1 Mapping the Hard Cases

We described in the Introduction the problems and challenges of regulating the Internet, given the dynamism of markets and the even greater dynamism of code, whether closed or open.

The claim that regulation can serve both economic and social efficiency and human rights goals is hardly novel (Mill 1869; Teubner 1986; Brownsword 2005; Brownsword and Yeung 2008). But we argue that the growing societal importance of the Internet makes the policy challenge increasingly important and that we need to reject simple magic bullet solutions based on study of one discipline (whether computer science, law, or economics), one industry sector (telecommunications or free software), or one solution (self-regulation or government control). Examining the claim that solutions can combine such disparate tools (regulation and code) and aims (efficiency and human rights) is the aim of our case study examinations in this book.

In this chapter, we explain our methodology. First, we assess the standard analyses of Internet regulation. We then explain how regulation of this virtual environment is best approached by examining the protocol stack rather than geographical approaches and assessing regulatory intervention according to the code solution or solutions used. However, following Shannon (1948, 1949), we reject a technologically determinist view of code as an efficient stand-alone solution and examine the predominant justifications for various regulatory systems, classified as broadly supported by economic or rights-based regulation (Lessig 1999; Balleisen and Moss 2010).

In the following section, we explore a particularly promising recent approach, multistakeholder governance. Its importance for our analysis is that it introduces both user rights and technical solution advocates into the otherwise frequently closed government-corporate regulatory discussion. Whatever the practical flaws of the previously researched practices of multistakeholder Internet regulation, it is rapidly becoming an element in regulatory design (Drake and Wilson 2008; DeNardis 2009).

Finally, we briefly outline our case studies, as well as our approach to their analysis. The case studies cover both fundamental rights-based Internet fields (censorship, privacy, copyright) and information infrastructures that are attracting increasing regulatory attention (social networking sites and network neutrality).

Standard Approaches to Internet Regulation

There are three existing conflicting approaches to Internet regulation from a technical and legal policy perspective: continued technological and market-led self-regulation, reintroduction of state-led regulation, and multistakeholder coregulation.

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

The second explanation holds that from the legal policy perspective, governments need to reassert their sovereignty. It states that code and other types of self-regulation critically lack constitutional checks and balances for private citizens, including appeal against corporate action to prevent access or remove materials (Frydman and Rorive 2002; Goldsmith and Wu 2006). According to this explanation, government should at least reserve statutory powers to oversee self-regulation to ensure the effective application of due process and attention to fundamental rights in the measures taken by private actors.

However, it may also be argued that government regulation has serious legitimacy deficits, with as much government as market failure in Internet regulation to date, with overregulation evident in "censorship" (MacKinnon 2012). There has been widespread industry capture of regulators and legislators in, for instance, copyright law (Horten 2011). Incumbents lobby to protect and introduce new barriers to entry with regulatory or legislative approval, as in a perceived failure to enforce or approve network neutrality legislation (Marsden 2010). There has been continued exclusion of wider civil society from the formal policy discussion, where official views do not permit easy representation of new noncorporate technical or user rights lobbies (Mueller 2010).

The view that traditional regulation fails to embrace new multistakeholder discussion has partly been justified by states criticizing the extremely tenuous chain of accountability of participants within international fora to nongovernmental organization stakeholders. Former French president Sarkozy, host of the eG8 meeting in 2011, stated in relation to Internet governance (Poullet 2007) that “governments are the only legitimate representatives of the will of the people in our democracies. To forget this is to take the risk of democratic chaos and hence anarchy” (Howard 2011).

The civil society argument leads to the third multistakeholder coregulatory position: that formally inclusive multistakeholder coregulation—reintroducing both state and citizen—is the approach that has the best chance to reconcile market failures and constitutional legitimacy failures in self-regulation (Collins 2010; Marsden 2011).

Though intended to increase inclusiveness by representation beyond the government-business dialogue, there are significant questions as to the effectiveness, accountability, and legitimacy of civil society groups in representing the public interest. There is a body of work on Internet governance specifically addressing legitimacy gaps and development challenges in global institutions from an international political economy perspective (Mueller 2010; Drake and Wilson 2008).

