7 Smart Pipes: Net Neutrality and Innovation

As the Internet first became a mass medium during the 1990s, many companies (notably AOL, followed by mobile operators) tried to maximize advertising revenue by building "walled gardens" for their customers, to keep users within affiliated Web pages. However, they could not keep up with the rapid innovation and diversity of the rest of the Internet and the growth of dedicated search engine Google. Most were forced by their customers to become increasingly interoperable with the rest of the Internet (Ziewitz and Brown 2013).

The same commercial pressures, with additional state sovereignty concerns and capacity pressures on network operators, are again driving a partitioning of the Internet into more controlled private domains. Facebook is providing social tools that encourage its users to access external content from within its own platform. Many ISPs are deploying sophisticated traffic management tools that allow some types of data (e.g., real-time voice calls) and content sources (specific Web sites that have paid for privileged access) to be prioritized. While this can reduce congestion and security threats to networks, it can also be used to protect existing monopoly services and new proprietary services (Mims 2011).

The motivation to make the networks more intelligent (to create "smart pipes") is to reduce congestion to protect users' experience and, indirectly, the business of the ISP. The monopoly motive is directly concerned with the ISPs' profits and not directly with user welfare, especially where users have little transparency or ability to switch to another provider. Mobile networks have been particularly active in blocking voice over Internet Protocol (VoIP) and even rival texting services. This has led to political campaigns for network neutrality, the principle under which ISPs must give equal treatment to comparable traffic flows across their networks and not

block any application without user consent (Wu 2003b; Lemley and Lessig 1999).

Conventional U.S. economic arguments have always been broadly negative to the concept of network neutrality, preferring the introduction of tariff-based congestion pricing (David 2001). Hahn and Wallsten (2006) explain that network neutrality "usually means that broadband service providers charge consumers only once for Internet access, don't favor one content provider over another, and don't charge content providers for sending information over broadband lines to end users." This is the focus of the problem: network owners with vertical integration into content or alliances have greater incentives to require content owners (who may also be consumers) to pay a toll to use the higher-speed networks that they offer to end users (Economides and Tåg 2007). Note that all major consumer ISPs are vertically integrated to some extent with proprietary video, voice, portal, and other services.

The Federal Communications Commission in the United States has acted on several network neutrality complaints (notably those against Madison River Communications, an Internet service provider, in 2005 and Comcast in 2008) as well as introducing the principle in part through several merger conditions placed on dominant ISPs, but it delayed its report and order on network neutrality until its eventual publication in the *Federal Register* in September 2011. It was instantly challenged by various interested parties and would be litigated in the winter of 2012–2013. Development of European legal implementation of network neutrality principles has been slow, with the European Commission referring much of the detailed work to the new Body of European Regulators of Electronic Communications (BEREC), which was developing an extensive work program on network neutrality in 2012 (BEREC 2011). At the European member state level, statements of principle in favor of network neutrality have been made in, for instance, France, but no legislation was enacted before the end of 2011 (Cave 2011).

Public Policy Objectives

Network neutrality comprises two separate nondiscrimination commitments (Marsden 2010, 24): one of universal service and another of common carriage. Backward-looking "network neutrality lite" claims that Internet

users should not be disadvantaged due to opaque and invidious practices by their current ISP. The argument is that a minimum level of service should be provided that offers open Internet access without blocking or degrading specific applications or protocols—an updated form of universal service (Mueller 1998). That provides a basic level of service that all subscribers should eventually receive. Forward-looking "positive network neutrality" describes a practice whereby higher quality of service (QoS) for higher prices should be offered on fair, reasonable, and nondiscriminatory (FRAND) terms to everyone, a modern equivalent of common carriage (Noam 1994). The type of service that may be entitled to FRAND treatment could result in short-term exclusivity in itself, as, for instance, wireless and mobile cell towers may be able to carry only a single high-definition video stream (Talbot 2006) at any one time and therefore a monopoly may result. As common carriage dictates terms but not the specific market conditions (Cherry 2006; Marsden 2011), transparency and nondiscrimination would not automatically result in a plurality of services.

ISPs have argued that there is little public interest in controls over the operation of private networks and that regulation will stifle innovation in network management, the development of new services, and, ultimately, investment in new network capacity. Regulators such as Ofcom in the United Kingdom have accepted much of this laissez-faire position, arguing only that basic consumer protection and competition policies are required to ensure an efficient market in services (Kiedrowski 2007).

Public Policy and Fundamental Rights

Network neutrality is a more political issue than most telecommunications regulators are used to, as technologies of censorship are at stake (La Rue 2011). BEREC (2010, 20) explains: "Freedom of expression and citizens' rights, as well as media pluralism and cultural diversity, are important values of the modern society, and they are worth being protected in this context—especially since mass communication has become easier for all citizens thanks to the Internet." It adds that because economic regulators are narrowly focused, "intervention in respect of such considerations lies outside the competence of BEREC."

This lack of competence is often, but not always, a result of the legislative competences allocated by national parliaments to regulators. The

explicitly technoeconomic remit of most telecoms regulators in Europe gives them limited functionality in assessing rights-based issues such as data protection and freedom of expression. However, the so-called converged regulators of broadcasting and telecoms such as AgCom in Italy and Ofcom in the United Kingdom have no such legislative block on assessing human rights, and any reluctance to make such assessments is likely to be a result of organizational culture as well as the perceived groupthink of market-oriented technoeconomists. With increasing EU attention to rights-based issues, as a result of the incorporation of the Charter of Fundamental Rights within the Lisbon Treaty (in effect from December 1, 2009), national regulators have been slow to react to the fundamental rights concerns raised in this debate. The Court of Justice decisions in *SABAM* v. *NetLog* (2012) and *Scarlet Extended SA* v. *SABAM* (2011) force them to confront the issue in future.

