable bottlenecks in the Internet value chain. The Internet has disintermediated many traditional points of control (e.g., consumer electronics manufacturers in the case of digital music reproduction equipment and publishers in the case of censors) and opened up further possibilities for individuals to interact without (yet) significant regulatory intervention (e.g., social networking sites). Such platforms can help users to act in their own interests—for example, by enabling

**Table 8.3**

Institutional political economy

| | Data Protection | Copyright | Censors | Social networking | Smart pipes |
|---|---|---|---|---|---|
| Key actors: national, regional, global | DP regulators; consumer protection agencies (e.g., Federal Trade Commission). Coordination in EU, APEC. Police, advertisers, tech industry. | Rights holder associations; United States, EU, Japan operating at national, EU, and international (WIPO, ACTA) level. Have forum shifted to avoid civil society (WIPO to WTO to ACTA). | ISPs, international intermediaries, multinational content companies, largely local user groups. Coders multinational (World Wide Web Consortium, Platform for Internet Content Selection). Child protection groups. | ISPs, intermediaries, multinational content, largely local user groups. Coders in Silicon Valley. Child protection groups. | Telecoms regulators; ISPs, intermediaries, content companies, largely local user groups. Coders in multinational corps. Surveillance-industrial complex re. DPI. |
| How legitimate and accountable? | Mainly legislative creatures, hence democratically accountable. Less so outside Europe with self-regulatory solutions. | Much policy laundering, forum shifting, exclusion of civil society, bullying of developing world, fantasies that "the answer to the machine is in the machine," not the business model. | Accountability requires transparency to users. Private action subject to little accountability (e.g., put-back provisions). Engineering ethics an undeveloped area. | User-generated regulation offers some control. Generally opaque terms and application means users vulnerable to private action without appeal. | Telecoms regulators accountable through parliaments; self-regulatory solutions unaccountable except via telecoms regulators (where applicable). |
| Multistakeholderism | Annual regulators' conference open to all stakeholders. RFID process explicitly multistakeholder, although industry tried hard to ignore civil society. | Civil society involvement at WIPO weakened anticircumvention measures in Internet treaties (see Drahos and Braithwaite 2002) but led to forum shift. Activists had to fight to involve legislators (United States, EU) in ACTA debates. | Little representation for free-speech nongovernmental organizations in censorship discussion, with corporate-government discussions largely private. Some discussion apparent (e.g., in hotline governance). | Little formal multistakeholder consultation by corporates. Restricted to publicity of most egregious privacy breaches and lobbying of government. | Organized opposition to corporate blocking of applications in United States, Netherlands, and France; less attention paid elsewhere. Some effect on European Parliament preelection 2009. |

**Table 8.3**
(continued)

| | Data Protection | Copyright | Censors | Social networking | Smart pipes |
|---|---|---|---|---|---|
| Key technical actor buy-in | Firefox (DNT), Apple Safari blocks third-party cookies by default (no ad network, unlike Microsoft and Google). RFID industry wrote privacy framework with some other stakeholder input; code approved by Article 29 Working Party. | Early technological protection measures produced by small software companies ineffective. Hardware (Trusted Computing Group, TCG) and operating system vendors now more involved, but still limited effectiveness. ISPs have fought against three-strikes and blocking, although in the interests of many as they raise entry barriers and reduce neutrality. | ISP-level filtering prevalent since emergence of large-scale spam e-mail problem in early 2000s, continued by British Telecoms technical initiative. Need for standards and best practices to ensure minimal collateral damage from blocking, particularly where technology sold to totalitarian regimes' ISPs. | Walled-garden Facebook approach meant third-party application developers dependent on Facebook ecosphere. More open environments supported; significant research effort in interoperable social media to prevent high-walled gardens. | Organized by corporate vendors (e.g., Alcatel-Lucent, Sandvine). Mobile industry at forefront of qualify-of-service (QoS) efforts. Technical community supportive of drive toward QoS and managed services. Technical opposition to QoS bans. Also lobbied for greater bandwidth solution with minimal QoS. |
| Lessons | Strong intervention from legislators and regulators is sometimes needed to counteract police and industry with interests in weaker regulation. | Code distracted attention from business innovation for more than a decade. Three-strikes has been pushed through with little multistakeholder involvement, resulting in policies widely criticized as contrary to freedom of expression. | Private censorship accompanied by government encouragement, sponsorship (e.g., hot lines). Democracies increasingly need political control of export of material conducive to repression. | User-generated regulation in social media proved largely mythical in face of commercial pressures to reduce privacy for third-party advertiser use. Civil society ineffective. | Highly technical issue meant little traction for policy initiatives to shape code except in egregious cases. Much of technical community active in control environment. |