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

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

We assess these counterpoints in chapters 3 through 7 in empirically grounded, multidisciplinary case studies of five difficult areas—what we refer to as *hard cases*. Previous legal work has tended to examine the Internet from a position reflecting the technology's unregulated origins (Post 2009), even in debunking the borderless "Wild West" mythology of the early libertarian paradigm (Lessig 2006; Goldsmith and Wu 2006; Zittrain 2008). They equally have tended to be U.S.-centric. This debate has been effectively ended in favor of realistic pragmatic viewpoints (Reidenberg 1993, 2005; Goldsmith and Wu 2006; Wu 2010).

Regulatory and political economy work has concentrated on single issues or themes, such as the domain name system or privacy issues. There has been significant analysis in individual issue areas, notably the Internet Corporation for Assigned Names and Numbers, or ICANN (Mueller 2002) and Internet standard setting (Camp and Vincent 2004). Holistic examinations have tended to be compendia, such as Marsden (2000), Thierer and Crews (2003), and Brown (2013), or examine the Internet from development or other political economy perspectives (Cowhey, Aronson, and Abelson, 2009).

Our approach takes a multidisciplinary perspective from both computer science and law, following Kahin and Abbate (1995), Berman and Weitzner (1995), and Lessig and Resnick (1998). We cover European as well as U.S. regulation and policy, and in the following section explain why a geographically specific attempt to regulate will largely fail to achieve optimal code and regulatory solutions.

Geographies of Internet Regulation

It is not feasible to map Internet regulation as a patchwork of national networks where international regulatory discussion centers on areas with overlapping jurisdictions or unclear jurisdiction. This comparison of Internet regulation with the Law of the Sea or medieval mercantile law (Lex Mercatoria as Lex Informatica: Reidenberg 1998) is untenable in practice; unlike maritime transactions, Internet transactions commonly take place in real time in multiple jurisdictions, potentially using the same computer software worldwide (Lessig 1999; Murray 2006). China or Iran may be able to maintain their own hermetically sealed intranets despite the economic and social losses associated with such self-imposed isolation (in which China and Iran both have an unfortunate historical inheritance), but interconnecting with the Internet will lead to contamination of that drastic solution. Longer-term Internet control by authoritarian regimes is likely to be more subtle (Morozov 2011).

That is not to say the Internet is unregulable or that such a status should be assumed. However, to state that any country can effectively create a wall (like a naval blockade) around its domestic Internet appears empirically to be an exaggeration (Clayton, Murdoch, and Watson 2006), as with the Law of Space.

A further difference with traditional trade in goods is in the nature of those “goods”: information goods are often media or speech products that carry an explicit political or ideological message. Even dramatic attempts at national disconnection by repressive regimes during national uprisings in Burma and Egypt failed to prevent information exchange with the wider world.

For over a decade, governments have been able to require crude filtering of content to users based on geography. The imposition of sanctions on U.S. Internet host Yahoo! by the French courts in 2001 could not block all French users from accessing content that was illegal in France but legal in the United States. It was intended to restrict the vast majority of ordinary nonexpert users who did not have the ability or incentive to disguise their location (Reidenberg 2004, 2005; Goldsmith and Wu 2006). Expert witnesses told the French court that users could be blocked with about 70 percent effectiveness, although one witness later retracted this opinion (Laurie 2000).

The idea that one can map Internet regulation based on the location of bits is therefore superficially attractive but essentially a technologically determined attempt to reintroduce physical jurisdictional boundaries (Bender 1998). Ultimately the Internet’s highly connected nature has enabled at least sophisticated users to route around censorship, protected by encryption, which we explore in more depth in the next chapter.

If Internet transactions cannot be regulated in the same way as physical goods transactions, a second suggestion is that they be mapped using their nearest physical analog: the geography of their routing through servers. The problem here is significant and can be stated simply: the Internet remains largely a "dumb" network that routes packets without examining their contents. This lies behind the so-called end-to-end nature of the Internet: "intelligence" lies in end nodes such as PCs and smart phones, not between these nodes in network routers (Saltzer, Clark, and Reed 1984; Clark and Blumenthal 2011).

Though attempts are being made to "see" inside the packets to check their compliance with the law (as we will see in the chapter 7), governments still cannot very effectively act as customs officials and stop, check, deport, or import packets (Burk 1999; Marsden 2010). Though this is a technological possibility in Internet design, it would create a significantly different environment where, for instance, the anonymity of senders was removed or at least heavily penalized (Deibert et al. 2008, 2010; Johnson et al. 2003).