Forms of private censorship by intermediaries have been increasing over the past decade even as the law continues to declare those intermediaries (mainly ISPs, but increasingly also video hosting companies such as YouTube, social networks such as Facebook, and search providers such as Google) to be "three wise monkeys." These intermediaries are not subject to liability for their customers' content under the "mere conduit" regimes of the United States and EU so long as they have no actual or constructive knowledge of that content: if they "hear no evil, see no evil and speak no evil" (Marsden 2010). Deep packet inspection (DPI) and other advanced traffic management techniques will give ISPs much more granular knowledge of what their customers are downloading and uploading on the Internet. ISPs could filter out both annoying and illegal content. For instance, they could "hear" criminal conversations, such as those by terrorist sympathizers, illegal pornographers, harassers, those planning robberies, libelous commentary, and so on. They could also "see" illegal downloading of copyrighted material. They could be obliged to cooperate with law enforcement or even copyright industries in these situations, which would create even greater difficulties where that speech was legal in one country but illegal where it was received (Deibert et al. 2010).

Traffic management techniques affect not only high-speed, high-money content but, by extension, all other content too. You can build a high-speed lane on a motorway only by creating inequality, and often those "improvements" slow down everyone currently using the roads. The Inter-

net may be different in that regulators and users may tolerate much more discrimination in the interests of innovation. To make this decision on an informed basis, it is in the public interest to investigate transparently both network neutrality "lite"' (the slow lanes) and network neutrality "heavy" (what rules allow higher-speed content). For instance, in the absence of regulatory oversight, ISPs could use DPI to block some content altogether if they decide it is not to the benefit of ISPs, copyright holders, parents, or the government. ISP blocking is currently widespread in controlling spam e-mail, and in some countries in blocking illegal images, as we described in chapter 5.

One of the main claims by ISPs wishing to manage Internet traffic is that Internet traffic growth is unmanageable by traditional means of expansion of bandwidth and that therefore their practices are reasonable. In order to research this claim, regulators need access to ISP traffic measurement data. There are several possible means of accessing data at Internet exchange points, but many data are private either because they are between two peers that do not use an exchange or because they are carried by a content distribution network (CDN). No government regulator has yet produced any reliable data, and carriers' own data are subject to commercial confidentiality.

A common ISP mechanism to reduce network congestion is to set caps on the monthly bandwidth available to each customer. This was the default in most countries prior to the introduction of broadband modems in the late 1990s. Only in countries with unmetered local calls, such as Canada and the United States, was Internet use "all you can eat" (Oftel 2000). With the introduction of broadband cable in Canada, the Canadian Radio-Television and Telecommunications Commission permitted monthly download caps on users. This was justified by the shared resource used by cable modem subscribers in the local loop (Geist 2011). The commission (2011) reiterated its permission for caps, justified by reference to its responsibilities to ensure competition under Telecommunications Act 1993 Section 7. Comcast in the United States created a 250 GB cap (Burstein 2008), which was considered more transparent than its previous use of DPI and other techniques to prevent peer-to-peer (P2P) transfers.

Most caps relate to maximum download capacity and are assessed independent of the maximum download speeds that users can receive, the latter being the headline rates that are generally used in broadband

Table 7.1
Public policy and market failure

Social impact of technology	Use of monitoring of traffic still largely hidden from fixed end users. Mobile broadband and streaming video growth likely to increase user concerns.
Policy drivers—entry barriers, network and scale effects, competition	QoS technology imposes nontrivial network costs that increase with scale, though deployment expertise offers scale economies. Security dual use reduces costs.
Fundamental rights in policy design	Notable by the absence of rights from early deployment, discussion on this issue is growing with regulatory oversight.
Lessons	Permitting technology development without privacy and expression oversight can lead to invasive technologies. Telecoms regulators inadequate to discuss rights-based policies.

advertising to consumers. OECD (2008) found that of 215 broadband packages sampled, almost half would result in users' exceeding their monthly caps within three hours at advertised maximum speeds. Countries that were at the bottom of the OECD tables for bandwidth provision, Australia and New Zealand, have adopted the radical step of commissioning a national fiber local loop to replace their incumbent telephony monopoly. Public intervention is by no means a taboo in broadband investment, and the European Commission has repeatedly approved all nonurban public investment in fiber deployments proposed by member states, while Australia is building a publicly funded national fiber wholesale network. The lessons of public policy and market failure are illustrated in table 7.1.

Types of Code Regulation

Most voice calls and video today use a dedicated copper telephone line or cable line; tomorrow they may use high-speed fiber lanes on Internet connections, which could make a good business for ISPs that wish to offer higher capability for managed services (such as high definition video with guaranteed quality of service) using DPI. It is both smart pipes' intelligent networks and the greater capacity of fiber-optics that enable such services. Not all ISPs will do so, and it is quite possible to manage traffic less obtrusively by using the DiffServ protocol to prioritize traffic streams within the same Internet channel. The DiffServ protocol specifies a simple, scalable,

and coarse-grained mechanism for classifying and managing network traffic. Waclawsky (2005) stated in regard to ISP traffic management protocols that "this is the emerging, consensus view: [it] will let broadband industry vendors and operators put a control layer and a cash register over the Internet and creatively charge for it." The Third Generation Partnership Project (3GPP), the standards body for 3G mobile telephony, has been working since 2000 on a set of standards called IMS (IP Multimedia Subsystem 2006): an operator-friendly environment intended to generate new revenue by way of DPI. In 2005, fixed-line carriers and equipment vendors created IPSphere (2006), a new set of standards for network intercession in IP application flows. Both sets of standards support the ability to filter and censor by file type and content provider on the Internet. In an extreme case, one could degrade all content that is not tagged as paying a premium carriage fee. This enables the carrier to discriminate and decide which content to delay and which to permit to travel at normal speeds to the end user. Users can encrypt all traffic to prevent inspection in the same way that firewalls on Intranets were evaded using Port 80 and other techniques (Clayton, Murdoch, and Watson 2006). (Port 80 is the hypertext transfer protocol's usual port on a computer modem; thus routing traffic through this port makes it highly unlikely to be blocked).