the restriction of third-party code's access to personal data on social networking sites and smart phones—but may need regulatory encouragement to do so when it is not in the platform operator's own commercial interest.

Companies can be regulated much more easily than individuals because of their tangible nature: they are easily identifiable and have assets that can be seized to prevent further malfeasance and remedy existing wrongs. Governments have found ways to maintain this despite the increasing ease of offshoring through mechanisms such as regulation of payment intermediaries (gambling) and the arrest of corporate officers who pass through their jurisdiction (gambling again).

As the Internet shifts control to individuals, this makes regulation more difficult. Because actors are often offshore or enforcement is driven by the commercial interests of corporate stakeholders (or both), there is a technocratic focus on interests of companies rather than citizens or users—often seen as the problem or the product, for instance, in copyright or social networks or network neutrality. Unsurprisingly this results in a lack of legitimacy or accountability given the objectification of the citizen. This can be summarized in the term of abuse: "the freetard" (Marsden 2010). It would be akin to politicians treating the voter as the problem. It is a worrying expansion of the traditional methods of setting copyright policy and the dominance of the private property right over other fundamental interests, particularly given that communications policy is essential to participative democracy.

The often mythical quality of multistakeholderism is proven by the extraordinary lack of real consultation that has taken place, particularly over network neutrality and copyright, most consultation being ex post and somewhat ad hoc. We return to this in the examination of code below. Ex ante policy consultation often focused on corporate concerns, behind closed doors, rather than those of citizens, which tended to be rushed and after-the-fact types of discussion regarding implementation. The impression given is that multistakeholderism was a slogan and a last-minute concern rather than an integrated element in decision making, let alone civil society an equal partner in trilateral discussion with government and industry.

Fundamental rights concerns remain, with governance of several case studies predetermining:

- Lack of concern, experience, and skills and lack of remit or enthusiasm to deal with fundamental user rights such as with copyright (economic concerns within departments of commerce and business, trade negotiators: Drahos and Braithwaite 2002)
- Censors (security concerns within interior ministries and their executive agencies and effective child protection group lobbying not matched by free speech advocates)
- Network neutrality (e.g., the technocratic and competition-oriented, narrowly defined statutory remit of a telecoms regulator)

Commercial interests dominate technical actors in policy debates, which has resulted in investment in control by dominant operators in bottlenecks rather than innovation by start-ups—again, particularly in copyright and network neutrality. Proprietary code dominates open source, standards-based solutions are limited, and therefore interoperability and wider concerns over ensuring the fungibility of code are relegated to marginal issues compared to the immediate commercial imperatives of monopolistic actors. If we had examined search neutrality or personal Internet security, we would have found similar proprietary solutions adopted rather than a search for industry consensus.

The lack of standards-based solutions in our case studies so far is a reflection of the dynamism and technological innovation in the studies, but also in the lack of impetus by market actors or regulators to negotiate and implement common standards. The former element is a feature of the period of technological development we examine, whereas the latter is a deliberate policy choice. Therefore, we see nothing inevitable about this trend toward proprietary standards. We see an opportunity for reexamination of the regulatory options in these case studies as the overarching lesson. This neither proves nor disproves Zittrain's "tethered appliance" thesis (Zittrain 2008), but it does indicate that the room for regulatory action still exists and should be reconsidered.

Monopolistic industry structure often means that users have no effective choice, for instance, over using music restricted by digital rights management (DRM) before the iTunes move to unprotected formats, or network-neutral ISPs. Where there is oligopoly, there is less or no concern for end user acceptance or resistance. It should be good business, good design, and good regulatory compliance to road-test new services and products prior to their imposition on an unsuspecting public.