Early analysts viewed technical and geographical challenges to existing regulatory functions (Johnson and Post 1996) as insurmountable obstacles to regulation. Later analysis demonstrated that there was much greater interdependence between the allegedly global and unregulable Internet and national rules (Thierer and Crews 2003; Marsden 2000).

The ability of the state to seize physical assets and interrogate evidence (such as data on servers) is at the center of national enforcement (Brown, Edwards, and Marsden 2009), as well as traditional state censorship. Our selection of hard cases is an attempt to investigate the gaps where full state regulation is unfeasible, unwieldy, or unnecessary. A strong working assumption of our research is that many such institutions will map not to geographical boundaries but to sectoral or technical realms (Bar et al. 2000; Barnes 2000).

National law does not create effective solutions to prevent code-based problems, but a better solution may be a combination of a pooling of sovereignty to create global standards in support of effective code and protection of users' rights. There has been a growing realization that the Internet presents a complex series of challenges to existing laws, but that a nuanced and interdependent (if complex) relationship has emerged between existing nationally based legal systems and a global (or at least multipolar) Internet architecture based on code.

The role of state sovereignty has been reintroduced by both the Internet's mass adoption and by government desires to reintroduce substantial monitoring and other functions to maintain state security. These were particularly driven by the September 11, 2001, terrorist attacks in the United States and subsequent attacks in Bali, Madrid, London, and elsewhere (Ball and Webster 2003), and the growing scourge of virus writers, spammers, fraudsters, child pornographers, and pedophiles using the Internet (Brown, Edwards, and Marsden 2006).

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

Regulating Through Code

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

(Berners-Lee and Fischetti 2000). Internet self-regulation emerges from that technical perspective.

Problems of both a regulatory and disciplinary nature remain. The lack of interaction between (most) engineers and (most) social scientists mean that the technology is often as unsuitable for wider societal goals as the law is unsuitable for many practical enforcement processes (de Sola Pool 1983).

A technical view of mapping begins with the classic open systems interconnect (OSI) "layers model," which was adapted to represent the stack of protocols that enable end-to-end signaling of communications traffic (Werbach 2002). There are cross-cutting issues that affect the stack as a whole, examples such as digital rights management (DRM) and security. Content and applications and their regulation sit atop the Internet's deeper architecture, which is typically represented by the "protocol stack."

We can illustrate the stack as an iceberg, with the content as the visible layer above the water and the technical layers submerged from sight for nonexpert users, as shown in figure 1.1:

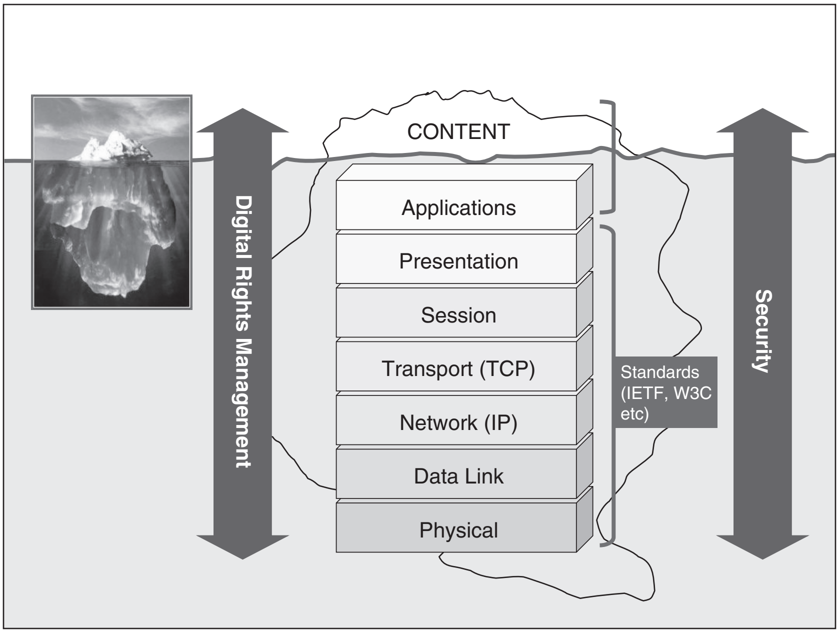

Figure 1.1
Graphically representing content sitting above the standards iceberg

There are rules written into the entirety of the protocol layers “iceberg” (Wright 2006) that affect users’ perspectives of how to receive and share content or how to ensure the security of their use and enjoyment of that content.