Until recently in the United States, the Internet had been subject to telecommunications regulation only for interoperability and competition, building on inquiries that regulated computer data transfer by the Federal Communications Commission (Werbach 2005), and the design principle of end-to-end described by Saltzer, Reed, and Clark (1984), which dominated early Internet design. That principle itself was superseded by the need for greater trust and reliability in the emerging broadband network by the late 1990s, particularly as spam e-mail led to viruses, botnets and other risks. As a result, end-to-end has gradually given way to trust-to-trust mechanisms, in which receipt of the message by one party's trusted agent replaces the receipt by the final receiver (Clark and Blumenthal 2011). This agent is almost always the ISP, and it is regulation of this party that is at stake in network neutrality. ISPs are not only removing spam and other hazardous materials before they reach the (largely technically uneducated) subscriber; they also can remove other potentially illegal materials on behalf of governments and copyright holders, to name the two most active censors on the Internet, as well as prioritizing packets for their own benefit.

Given the difficulty in assessing whether network layer innovation is necessary, network engineers' calls to avoid neutrality regulation are strikingly vehement. Handley (2011) suggested that the role of standards organizations, especially the Internet Engineering Task Force (IETF), is to provide "tussle space" (Clark et al. 2002) for ISP and content provider business models to emerge, notably by ensuring that protocols permit application layer innovation. He points out that network neutrality is problematic for the standards community because it involves legal and economic issues that are outside the IETF core competence, offers rival business models to which IETF must be agnostic, and has different ramifications in different countries. For instance, U.K. ISPs have widely deployed DPI, whereas in the United States and Germany, DPI is much less often deployed.

Initial treatment of network neutrality discussed four "Net freedoms" (Federal Communications Commission 2005) for end users: freedom to attach devices, run applications, receive the content packets of their choice, and receive "Service Plan Information . . . meaningful information." Even now, scholars are suggesting that freedom to innovate can be squared with design prohibitions (van Schewick 2010), despite over a decade of multibillion-dollar protocol development by the ISP community resulting in the ability to control traffic coming onto their networks (Waclawsky 2005) and wholesale rationing of end user traffic (Odlyzko and Levinson 2007). Berners-Lee (2006) explained: "There have been suggestions that we don't need legislation because we haven't had it. These are nonsense, because in fact we have had net neutrality in the past—it is only recently that real explicit threats have occurred." Berners-Lee was particularly adamant that he does not wish to see the prohibition of QoS because that is precisely the claim made by some U.S. network neutrality advocates—and opposed by the network engineering community.

Deep Packet Inspection and Traffic Management

In order to manage traffic, new technology lets ISP routers (if so equipped) look inside a data packet to "see" its content, using DPI and other techniques. Previous routers were not powerful enough to conduct more than a shallow inspection that simply established the header information—the equivalent of the postal address for the packet. An ISP can use DPI to determine whether a packet values high-speed transport—as a television

stream does in requiring a dedicated broadcast channel—and offer higher-speed dedicated capacity to that content, typically real-time dependent content such as television, movies, or telephone calls using VoIP.

Avoidance of DPI and other inspection techniques by encryption was a concern for Clark et al. (2002, 9): "Encrypting the stream might just be the first step in an escalating tussle between the end user and the network provider, in which the response of the provider is to refuse to carry encrypted data" (though he imagined only an authoritarian national monopoly ISP engaging in such behavior). Handley (2011) agrees and argues that standards bodies can designate the protocols to build the playing field, not to determine the outcome, particularly because design is not value neutral. He uses the session initiation protocol (SIP, specified in the IETF's RFC 2543) as an example of a standard that can be used by both network neutral ISPs and those desiring more intrusive traffic management, avoiding the dilemma that IETF becomes "stuck between [DPI], and innovation-inhibiting regulation." Note that "SIP is designed to be independent of the lower-layer transport protocol" (RFC 2543, 1999, 1).

The main public policy problem with DPI is its potential for surveillance and privacy invasion; with regulation, it eliminates the "tussle space," and government has to pick winners, as well as encourage rent-seeking behavior by those potential winners. Handley (2011, 11) lists five types of prioritization that have the potential to discriminate against particular applications, of which DPI is worth further attention, if only because it is the most expensive and intrusive of the technologies listed, and therefore ISPs have a particularly acute choice between investment in bandwidth capacity and in DPI to control the level of traffic at existing bandwidth. To some extent, there is a binary choice, and at the margin "either we end up with a network where innovation can only be within narrow bounds, constrained by yesterday's common applications, or the regulators eventually step in and prohibit broad classes of traffic prioritization" (Handley 2011, 16). Crowcroft (2011) makes the additional point that there has been little innovation within the network architecture for thirty years and that neutrality regulation might make this problem worse. He concludes that "we never had network neutrality in the past, and I do not believe we should engineer for it in the future either" (12).