Table 8.4 shows that code control over the various policy areas is maintained through various layers of the protocol stack, not merely the application layer. This is obviously the case with smart pipes, where the code innovation is designed to reach deep into the protocol stack to engage in deeper inspection of the bit stream. It also influences privacy, not least because informed consent for smart pipe–type activities is not unambiguous. It also affects censors, as network-level filtering depends on inspection that may be deeper than the packet header. By contrast, copyright enforcement, in the period before ISPs were directly involved in the activity, depended on tracing the end user by presenting to the ISP the IP address downloading suspected of infringing on material, and code enforcement of DRM. This may change as HADOPI (Haute autorité pour la diffusion des oeuvres et la protection des droits sur internet) types of regimes emerge and ISPs are required to conduct more strenuous enforcement on behalf of copyright holders, though blocking Web sites (e.g., Newzbin or Blogger) is relatively trivial for ISPs already engaged in blocking of various forms of pornography. This was a key factor in the decision by the English High Court to grant an injunction requiring British Telcoms to use its Cleanfeed system to block access to the Newzbin site. At the same time, the EU Court of Justice has found in two key decisions (*Scarlet Extended SA* v. *SABAM* 2011; *SABAM* v. *Netlog* 2012) that a general obligation cannot be imposed on ISPs or Web sites that monitor their customers' activities for illegal behavior.

For ISP censors, the mode chosen can cause substantial unintended collateral damage. The emergence of standards for Cleanfeed-type blocking may mitigate some free speech concerns and prevent the blocking of Wikipedia as in the infamous 2009 U.K. episode, in which blocking of one image by industry-standard filtering technology caused all U.K.-based edits to Wikipedia to be blocked (McIntyre 2011, 2012). Overall it is clear that both the sophistication of controlling code and its reach down into the protocol stack are at a stage of evolution not previously seen in the public Internet. There is no inevitability about even more widespread adoption of code to control user behavior and a deeper infiltration into transport layer, but that does appear to be the direction of travel.

**Table 8.4**

Types of code and code regulation

| | Data protection | Copyright | Censors | Social networking | Smart pipes |
|---|---|---|---|---|---|
| Layer | New focus on RFIDs, browser code (do not track, cookies) and privacy by design | 1990s focus on technological protection measures has largely been failure. Now three-strikes, ISP blocks. | Application or network or both. Chinese ISPs use Golden Shield to filter at entry point to network (and nation), supported by filtering software in client PCs. Western nations typically at network (e.g., Cleanfeed) and filters at client level. | Application (including third-party applications and media partners); platform. | Varies but typically network or transport layer. |
| Location (manufacturers, ISPs, servers, clients) | Software and system architects. | Previously software and hardware vendors; now ISPs. | Clients for filters, manufacturers and ISPs for transport-level filters. | Server side with some mobile-based features. | Hardware and software vendors' DPI solutions; ISP traffic management solutions. |
| Enforcement of code | Threat of Data Protection Directive enforcement; revision of Data Protection Directive. | WIPO Internet treaties require anticircumvention measures. Digital Millennium Copyright Act and European Copyright Directive (EUCD) ban devices and circumvention. Haute autorité pour la diffusion des oeuvres et la protection des droits sur internet, Digital Economy Act (DEA), and infringement actions used to impose on ISPs. | National: Egyptian nihilist "plug pulling" but negation of code. Green Dam local filters; Golden Shield national solution. Heavy government pressure in the United States and EU for self-regulation by ISPs. | Terms of use—enhanced by contractual terms with third-party application providers and media partners. | Termination monopoly held by ISPs—nontransparent term of use for end user. Competition regulation. |