The technical infrastructure provides the underpinning of the content layer, and design choices in those layers underpinning content have a significant influence on the content itself (Reidenberg 2005; Lessig 1999). We selected case studies that have a significant material impact on the content layer, including those that may be located further from the end user’s visibility. For example, the relatively anonymous end-to-end nature of the Internet facilitates the transmission of unsolicited commercial e-mail (spam). Laws restricting this content cannot be effective for most consumers without also enlisting the support and deployment of services deployed outside the user’s own computer (Clark 2005; Brown, Edwards, and Marsden 2006) through some level of classification and filtering at other points in the network.

The hard case studies that we analyze in later chapters demonstrate the links between core protocols and content regulation in the areas of data protection, network neutrality, censorship, copyright, and social networks. For instance, DRM and security affect content consumption but can also be embedded within architectures and hardware. This type of joined-up thinking between content-based laws and architectural principles runs through our logical analysis of the case studies. It explains in large measure governments’ acknowledgment of the futility of attempts to regulate using law alone.

For a road traffic comparison, one cannot enforce fundamental changes in road users’ behavior without the support of automobile manufacturers, transport planners, as well as suppliers, pedestrians, bicyclists, and environmental groups. Instrumental regulation-led description of the Internet must acknowledge the underlying architecture in the same way as road traffic rules and conventions must acknowledge the environment in which they operate (safety rules do not permit bicycling at night without lights, for instance).

Though one does not have to understand every element in design to implement a rule, or every protocol in the layers model, it is essential to understand the system fundamentals. The end-to-end IP-based Internet is by definition an interoperable and technically neutral regime on which many open standards result in open source products or services for use without charge, protected by copyright licences (such as the General Public License) that require any derivative software to be freely available and modifiable (EC 2011a). In such a regime, anyone can design based on publicly and freely available protocols and software and interoperate with anyone else properly deploying the same protocols with the same rules. This open interoperability gives enormous practical advantages, which resulted in the development of the public Internet as it is widely experienced today.

Economic and Human Rights Justifications for Regulation

Code is not designed in a bubble by automatons, and it is not consumed in a bubble. Inherited regulation from other mass and personal media is relevant—an instance of regulatory path dependence.

Internet regulation can be discussed from the perspective of, for instance, laws relating to copyright, child protection, or freedom of speech. These are reflected in differing systems of regulation converging on the Internet, for instance, telecommunications, mass media, or information technology law. A growing body of analysis has focused on the interdependence of the various environments merging on the Internet and the question of regulatory divergence or convergence (Zittrain 2006; Schulz and Held 2001; Tambini, Danilo, and Marsden 2007).

We can somewhat simplify differing regulatory approaches into two types: those based on human rights such as child protection and freedom of speech and those based on economic efficiency (competition policy and competitiveness: for instance, infrastructure regulation, often characterized as technocratic in character). Although economics (Laffont and Tirole 2001) and human rights (Murray and Klang 2005) approaches to Internet regulation may have different emphases, there can be common ground (Lessig 1999; Ogus 1994). We show a schematic of the approaches and their predominant justifications in table 1.1.

Copyright is a particularly controversial issue in digital markets, where works can be perfectly reproduced, adapted, and redistributed at almost no marginal cost. It is primarily categorized in Anglo-American political discourse as an economic issue, while acknowledging authors' moral rights and the speech rights–based debate surrounding technical protection measures that can stop users from taking advantage of copyright exceptions.

Table 1.1
Representative regulatory systems and their predominant justification

Human rights intervention	Economic and competition frameworks
Freedom of expression	Digital rights management and trusted computing
Social network regulation	Personal Internet security
Consumer protection regulation	Network neutrality rules
Child protection blocking	Copyright and associated rights
Data protection	Telecoms infrastructure regulation

Though control over key infrastructure may be placed in the field of economic issues, these have fundamental impacts on users' rights and responsibilities.