The applications standards community is less sanguine about network-layer discrimination than the network engineers, perhaps unsurprisingly

as it is their services that stand to receive discriminatory treatment. The end-to-end applications argument has been made forcefully by World Wide Web inventor Tim Berners-Lee (2011), and it is worth recalling that he made WWW standards royalty free and nondiscriminatory as a design choice in the creation of the World Wide Web Consortium in 1994 (Marsden 2011). He argues strongly against application discrimination, though he is careful not to argue for legislation prohibiting QoS that does not discriminate in this way.

Similarly, Handley places faith in nondiscrimination by application via the Re-feedback of Explicit Congestion Notification (Re-ECN) protocol developed by Briscoe (2008). However, development and deployment of draft protocols (see RFC 2009) as solutions in an area that directly affects free speech is a heroic endeavor for a politician, however logical to an engineer. Given the range of issues, the ITU Focus Group on Future Networks (2010) concluded that much wider liaison both within ICT industry standards bodies and with neighboring and converging areas was essential to determine future network architectures.

DPI equipment can also be used for blocking specific content, as requested by many governments. If a government is willing to require ISPs to install DPI equipment, dual-purpose technology that can be used for much more than law enforcement purposes, do ISPs have an incentive to use that equipment to its maximum commercial effectiveness? This is a matter of pressing and legitimate public policy. This problem of when QoS tools may be used arose in the context of behavioral advertising when British Telecom entered into secret subscriber trials with Phorm, a U.S.-based targeted advertising corporation in 2006, though in the wake of the controversy, U.K. ISPs have ceased to trial with Phorm (McStay 2011) and it appears to have exited the European market in favor of the regulatory environments in the new markets of South Korea and Brazil (Clayton 2008; Marsden 2010).

DPI and other techniques that let ISPs prioritize content also allow them to slow down other content, as well as speed up content for those that pay (and for emergency communications and other network-preferred packets). This potentially threatens competitors with that content: Skype offers VoIP using normal Internet speeds; uTorrent and BBC's iPlayer have offered video using P2P protocols. Infonetics (2011) states: "Although residual concerns over Net neutrality and operators' proclivity for all-you-can-eat services have made U.S. operators hesitant to do any widespread deploy-

Table 7.2
Types of code and code regulation

Layer	Varies but typically network and transport layers
Location (manufacturers, ISPs, servers, clients)	Hardware and software vendors' DPI solutions; ISP traffic management solutions
Enforcement of code	Termination monopoly held by ISPs—nontransparent term of use for end users

ments . . . the DPI market is growing at a healthy pace in other parts of the world. We anticipate particularly dramatic growth in emerging markets." They add that "operators across all regions plan to use DPI to enable value-added services, such as content-based charging and premium services that provide a guaranteed quality of service for applications like video streaming." This demonstrates the dual use of the technology, to both rate-limit and control the user experience for security and cost rationalization, as well as to provide faster secure service for premium content.

Encryption is common in these applications and partially successful in overcoming these ISP controls, but even if all users and applications used strong encryption, this would not succeed in overcoming decisions by ISPs simply to route known premium traffic to a "faster lane," consigning all other traffic into a slower nonpriority lane (a policy explanation simplifying a complex engineering decision). P2P is designed to make the most efficient use of congested networks, and its proponents claim that with sufficient deployment, P2P could largely overcome congestion problems. Table 7.2 illustrates the types of code and code regulation discussed in this section.

Institutional Political Economy

This policy field displays a plurality of market actors (content and carriage disguise the various interests within and between those sectors, such as mobile networks and vertically integrated actors) and a profusion of formal (state and supranational) as well as informal (standard-setting) regulators. It exhibits advanced examples of regulatory capture, especially in the more static and matured regulatory environment of telecoms.

The arguments surrounding network neutrality revive the surveillance-industrial complex (ACLU 2004) argument of long standing between civil society advocates of free speech and expression on the Internet together

with almost all noncommercial and some commercial content companies, and large ISPs and some commercial content providers. To briefly reprise the ACLU argument, the claim is that companies (and individuals, though this category is less relevant here) are pressured to voluntarily or compulsorily provide consumer information to the government; government processes and searches private data on a mass scale; and some companies are pushing the government to adopt surveillance technologies and programs based on private sector data, investing in the private sector's surveillance capability. We consider each in turn.

Large telecoms and commercial content companies largely oppose network neutrality, in that payment on a priority basis supports a cable TV type of model and protects their investments in commercial video rights and lower bandwidth networks. The argument is that noncommercial players and domestic users are unwilling to invest in better services and need to be rationed in order to be persuaded to pay for higher quality. There is some truth in this claim, but also in the counterclaim that ISPs and large content providers may be using technical means to protect their existing monopoly or oligopoly services, including telephone service and premium TV channel provision. (Consider: if voice over the Internet is effective, why would any consumer pay for a telephone service or telephone calls? A similar argument applies to video.) In Canada, Telus has argued that rationing access by metering billing for consumers is ineffective because it has substantial competition, suggesting that a truly competitive market would produce increasing capacity offers to consumers (Geist 2011).