We can see within and between case studies evidence for the hypothesis that greater multistakeholder involvement will improve the quality of regulatory design, including the technical understanding of code. The RFID code of practice went through several iterations dictated by the original regulatory requirement of a more inclusive coregulatory practice. The first version was largely written by industry, but the result was flimsy, not least because of the exclusion of academic and civil society stakeholders and refusal to incorporate rights-based concerns. It was rejected by regulators. After strong pressure from other stakeholders, a much more comprehensive version was produced and approved by data protection (DP) regulators. A second example is technological protection measures (TPMs); the first generation was woefully ineffective because small start-up companies largely wrote the code. It took the involvement of large industry players such as Microsoft to produce regulatory technologies that were not trivially circumvented, but they nonetheless largely failed to have the desired impact. A third example is Cleanfeed, which is better targeted than previous IP and Domain Name System (DNS) blocking techniques and therefore appears to be less intrusive on freedom of expression as well as being relatively broadly accepted by the industry. A counterexample is the manner in which deep packet inspection (DPI) has been introduced on some ISP networks, where the lack of user consultation led to infamous incidents such as Comcast/Sandvine's BitTorrent seeding or BT/Phorm's secret DPI and behavioral advertising trials. (Phorm's system trials used deep packet inspection of the ISP customer's Web browsing, in order to insert ads relevant to that browsing behavior, without user permission being given.) These were poster children for the failure to consider multistakeholder discussion prior to design or even implementation of innovative control technologies.

The enforcement of product or service terms and conditions by code (including the statutory terms and conditions of copyright) is usually blunt. This quickly becomes problematic when it has an impact on fundamental rights, for example, when DRM stops blind users from accessing text materials using text-to-speech software. It is a significant problem in policy areas that are central to democratic rights and where legal enforcement is hedged with all sorts of conditions that are too subtle for implementation through code (e.g., copyright fair use or dealing). For example, offering users a binary choice of acceptance of new terms of service for a social network that their entire community uses, or rejection of new conditions leading to termination of account, is no choice at all. In a similar fashion, enforcing unilateral opaque and often subjective terms for use of an ISP's service does not contribute to a meaningful exchange of views with users over network neutrality. Even exiting a service when rejecting a change of code can be difficult or impossible for the user, as, for instance, in removing personal data from a social network or ISP (both of which retain data for extensive periods, either imposed by regulation such as data retention or reduced from infinity by the pleas of data protection regulators and politicians).

Table 8.5 compares the outcomes in each of our case studies. Transparency is a prerequisite for dispute resolution. It is notable in these cases that the opacity of the implied terms and business practices of service providers has created a perception of untargeted and capricious enforcement against users. Increased transparency must be a basic regulatory requirement in order to make markets operate more effectively as well as to provide at least a baseline for users to understand their rights. The calamitous consequences of the sanction of service denial for users who have invested many hundreds of hours in creating an online identity or integrating into an online community may often be disproportionate to the types of infringement of which users are accused. This makes transparency absolutely essential to any informed regulatory bargain between users and service providers. Sanctions and even accusations of breach of terms can be poorly targeted because of the difficulty in establishing the identity of the infringer with a shared resource such as an IP address. Appeals and due process, where they exist at all, have been ill defined and underdeveloped. This should make corporations especially sensitive to the effect of enforcement actions on a wrongly accused party.

The potential for user-generated regulation has not yet been fully explored. Companies have embraced it when it can provide them with a benefit, such as protection for liability for hosting copyright-infringing content. But it has so far been ignored when benefits would instead accrue to users. For example, a take-down button for third-party tagged, posted content that prevents distribution until agreement from the subject is sought would help protect users from the spread of embarrassing photos, but would be against the general interests of social networking in increasing the quantity of content available on their networks.