These distinctions help us begin to sketch some of the fundamental rights problems in Internet regulation and develop our analysis. In looking for hard cases, we focused on copyright, data protection, censorship through filtering or technical blocking, social networking, and Internet service provider (ISP) network regulation. Competition policy and government aid (e.g., to the digitally excluded or marginalized) are a matter of particular relevance given that the returns to scale in digital industries are very high, tending to a high degree of concentration in each industry (Noam 2011).

The transdisciplinary approach that Clark et al. (2002, 2005) urge also offers a more holistic approach to regulatory design. The approach of using interlocking analysis taken from geographical, substantive, and disciplinary examination of the Internet is that most commonly used by legal and social scientific analysts of Internet regulation. We conduct our case studies with this approach in mind, along with a focus on human rights and due process, and economic analysis, which creates more effective regulation when married with technically efficient uses of code. We return to the wider benefits and changes of this approach in the concluding chapter.

Internet Regulation and Multistakeholders

Government and industry acting together is not the whole of the Internet story, whose unique regulatory characteristic lies in the two sides of the citizen's separate role. First, the citizen is increasingly involved in formal decision making and informal lobbying in the international and national system: consider the Congress of Non Governmental Organisations in the U.N. system, or the role of the EU Economic and Social Committee, or at a national level, the influence of single-issue lobbies such as environmentalists or human rights groups (Baird 2002; Hoffman 2005).

This pluralism is increased in the Internet regulatory map by the influence of "Netheads": highly influential and often stridently independent Internet engineers and technologists, who play a significant role in the standards and other regulatory processes (Cerf 1994; Lessig 1999; Gould 2000, Kahin and Abbate 1995), particularly in the infrastructure technology but also in content, applications and services. The Internet Technical Advisory Committee to the Organization for Economic Cooperation and Development (OECD) is an example we return to in the concluding chapter.

We need to unpack the term *governance* for computer scientists and lawyers, who are more comfortable with the term *regulation*, whether in its narrower legal enforcement sense (Baldwin et al. 1998) or the broad Lessigian architectural concept we outlined in the Introduction. Previous work has analyzed regulation on a continuum from state regulation to coregulation and regulated self-regulation to self-regulation, and on to standard setting and regulation by individual communities and by norm setting (Posner 1984; Ogus 1994; Leiner et al. 1998; Gaines and Kimber 2001), which matches the soft law negotiation process in which governance can be placed (Senden 2005). *Self-regulation* is defined broadly as a rule or the formation of norms: it exercises a function that shapes or controls the behavior of actors in that environment, which may include software code (Pitofsky 1998; Lemley 1999).

The term *governance* began to be used widely in political science literature in the 1990s to describe intermediate forms of self-regulation in the post–Cold War globalization literature (Pierre 2000). It emerged from the study of the firm in organizational theory (Williamson 1975, 1985, 1994). The term appears to have been first used in its political science meaning in Jones and Hesterly (1993) and has since developed a specific meaning in analysis of European federal-state politics (Kohler-Koch and Eising 1999). Governance is further discussed in much of the political science literature in terms of networks and informal rule-making institutions, such as multinational corporations and—particularly relevant for Internet governance—standard-setting organizations (Christou and Simpson 2009).

Practitioners and academics have adopted varying definitions of Internet governance (see Working Group on Internet Governance 2005 and Reding 2005) that fall into what might be termed minimalist (Mueller, Mathiason, and McKnight 2004) and maximalist (Drake 2005) areas. We use the term *Internet regulation* to refer to the range of public-private interactions covering substantive national and regional-plurilateral rules and practices governing specific Internet topics (Scott 2004; Marsden 2000; Grewlich 1999), similar to the broad use in Zysman and Weber (2000), noting that *governance* is a yet broader term that encompasses the institutional politics surrounding such regulation, including regimes with no enforcement powers at all, not even by norms, which therefore fall outside legal analysis (U.N. Economic and Social Council 2006).