The use of "throttling" technology (by which a network administrator slows down non-preferred packets)—essentially P2P applications being slowed by use of Sandvine technology—was at issue in the Federal Communications Commission (FCC) order (2008) against Comcast, a major cable broadband ISP. A Comcast deposition to the FCC stated that BitTorrent throttling began in May 2005. Comcast's claims not to have throttled and blocked traffic when exposed in May 2007 had been misleading. The FCC ordered Comcast to do the following within thirty days:

1. Disclose to the commission the precise contours of the network management practices at issue here, including what equipment has been used, when it began to be employed, when and under what circumstances it has

been used, how it has been configured, what protocols have been affected, and where it has been deployed;

2. Submit a compliance plan to the commission with interim benchmarks that describe how it intends to transition from discriminatory to nondiscriminatory network management practices by the end of 2008

3. Disclose to the commission and the public the details of the network management practices that it intends to deploy following the termination of its current practices, including the thresholds that will trigger any limits on customers' access to bandwidth.

Most damning, the FCC found that "Comcast has an anti-competitive motive to interfere with customers' use of P2P applications." This was because P2P offers a rival TV service delivery to cable, which the FCC found "poses a potential competitive threat to Comcast's video-on-demand (VOD) service." The Comcast use of DPI to discriminate between providers of P2P was also condemned in strong terms: "Comcast's practices are not minimally intrusive, as the company claims, but rather are invasive and have significant effects." The commission concluded that Comcast's conduct blocked Internet traffic, rejected Comcast's defense that its practice constitutes reasonable network management, and "also concluded that the anti-competitive harms caused by Comcast's conduct have been compounded by the company's unacceptable failure to disclose its practices to consumers."

The FCC justified its regulatory authority to issue the Comcast order and open Internet order (Federal Register 2011), invoking its Title I ancillary jurisdiction under the Communications Act to regulate in the name of national Internet policy as described in seven statutory provisions, all of which speak in general terms about promoting deployment, promoting accessibility, and reducing market entry barriers. On these grounds, Comcast in 2008 brought a suit to the court of appeals to overturn the order, succeeding in 2010 (Frieden 2011). The FCC ruling against Comcast's attempts to stop P2P by sending phantom reset packets to customers reflects another easy case, as obvious as the VoIP blocking in Madison River in 2005. Comcast announced a 250 GB monthly limit in early September 2008, replacing its previous discretionary terms of use reasonable caps (Burstein 2008). Comcast also replied by explaining its use of Sandvine technology and its plans to introduce a "blunter weapon" in its future

shaping of traffic. Comcast responded to the FCC network neutrality ruling by claiming that it engineers its own VoIP product with QoS and avoids the public Internet.

The "open Internet" and network neutrality consultations launched by the European Commission in 2010 produced over 300 responses, fairly evenly divided between industry and users, the former generally in favor of discrimination and the latter opposed. (The consultation was described as *open Internet* in an attempt to prevent political rows that characterized the use of the term *net neutrality* in the United States.)

There was very little input by content providers, but a great deal by ISPs and relevant equipment manufacturers. Ofcom in the United Kingdom had fewer than 100 responses to its so-called network neutrality consultation earlier in the same year. By contrast, the 2009–2010 inquiry in the United States produced almost 30,000 responses, though many of these were very similar or identical. The level of interest was also reflected in an online petition in favor of network neutrality signed by almost 2 million individuals. In the United Kingdom, by contrast, the use of online petitions at the prime minister's Web site was more exercised by the by-product of network neutrality: behavioral advertising trials and a petition condemning the secret trial by Phorm produced almost 10,000 votes. Though public opinion is fickle, it was clear in summer 2011 that a very large group of Netherlands voters were very upset that KPN Mobile threatened to use DPI (Preuschat 2011) to block WhatsApp, which produced the political support for its network neutrality law. We may expect to see more protest behavior by "Netizens" who do not agree with network neutrality policies, especially where ISPs are seen to have failed to inform end users fully about the implications of policy changes. Regulators and politicians are challenged publicly by such problems, particularly given the ubiquity of e-mail, Twitter, and social media protests against censorship. Research into social activism against corporate control of the Internet is a growing research field (Powell and Cooper 2011; Hart 2011).

The total responses do not reflect the degree to which policymakers listen to the various responses, and the general bias toward business constituencies was reflected in the composition of the speaker panels for the European Parliament and Commission joint hearings on network neutrality and the open Internet organized in Brussels after the conclusion of the consultation in November 2010. The vast majority of speakers represented

industry prodiscrimination interests, with only members of the European Parliament, content provider BBC, and a single civil society stakeholder presenting dissenting views from the commission-organized morning session. The afternoon session was more balanced due to the presence of many consumer-oriented members of the European Parliament. The U.K. government organized a private network neutrality summit in March 2011, at which two user groups were invited, together with the Taxpayers Alliance. This reflects the wider view of telecoms policymakers that civil society organizations are outsiders to the usual telecoms economic discussion and raise intractable problems. Telecoms policymakers in government are only slowly learning the need for rights-based dialogue.

Net Neutrality, Censorship, and Developing Countries

The problems of development and the global digital divide are intimately connected to network neutrality (Internet Governance Forum 2008). Internet connectivity is still very expensive for most developing countries, despite attempts to ensure local Internet peering points (exchanges) and new undersea cables, for instance, serving East Africa. Flooding the developing world's ISPs with video traffic, much of which comes from major video production countries such as India, Nigeria, and the United States, could place local ISPs in serious financial peril. Casualties in such undertakings include countries blacklisted by major ISPs for producing large amounts of spam.

The second development problem that the network neutrality debate centers on is the wireless or mobile Internet. Most developing countries' citizens have much lower bandwidth than the West, and most of their connectivity is mobile: India is probably the poster child for a country with at least ten times more mobile than fixed phone subscribers. In the next several years, Internet users in the developing world will test the limits of mobile networks, and capacity as well as price might determine the extent to which they can expect a rapidly developing or a Third World Internet experience.