**Table 8.5**

Outcomes and divergences

| | Copyright | Privacy | Censors | Social media | Smart pipes |
|---|---|---|---|---|---|
| Transparency | Unclear causation from present system—Hargreaves (2011) analysis very useful (e.g., digital copyright exchange). More transparency to more just solutions? | Limited impact of opaque privacy policies and user education—often unintelligible to users, who often are in a poor position to judge privacy risks. | Block lists private—obscure reasons for removal—no generic reporting duty on ISPs. | Most important social networks deliberately obscure in software updates and privacy policy changes. Little evidence of good practice. | Refusal to create transparency a critical element in early U.S. cases. European extensive work on creating greater transparency through regulation. |
| Enforcement | Problem of the second user—individuals can be a network and succeeding infringements impossible to police (as well as fair use). Enforcement against corporations possible; legal business models and licenses effective enforcement in the sense of recompense. Three-strikes massively disproportionate. | Varied levels of enforcement by EU regulators suggest cultural factors also important.<br>Data breach requirements and code solutions could increase privacy protection more uniformly. | Put-back would help to make enforcement fairer. Private censorship removes user rights. General classes of content censored (e.g., Usenet). Blind alley as bad guys can always access. | Individual reuses of data not susceptible to corporate-type enforcement. Nudges and defaults more useful: “Distributed enforcement.” Policy on child protection moving toward offering greater user involvement in safety. | Network neutrality “lite” solutions to prevent protocol, application blocking so far limited to statute in Netherlands, and regulatory declarations (e.g., in Singapore, United States). Bandwidth or service plan capping resulted. |

**Table 8.5**
(continued)

| | Copyright | Privacy | Censors | Social media | Smart pipes |
|---|---|---|---|---|---|
| Interoperability | DRM closes off interoperability—iTunes prior to move to unrestricted MP3 format, for instance. Continued issue with e-book formats. | Broad European standards are driving a global race-to-the-top, with export controls and "adequacy" assessments driving interoperability between national regimes. | Cleanfeed better approach compared to DNS blocking collateral damage. Iran worst of all possible worlds: not even interconnection. | Open social—why can't all users move data and interconnect? Note portability is insufficient. | Vendor off-the-shelf solutions adapted to ISP—but little transparency on policy. |
| Efficiency | Levy one option for efficient enforcement? New business models are key. | Efficiency via internalized data controller self-enforcement? Norm enforced by law. | Answer should be to go to source: arresting producers, not blocking viewing. | Corporate governance conformity to best practices arguably best outcome. Has the Federal Trade Commission or European Commission achieved this through recent scrutiny? | Anything but telecoms trench warfare or entirely shutting off third-party innovation must beat either extreme. Coregulation suggested as best option. |

Given the problems we have identified with transparency and enforcement, the minimum that we might expect end users to be able to retaliate with is to take their business elsewhere. However, absent interoperability, it may well be that the user is locked into a service that may have treated him or her in an arbitrary or unfair fashion. Therefore, in order for any type of consumer sovereignty even to be broached, some minimum level of interoperability would be required in circumstances where there is no realistic prospect of users otherwise migrating to a different service provider. A classic example is the social network, which refuses to return all personal data and to delete all evidence of the user. Another is DRM "locks" that close off interoperability—users cannot move their music collections to another service or even sometimes hardware platform, leaving them vulnerable to the shutdown of services—as happened with music services from MSN, Walmart, and Yahoo! By contrast, cookies are an interoperable way of permitting users to opt out of services, even if this is somewhat of a false choice given the extraordinary preponderance of cookies across advertising-supported Web sites. Interoperability in the cases of censors and network neutrality is more an issue between service providers.

Efficiency conclusions lead us to consider the fork in the path that has not been taken. In each of our case studies, greater attention to user rights and interoperability would have led policy in a different direction, which would have been based on greater transparency and focus on due process where enforcement was found necessary. Thus, a greater emphasis on business model innovation would have avoided much of the copyright enforcement saga of the past decade, as would maintenance of the 1990s principle of end user filtering for censorship. Network neutrality may have remained a minority concern had greater transparency been agreed on and publicized at an early stage by the ISP industry. Social networks that respected end user privacy and prevented children's membership of adult environments may have not grown as quickly, but would have created an environment in which users had greater trust and confidence that their rights would be protected (much as trust in electronic commerce is seen as key to encouraging nonshoppers online to participate in the Internet economy more fully).

These different futures may be seen as utopian, but it is important that policymakers are reminded that an alternative future can be mapped out based on their policy choices, as well as market and social developments.

That suggests that keeping such choices open is an important element of the policy environment, which is why interoperability and transparency assume such important roles in our final chapter. It also suggests that the best way to avoid the need for heavy-handed regulatory intervention is to maintain—through interoperability and standards—the potential for innovation within the Internet environment, such that the conditions for alternative futures have not been made impossible due to deeply embedded monopolistic market structures and practices.