Three paradigmatic examples of multistakeholder governance have previously been identified and widely studied in the Internet literature: the Internet Governance Forum (IGF), ICANN, and the newer regulatory issue of user-generated content. First, in the U.N. system, the IGF (created out of the World Summit on the Information Society) has enabled a highly influential type of civil society involvement in its activities. It as yet has no formal membership and no formal enforcement powers. Its “dynamic coalitions” formulate and publish opinions that have some political soft power, given the high degree of stakeholder involvement in the discussions. The presence of national government representatives at high levels in the IGF process demonstrates its importance and potential for precedent setting, as does its continued existence from 2006 with an annual mandate until 2015.

The idea that roles and responsibilities in the global and highly dynamic environment enabled by the Internet can be allocated on a temporary and contingent basis according to inclusive and nonhierarchical relationships is of course not new. Roles have often shifted among government, corporations, and civil society, but it appears that the United Nations is underwriting a more durable multistakeholder relationship in regard to Internet governance. This is a novel and fascinating attempt to achieve global dialogue around responsibilities in Internet regulation and was thought to represent a significant new networked governance paradigm (MacLean 2004; Murray 2006). However, the lack of significant influence and perceived marginalization of civil society over governance outcomes has led many academic analysts to doubt its real impact (Mueller 2010, Kleinwächter 2011).

The second example is that of ICANN, a coregulatory institution created by the U.S. government and contracted as a private corporation "responsible for managing and coordinating the Domain Name System (DNS) to ensure that every address is unique and that all users of the Internet can find all valid addresses." Domain names are an essential resource for effectively using the Internet: without such addresses and related numbers, it is difficult for other users to locate your computer (Kahn and Cerf 1999). The DNS is therefore a classic global public good (Kaul, Grunberg, and Stern 1999).

ICANN has been the main international organization charged with legitimising the user's role in Internet coregulation (Machill and Ahlert 2001), including through an attempt to introduce Internet voting in elections to the board (Mueller 2000, 2002; Froomkin 2000). It has also introduced an elaborate consultation and governance structure, but much of the debate has reinforced observers' views that civil society is marginalized in favor of governments, particularly the U.S. government (Komaitis 2010; Mueller 2010). In 2009, the Joint Project Agreement between the U.S. Department of Commerce and ICANN was replaced with an "affirmation of commitments" that reinforces ICANN's status as a nonprofit, multistakeholder organization with a bottom-up policy development process (Marsden 2011).

A third multistakeholder example concerns user-generated or Web 2.0 content (O'Reilly 2005; OECD 2007). Self-regulated communities of users and distributors of content, including peer-to-peer (P2P) networks such as KaZaA (Karagiannis, Rodriguez, and Papagiannaki 2005), and communities such as Facebook, Twitter, and YouTube, are transforming the Internet experience. Online communities have hundreds of millions of members regulated through a combination of the community's conditions or terms of use, general law (including, for instance, libel and copyright law)—the technical means for users to self-regulate, by, for instance, rating and labeling content; as well as reviewing and choosing to set content or users as trusted friends or otherwise (Marsden et al. 2006, 2008).

Radically different models of user control, rating, and filtering are enabled by such networks, though their relations to formal regulation and law are contingent on corporate whim (Berners Lee 2000; Benkler 2002, 2006; Braman and Lynch 2003; Braman 2009). These creators are also adopting new royalty-free licensing for their content, whether software that is collaboratively developed and freely distributed (the General Public License, for instance, for the Linux operating system) or content (e.g., via the Creative Commons project, which has created standard licenses to allow the sharing and "remixing" of content; Guadamuz 2009).

These three examples demonstrate the potential but also the perilous existence and relevance of less formal multistakeholder approaches and governance, as opposed to legal regulation with enforceable mechanisms and accountability. The importance of multistakeholder partnership as a fundamentally participatory approach to Internet policy is contested by its critics and, even more so, its supporters, who claim to have been marginalized and treated as symbolic, rhetorical, but powerless partners with corporations and governments in international standard setting. Our case study selection examines this paradigm more closely to assess whether governments' symbolic embrace of multistakeholder processes is reflected in genuine partnership in regulatory discussions.

Institutional Analysis of Internet Regulation

The growth of firms and other market institutions (Hodgson 1988) is explained by transaction cost analysis and intellectual property rights and other nondisclosure by protection of information outside those institutions (Stiglitz 1985). When one combines the two in information technologies, which are both disproportionately strategic and tend to market failure on a global scale, one has the ingredients for a compelling market failure scenario.