Universal service is still a pipe dream for many in the developing world, and when that arrives, the definition it is given will determine the minimum threshold that ISPs have to achieve. As Mueller (2007, 7) states, network neutrality "must also encompass a positive assertion of the broader social,

economic and political value of universal and non-discriminatory access to Internet resources among those connected to the Internet."

The types of non network neutrality employed in West Asia and North Africa in winter 2010–2011 were politically rather than economically motivated, that is, by political censorship designed to prevent citizens' access to the Internet, as seen in chapter 5. Mueller (2007) argues that the tendency of governments in both repressive and traditionally democratic regimes to impose liability on ISPs to censor content for a plethora of reasons argues for a policy of robust noninterference. That is especially valuable in countries where there is much less discussion of how government deployment of ISPs as censors can endanger user privacy and freedom of expression. Mueller suggests that the network neutrality metaphor could be used to hold all filtering and censorship practices up to the light, as well as other areas of Internet regulation, such as domain name governance.

Table 7.3 summarizes the political economy concerns raised in the network neutrality debate, in which large corporate interests sought to capture the policymakers' agenda, with a vociferous lobbying campaign in the United States and a muted one in Europe (Sluijs 2010), led by civil society groups aiming to preserve the open Internet. It is notable that the

Table 7.3
Institutional political economy

Key actors: national, regional, global	Telecoms regulators; ISPs, intermediaries, content companies, largely local user groups. Coders in multinational corps. Security-industrial complex re DPI.
How legitimate and accountable?	Telecoms regulators accountable through parliaments; self-regulatory solutions unaccountable except through telecoms regulators (where applicable).
Multistakeholderism	Organized opposition to corporate blocking of applications in United States, Netherlands, and France; less attention paid elsewhere. Some effect on European Parliament amendments to telecoms package 2009.
Key technical actor buy-in	Organized by corporate vendors, notably Alcatel-Lucent, and Sandvine. Mobile industry at forefront of 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	Highly technical issue meant little traction for policy initiatives to shape code except in egregious cases. Much of technical community active in control environment.

European telecoms regulators, and government officials, were initially deaf to the human rights concerns raised. The European Data Protection Supervisor (2011a) then explained its concerns in this area, which concerned data protection and the impact on privacy of the widespread deployment of DPI.

Outcomes

Unsurprisingly, network neutrality regulation has been fiercely resisted by the ISPs that wish to discriminate and charge nonaffiliated content providers higher prices or throttle popular existing services. Neutrality regulation to date has relied mainly on a series of declarations and merger conditions. Mergers afford regulators the opportunity to introduce such relatively minor adjustments, as merger parties are eager to conclude the overall deal and trade off the relatively minor inconvenience of controls on traffic management in the interests of successful approval. In the same way as consumers—even with perfect information—may not view traffic management as the primary goal of their subscription to broadband (and are thus easy targets for restrictive conditions so long as industry standards prevent real choices among ISPs), so ISPs may make strategic choices to accept some limited traffic management conditions as a price of approval. The failed 2011 merger of AT&T Wireless and T-Mobile illustrated the propensity to argue for enforcing network neutrality through merger conditions, as did the merger of Level 3 and Global Crossing, important tier 1 backbone providers with extensive content delivery networks, and the Level 3 legal dispute with Comcast (Frieden 2011).

In the discussions to amend the E-Communications Framework by Directives 2009/136/EC and 2009/140/EC, large, well-resourced European incumbent ISPs saw the opportunity to make common cause with mobile operators (Wu 2007) and others in an alliance to permit filtering. Politicians in 2012 were reviewing the ECD (European Commission 2012) and implementing local laws that favor, for instance, their copyright industries, such as the Digital Economy Act 2010 in the United Kingdom and the Haute autorité pour la diffusion des oeuvres et la protection des droits sur internet law in France (EC 2011b). Regulations are erecting entry barriers with the connivance of the incumbent players, with potentially enormous consequences for free speech, free competition, and individual expression (Akdeniz 2011). This may or may not be the correct policy option for a

safer Internet policy (to prevent exposing children to illegal or offensive content), though it signals an abrupt change from the open Internet (Zittrain 2008). It is therefore vital that regulators address the question of the proper approach to network neutrality to prevent harm to the current Internet, as well as begin to address the heavier questions of positive or tiered breaches of network neutrality.

Privacy inquiries can also have an impact on regulatory control of traffic management, with the U.K. government threatened with legal action by the European Commission for implementation of the EU data protection framework that allowed the secret and invasive behavioral advertising practices of British Telecom and Phorm in 2006. The introduction of network neutrality rules into European law was under the rubric of consumer information safeguards and privacy regulation, not competition rules, and the U.S. Congress has been exploring privacy rules and controls on ISP behavioral advertising activities.

Although network neutrality was the subject of FCC regulatory discussions and merger conditions from 2003 (Frieden 2011), its status has remained unclear, with no legislation passed by Congress, and FCC actions reserved to isolated examples of discrimination that were litigated. President Obama was committed to network neutrality regulation from his Senate career in 2006 and during his first presidential election campaign (Marsden 2010). A Notice of Proposed Rule Making by the FCC extended a consultation on network neutrality over 2009–2010. This process was finishing just as a court of appeals in April 2010 judged that the FCC's regulatory actions in this area were not justified by its reasoning under the Communications Act 1996 (*Comcast* v. *FCC* 2010). The successful Comcast appeal meant that the FCC had three legal choices: reclaim Title II common carrier authority for ISPs under the 1996 Telecommunications Act, ask Congress to relegislate to grant it Title I authority, or try to assert its own Title I authority subject to legal challenge (Frieden 2010). It adopted this last course in its Order of December 23, 2010 (FCC 2010), which was challenged before the courts in 2012 (Frieden 2011). This stay of regulatory action in a general election year leaves the FCC in suspended animation in 2012 (Marsden 2010; Donahue 2010).

