Office of Communications (Ofcom) (2009). *Delivering Superfast Broadband in the UK: Regulatory Statement.*

Sharkey, W. W. (2002). 'Representation of Technology and Production', in M. Cave, S. Majumbar, and I. Vogelsang (eds.), *Handbook of Telecommunications Economics, Vol. 1*, Amsterdam: Elsevier.

Ure, J. (ed.) (2008). *Telecommunications Development in Asia*, Hong Kong: Hong Kong University Press.

Wellenius, B. (2008). 'Towards Universal Service: Issues, Good Practice and Challenges', in J. Ure (ed.), *Telecommunications Development in Asia*, Hong Kong: Hong Kong University Press.

Whish, R. (2008). *Competition Law* (6th edn.), Oxford: Oxford University Press.

CHAPTER 21

REGULATION OF CYBERSPACE

JÜRGEN FEICK
RAYMUND WERLE

21.1 Introduction

In February 1996, John Perry Barlow, one of the founders of the Electronic Frontier Foundation, released on the Web what he called 'A Declaration of the Independence of Cyberspace'.[1] The declaration was quickly published on numerous websites and is still available on many of them. Barlow's declaration was a reaction to the passing of the US Telecommunications Reform Act and specifically to its Title V, the Communications Decency Act—a governmental attempt to regulate (indecent) content on the Internet. In the declaration he rejects any form of regulation imposed by governments or other outside forces as they would undermine 'freedom and self-determination', and therefore be detrimental to Cyberspace. Only the 'Golden Rule' of reciprocity (treat others as you would like to be treated) should be generally recognised, according to the declaration.

A mere three years after Barlow's plea for an unregulated or self-regulated Internet, Harvard law professor Lawrence Lessig coined his famous 'Code is Law' metaphor (Lessig, 1999). Borrowing from Joel Reidenberg's 'Lex Informatica' (1998), Lessig argued that not only governments but also firms and people regulate the Internet. Thus, instead of being dominated by laws and ordinances, the Internet

is largely regulated by architecture or code, hardware, and software that shape Cyberspace. Those who develop and implement code determine who can use the Internet, if and how users are identified, if and how use is monitored, if and how access to information is provided and, more generally, how 'regulable' or 'unregulable' Cyberspace is.

The issue of regulation developed parallel to the increasing social, cultural, economic, and political leverage of the Internet and later Cyberspace, which has become a de facto synonym for the World Wide Web (Resnick, 1998). Concurrently, the perception of these problems has changed. Today, the question is not whether Cyberspace can be regulated, but rather what is regulated, why it is regulated, how it is regulated, and who regulates it (cf. Hofmann, 2007a). These are questions which are often raised in studies of regulation (cf. Baldwin and Cave, 1999), but the answers to these questions concerning the regulation of Cyberspace presumably differ from other regulatory domains. Not only does the Internet provide new means and tools of regulation and afford regulatory influence to actors and organisations which traditionally have been the targets of regulation, it also makes regulation (especially national regulation) by public authorities increasingly difficult or even ineffective, and futile.

Some of these aspects, concerning especially the role of government vis-à-vis private industry, civil society, or international organisations, moved into the centre of the discussions and deliberations of the 'World Summit on the Information Society' (WSIS), which was convened by the United Nations and the International Telecommunication Union. It was held in two phases, in Geneva in December 2003 and in Tunis in November 2005, and involved thousands of delegates and stakeholders from a diverse array of organisations and groups. WSIS has made the general public aware that with the Internet's reach extending worldwide, a battle over its control has arisen (cf. Dutton and Peltu, 2009). However, widespread discontent with what is regarded to be illegitimate, unilateral oversight over the Internet by the United States did not suffice to trigger consensus concerning the establishment of an international political control structure. Except for the case that WSIS unveiled the political nature of Cyberspace the only palpable result was the creation of a forum for multi-stakeholder policy dialogue: the Internet Governance Forum (IGF). The IGF meets once a year to exchange information, discuss public policy issues, make recommendations, and offer advice to stakeholders. Not surprisingly, it lacks all regulatory power, due to the unbridgeable gap between those who accept regulation only where it is necessary to safeguard the technical functioning of the network, if at all, and those who emphasise the variety of potential activities which can only flourish if order in Cyberspace is guaranteed through regulation, as pointed out by the WSIS discussions.