Where information communication technology has become the primary driver of growth, the intervention of governments in markets increasingly bears the hallmark of these institutionally based strategic analyses. To put it bluntly, who regulates information giants such as Microsoft, Facebook, and Google, and in whose interests? We cannot analyze the legal environment and software code in Internet regulation without considering the relationships of government, business, and users in civil society.

McCahery et al. (1996, 2) set out three “primary and interrelated concerns” in their study of regulation with a globalization agenda:

- Institutional response to dynamic economic change
- The “functional policy concern” regarding the utility and geometry of regulation
- The democratic deficit, resulting from the institutional (i.e., constitutional) underdevelopment of the regimes formed to regulate international economic actors

These questions of how, where, and with what tools to regulate in an increasingly complex and interdependent environment are vital:

- How do regulatory institutions respond to dynamic change in economic conditions?
- How are these governance reforms influenced by political (social, cultural, and ideological) and economic factors?
- To what extent do national and regional regulators diverge in their response to global technological factors?

These questions are part of the research hypothesis addressed in the school of institutional analysis termed the *new institutional economics*. The new institutionalism recognizes an increased complexity of both political and economic markets and the interaction between the two. The sociological version of institutionalism analyzes the mode of action constrained by normative, moral, and cognitive boundaries (Blom-Hansen 1997). Whereas economic institutionalism places microlevel motivations as the driver of change, sociological institutionalism adopts a macrolevel approach.

North (1990) acknowledges the contribution of sociological institutionalism within his concentration on historical institutional path dependency and thus provides a broader explanation of the incremental development of policy. This contrasts with the public choice variant of economic institutionalism (Moe 1997), in which the microfoundations of theory place too limited a role on institutions and actors. North begins from a view that acknowledges the economic compromises and failures of existing markets and public choice from an assumption that the individual pursues self-interest in a more economically rational and determinist approach.

North explains: “It is no accident that economic models of the polity developed in the public choice literature make the state into something like the mafia . . . the traditional public choice literature is clearly not the whole story" (140). He then explains why the parameters of investigation must be broadened from the narrowly neoclassical economic to encompass prior institutional structures and practices: "Informal constraints matter. We need to know much more about culturally derived norms of behavior and how they interact with formal rules to get better answers to such issues" (140).

Public choice has a weakness beyond the overly simplistic reliance on economic resources: it reveals taxpayer preferences where mobility is assumed (thus competition between geographically fixed regulatory jurisdictions) rather than the total electorate, and therefore policy "dictated by the private preferences of a narrow, arbitrarily identified class of itinerant at-the-margin consumers or investors . . . competition can force the pursuit of policies . . . removed from the public interest" (McCahery 1996, 15). This can lead to a deregulatory race to the bottom in which protections for nonmobile and vulnerable citizens are regressively removed. As McCahery puts it: "Competition influences results traditionally thought to lie in the discretion of sovereign regulators" (13).

Critics of public choice indicate that government actors are not necessarily efficiency maximizers in a narrow monetary sense (Tiebout 1956) and can resist races to the bottom. However, this potential for capture by regulated interests, notably large corporate lobbies, is an essential insight that we use throughout our analysis.

The Case Studies

This brings us to our five case studies, to each of which we dedicate a chapter. They address the topics of privacy; copyrights; censors; social networking; and smart pipes. The first three are case studies in fundamental rights with economic implications. The final two are studies of the most innovative platforms to develop new markets and protect those fundamental rights. They are also in a period of regulatory flux, yet with significant regulatory development in the past five years such that it is possible to draw some conclusions. We deliberately omitted search, whose development was critically dependent on further antitrust activity in Brussels and Washington. Furthermore, the concerns with multistakeholder representation and procedural justice that we explore in other case studies have been recently developed extensively in the search engine case (Zittrain 2008; Deibert et al. 2010).

Privacy Privacy and data protection is a well-studied field—not least because it has proven difficult for legislators and regulators to keep up with the rapid pace of change in Internet technologies that gather, process, and share data related to individuals. Most existing data protection legislation focuses on the behavior of governments and companies as they process the data. In chapter 3, we assess more recent attempts to shape the development of Internet technologies in an effort to improve the efficacy of regulation by embedding privacy by design into new systems.