The EU institutions in late 2009 agreed to impose transparency and network neutrality "lite" conditions on ISPs in directives that had to be implemented in national law by May 2011. BEREC (2010) noted that legal

provisions in the directives permit greater symmetric regulation on all operators, not simply dominant actors, but asked for clarification on these measures: "Access Directive, Art 5(1) now explicitly mentions that NRAs are able to impose obligations 'on undertakings that control access to end-users to make their services interoperable.'" The wider new scope for solving interoperability disputes may be used: "The potential outcome of disputes based on the transparency obligations can provide a "credible threat" for undertakings to behave in line with those obligations, since violation may trigger the imposition of minimum quality requirements on an undertaking, in line with Art 22(3) USD."

The European Commission in 2011 consulted on the future of the Universal Service Obligation (EC 2010), which may be extended to 2 Mbps broadband (affecting member state law some years later), marking a new line in the sand in Europe for minimum service levels. That may also require commitments to offering that access to the open Internet, not a throttled, blocked, walled-garden area.

Internet Interconnection, Content Distribution Networks, and Managed Services

It is not only in the last mile or in the consumer's ISP that network neutrality may be affected by policy decisions to differentiate traffic. Internet peering (the cost-free exchange of traffic by similarly sized ISPs) has been largely replaced by paid interconnection (Faratin et al. 2008), and in 2010 a dispute between Comcast and Level 3 was claimed by the latter party to involve a network neutrality dispute disguised as an interconnection dispute (Clark, Lehr, and Bauer 2011). A European dispute between Orange and Cogent in connection with Megavideo traffic involved similar claims. (Orange is the largest network provider in France, Cogent is a multinational tier 1 Internet provider, and Megavideo is a video-hosting company that uses Cogent networks for distribution.)

The timing of the dispute as Comcast was bidding to buy the television network NBC caused some suspicion that Level 3 was leveraging the political pressure on Comcast at a critical stage of the merger review. There have also been claims that Comcast may leverage its Internet access business to stream NBC programming at a discount to nonaffiliated programming, which led to a specific merger condition prohibiting such differentiation (Frieden 2011).

Network neutrality lobbyists intervened only partially successfully in the NBC/Universal merger of 2010, the abortive AT&T/T-Mobile merger of 2011, the AT&T/Southwestern Bell and Verizon/GTE mergers of 2006, and the auction of 700 MHz frequencies of 2007. In all these cases, there were significant resources deployed by the pro– and anti–network neutrality lobbies in Washington, D.C. It is difficult to assess the importance and public support for each lobby given the intimate connections between the lobbies and the politicians on both sides of the debate.

A 2011 dispute in Canada regarding the conduct of Shaw Communications, a West Coast ISP, revived these concerns, as the company appeared to indicate that its online movie subscribers would not exceed bandwidth caps with its affiliated service as opposed to competitors such as NetFlix. Shaw put out a statement explaining that the initial marketing material was in error and that Internet streaming of its own service would contribute to the bandwidth cap, but a dedicated cable-only service would not, much as AT&T uVerse uses the same physical fiber to deliver video service and data service, the former as "managed services" and the latter as non-managed IP (Anderson 2011). The difficulty for regulators will be to identify which data are a managed service and which are the straightforward IP stream.

Further questions for regulators will include whether ISPs can provide content distribution network services to content providers in competition with third parties. CDNs such as Akamai provide a virtual ISP access service by locally caching content for content customers close to the local telephone exchange, by investing in tens of thousands of servers distributed across networks and geographies. This is sometimes described as OTT (over-the-top) video service. Google has built a very large proprietary CDN for its own traffic, notably its video YouTube service, and other large content carriers such as the BBC and Facebook may follow suit. A further question arises because these CDNs are almost entirely downloading content to customers rather than acting as peers, and therefore creating a very large traffic imbalance. As a result, we can expect to see paid interconnection increasing and peering decrease (Marsden 2010).

Current telecommunications laws typically allow for disputes between public carriers, mainly ISPs. Search engines, video hosting sites, and CDNs are not public carriers but private carriers, and therefore their relations with ISPs are regulated by contract law rather than regulators, with the latter

having no legislative mandate to affect those private parties' relations. Calls for search neutrality or regulation of CDNs may therefore be effective lobbying discussion but do not relate to current telecoms regulation (Frieden 2011).

ISP transparency regarding network management practices has been the main component of these policies, although best regulatory information practices have yet to emerge. Faulhaber (2010) has suggested four basic principles based on examination of other industries' information regulation: "(1) disclose all information relevant to customer choice, 2) to which customers have easy access, 3) clearly and simply, and 4) in a way that is verifiable" (738). Stronger consumer confidence could be built if information was cross-compared by an accredited independent third party that is not reliant on broadband industry funding, such as a consumer protection agency. This could be carried out at arm's length by a self- or coregulatory agreement (BEREC 2011; Marsden 2012).

The FCC and European Commission position is that only "reasonable network management" should be permitted and that end users should be given clear information on this reasonableness (Faulhaber 2010). Both have relied on nonbinding declarations to make clear their intention to regulate the reasonableness of traffic management practices. The Canadian Radio-Television and Telecommunications Commission has relied on inquiries (to the dissatisfaction of consumer advocates). Norway (Norwegian Code 2009) and Japan have nonbinding self-regulatory declarations that thus far have not been enforced. In 2011, Singapore instituted a network neutrality requirement that ISPs do not block third-party applications, which is also the subject of the law passed in the Netherlands in March 2012 (Marsden 2012).

Wireless Network Neutrality

Wireless (in European terms, mobile) is a particular concern for network neutrality, and it was controversy over blocking by a mobile operator that led to the Netherlands law. Mobile remains a poor substitute for the fixed Internet (Noam 2011), and mobile smart phone users in 2010 downloaded only an average of 79 megabytes per month (Cisco 2011). Mobile is a trivial proportion of overall Internet traffic by volume, but it commands massive premiums over fixed traffic for the services provided. Cairncross (1997) explored how switched voice telephony was being replaced

by VoIP, the new technology that offered extraordinary efficiencies for both voice and data. In 2000, European governments auctioned off spectrum for that IP traffic to be carried by the extraordinarily profitable mobile oligopolies that had achieved spectacular growth in the 1990s. In 2010, 1 percent of all IP traffic was carried over mobile networks. A substantial part of mobile traffic is intended in the future to be handed off to femtocells (a small, low-power cellular base station typically found in households or work premises rather than in public networks), WiFi cells, and other fixed wireless infrastructure, piggybacking on the relatively stable and mature fixed Internet that is expanding at approximately its historical growth rate of 50 percent annually to meet capacity (Cisco 2011). Despite this empirical evidence to the contrary, a cliché in network neutrality discussions is the "explosive growth" of the Internet (Cooper, Soppera, and Jacquet 2011).

Regulations passed in licensing mobile spectrum can affect network neutrality at a fundamental level. Interoperability requirements can form a basis for action where an ISP blocks an application. Furthermore, wireless ISPs may be required to provide open access, as in the FCC auction of 700 MHz upper block C frequencies—used for 4G cellular data and worth almost $5 billion at auction—in 2008 (Rosston and Topper 2010) or in more general common carriage requirements traditionally imposed on public networks since before the dawn of modern communications, with railways and telegraphs. The FCC (2010) specifically asked for answers to regulation of managed specialized services and wireless network neutrality in 2010, and it announced that it was prepared not to enforce its proposed regulation on wireless services in the near future (FCC 2010). This means that the faster-growing and more competitive U.S. market will be less regulated than the more sluggish and less competitive European market.

European telecommunications regulators group BEREC explained, "Mobile network access may need the ability to limit the overall capacity consumption per user in certain circumstances (more than fixed network access with high bandwidth resources) and as this does not involve selective treatment of content it does not, in principle, raise network neutrality concerns" (2010, 11). It explains that though mobile will always need greater traffic management than fixed ("traffic management for mobile accesses is more challenging"), symmetrical regulation must be maintained to ensure technological neutrality: "There are not enough arguments to

Table 7.4
Outcomes and divergences

Transparency	Refusal to create transparency a critical element in early U.S. cases. European work on creating greater transparency through regulation.
Enforcement	Network neutrality "lite" solutions to prevent protocol, application blocking so far limited to statute in Netherlands, and regulatory declarations (e.g., in Canada, the United States). Bandwidth or service plan capping resulted.
Interoperability	Vendor off-the-shelf solutions adapted to ISP but little transparency on policy.
Efficiency	Coregulation often suggested as best option, with full transparency and ability for users to switch, accompanied by code solutions.

support having a different approach on network neutrality in the fixed and mobile networks. And especially future-oriented approach for network neutrality should not include differentiation between different types of the networks." It concludes that mobile should be subject to the network neutrality "lite" provisions available under Directives EC/136/2009 and EC/140/2009, listing some breaches of neutrality: "blocking of VoIP in mobile networks occurred in Austria, Croatia, Germany, Italy, the Netherlands, Portugal, Romania and Switzerland" (3). Reding (2012, para. 4) stated, "This 'Internet freedom provision' represents a great victory." Commentators are not convinced that the 2009 law on network neutrality was being effectively implemented (Marsden 2012; European Data Protection Supervisor 2011).

Table 7.4 shows the outcomes and divergences of the policy process.

The Future of Network Neutrality and the Open Internet

The pace of change in the relation between architecture and content on the Internet requires continuous improvement in the regulator's research and technological training. Regulators can monitor both commercial transactions and traffic shaping by ISPs to detect potentially abusive discrimination. An ex ante requirement to demonstrate internal network metrics to content provider customers and consumers because of a regulatory or coregulatory reporting requirement may be a practical solution. The need for better research toward understanding the nature of congestion

problems on the Internet and their effect on content and innovation is clear (Marsden 2012).

Chapter 6 showed us how the state security apparatus has co-opted private actors, notably ISPs, to enable it to carry out surveillance of the entire civilian population and to counter the twin bogeymen of content censorship: pedophilia (which is better pursued by arresting abusers) and "glorification of terrorism" (ditto). In this chapter, we saw how ISPs have taken those technologies of control to throttle content requested by their own users, which competes with their own or affiliated content. This is done to extract greater profits from users and content providers and to slow Internet growth to more manageable levels. This will have a substantial—if unmeasurable—effect on the freedom to innovate for start-up entrepreneurs. We also saw in chapter 4 that copyright industries have used the state and private control technologies to attempt to stem the flow of material shared freely online.

The security-industrial complex is now a substantial industry in advanced economies, with significant legal and less legal export potential to dictatorial regimes. Its technologies of control and lobbying power, the latter largely obscured from public gaze, can only increase over the coming decade, a serious threat to individual human freedoms on the Internet.