Copyright As the Internet and digital duplication tools have lowered the marginal cost of reproduction and distribution of digital works toward zero, copyright has increasingly come into conflict with decades-old consumer behavioral norms about the use of copyrighted works. Rights holders have persuaded governments around the world to target new copyright regulation at personal computers, media devices, and Internet service providers (ISPs). In particular, new legal protection has been given to digital locks that restrict access to protected works; more recently some governments have placed requirements on ISPs to police the behavior of their users. The potential sanctions range from warning letters, through restrictions on connection speed, to disconnection. In chapter 4, we assess the outcome and broader lessons of these attempts to regulate the technology underlying the control of creative works.

Censors The debate over control of harmful and illegal material on the public Internet has developed from early debates in the United States over online obscenity leading to the Communications Decency Act 1996, through totalitarian regimes' great firewalls including China's 2009 "Green Dam" project, to democracies' self-regulatory actions, such as the U.K. Cleanfeed/Child Abuse Image Content system. Recent moves in Europe have stepped away from a decade-old self-regulatory approach toward a coregulatory approach in which ISPs and government agencies cooperate. ISP-level filtering of inadvertent viewing of illegal material is becoming mandatory, with definitions widened from child pornography to hate speech to extreme speech and then copyright (McIntyre 2013). The institutionalization of this new state-sanctioned and audited approach presents significant new challenges to freedom of expression and has led to calls for an Internet bill of rights in the European Parliament, U.S. Congress, and elsewhere (Reding 2012).

Social networking sites The mass take-up of social networking tools has heightened concerns over privacy, copyright, and child protection and created a generic center for regulatory activity that raises new questions about the scope and focus of Internet regulation. With over 1 billion Facebook users, regulators' concerns over ordinary citizens' use of the Internet have led to specific regulatory instruments that address the risks of such use (Facebook 2012; Office of the Data Protection Commissioner Ireland 2011). Chapter 6 builds on the literature and regulatory proceedings to assess the extent to which the more conventional issues-based regulatory instruments are being supplemented by generic social networking regulation.

Smart pipes Network openness is under reconsideration as never before, with increasing partitioning of the Internet, partly driven by security concerns, which is leading many ISPs to add capabilities to their routers to filter, inspect, and prioritize network traffic to a much greater degree than previously possible. This policy field displays both a plurality of market actors (content and carriage disguises the various interests within and between those sectors, such as mobile networks and vertically integrated actors) and a profusion of formal (state and supranational) and informal (standard-setting) regulators. It exhibits advanced examples of regulatory capture, especially in the more static and matured regulatory environment of telecoms. In chapter 7, many of the features of earlier case studies, from content industries (copyright and privacy) and networks (surveillance and cryptography policy, security policy), come together.

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

- Who were the key stakeholders (traditional and multistakeholder), and how far were they involved in policy debates, organizational design, and operational issues associated with the regulatory processes or institutions adopted? What was the institutional political economy (Mueller 2010)?
- How far did solutions have source, process, or outcome legitimacy (Weber and Grosz 2009), including human rights compliance, in the outcome? What influence did fundamental rights have in policy design? This exploration is based on both documents relating to design and later

judgments of human rights bodies (e.g., national parliamentary scrutiny committees, Council of Europe).

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

In the next chapter, we assess examples of both code created by "prosumers" (active users who are sharing and producing content, rather than passively consuming it—notably hackers) and economic regulation through competition law in more detail and construct a matrix for the individual case studies. In each case study, we examine whether governments have moved from sledgehammer prohibition-based, enforcement-oriented regulation, to smarter regulation that works technically, with some degree of outcome legitimacy in terms of goals. These might, for instance, support the creation of public goods and disruptive innovation in markets. A smart solution in terms of code and regulation would provide effectiveness in enforcement (whether by law or code), technical efficiency (in an engineering sense) and legitimacy, transparency, and accountability (to allay rights-based concerns). Unsurprisingly, the outcomes are likely to be trade-offs among these goals.

By analyzing and contrasting our case studies, we aim to formulate specific recommendations in the concluding two chapters. We seek to develop a more unified framework for research into Internet regulation, designed to work with these hard cases, and use the best of both software and legal code to create principles for regulatory intervention based on due process, effectiveness and efficiency, and respect for human rights. We describe this type of regulation as *prosumer law.*