21.2 A Conceptual View on the Regulation of Cyberspace

Before we look at specific approaches to the regulation of Cyberspace, a few conceptual remarks are in order. In the literature, various concepts are applied in the analysis of how individual, corporate, and collective actors have induced structural and procedural developments, and usage patterns. These concepts include influence, guidance, control, steering, regulation and, especially recently, governance. Governance and regulation are often treated as synonyms, but we prefer to draw a distinction between these two concepts. Following Renate Mayntz, we regard *governance* to be the more encompassing concept, which in a sociological perspective focuses on 'different modes of action coordination—state, market, corporate hierarchy', etc.—while *regulation* refers to 'different forms of *deliberative* collective action in matters of public interest' (Mayntz, 2009: 121, 122). According to this definition, the concept of regulation goes beyond command and control concepts of the regulatory policy type (cf. King, 2007: 3–21) and focuses in a wider perspective on the development and application of public or private rules directed at specific population targets.

Regulation has an impact on technology but is also affected by it. Technological innovations alter not only the issues, objects, and circumstances but also the modes and tools of regulation, including the aspects of who is able and legitimised to regulate (Hood, 2006). It would be misleading to search for a viable unitary regulatory model operating in Cyberspace. Given the increasingly complex and rapidly changing commercial and social usage patterns of the Internet, with the World Wide Web being their trans-border platform, we cannot even expect to find a tightly-knit web of regulatory rules. Rather, we encounter patchworks of partly complementary, partly competing regulatory elements in the form of legal rules and ordinances, mandatory and voluntary technical standards and protocols, international and national contracts and agreements, and informal codes of conduct and 'netiquette' (e.g. social conventions that are meant to guide all cyber-related interactions). Also, registers of requests for comments and lists of frequently asked questions occasionally serve regulatory purposes.

The engineers' response to the technical heterogeneity and complexity of the Internet, and to the technical requirements of a potentially huge number of services and applications has been to partition functions into sub-functions and allocate them to different protocol layers of the network. The Internet protocols distinguish five layers, including the physical one. In order to structure the issue area, this technical layering approach has been adopted by several studies of Internet governance and regulation. The idea of these studies is to increase the accuracy and precision of regulation by assigning a specific regulatory measure to a specific layer

and avoiding layer-crossing (Solum and Chung, 2003; Whitt, 2004). But this technocratic approach is obviously difficult to realise because there is no unambiguous correspondence between technical functions and social action. Thus, the studies usually restrict the number of layers to three. Benkler (2006: 383–459), for instance, distinguishes a physical layer (e.g. cables), a code layer (e.g. browsers, e-mail, Internet protocols) and a content layer (e.g. videos, music, speech). Similarly, Zittrain distinguishes a physical layer, a protocol layer, and an application layer, which includes but could also be separated from a content layer (Zittrain, 2008: 63–71). Generally, the lower layers are more technical and the upper layers more social. To address our questions concerning regulation, it is sufficient to differentiate only two layers: a technical layer and a content layer. The technical layer consists of the infrastructure of Cyberspace and encompasses the basic protocols such as TCP/IP, as well as browsers, and other software used to transmit content. It also includes cables, routers, and computers. The content layer consists of the application and use of software which facilitates accessing, transmitting, filtering, or storing all types of content (cf. Lessig, 2001).

21.3 Regulation of the Technical Infrastructure

Most of the literature on Internet regulation focuses on content and conduct rather than on infrastructural issues. Even though Lessig contends that regulating infrastructure (code) means at the same time regulation through infrastructure (see also Murray, 2007), most efforts to design, develop, and shape technology are perceived as the search for the technologically best solution and thus, as a purely coordinative effort. Regulatory or more generally political implications of these efforts are ignored or not fully appreciated (cf. Elmer, 2009).

It is undisputed that the Internet was only able to grow into a global network because it had met the critical operational requirements which any decentralised set of communications systems must meet in order to function as a single cohesive system. These requirements are compatibility, identification, and interconnectivity (Pool, 1983). Compatibility facilitates the smooth interoperation of networks in technical terms and is usually achieved through conformance to technical standards. Identification is accomplished by the assignment of unique addresses (numbers or names) to all users or objects which inhabit the networks. Interconnectivity entails the commitment or obligation of the providers, or operators of networks to link their networks to one another in compliance with compatibility and identification requirements.

21.3.1 Identification

The most prominent regulatory field at the infrastructural level relates to identification and the domain name system (DNS). The allocation of an unambiguous *address* (i.e. a 32-bit string of numbers) to each host that is connected to the network is essential for the routing and transmission of data packets. The system of domain *names* visible in e-mail and WWW 'addresses' is based on this address system. But in contrast to a string of numbers, names as identifiers are human-friendly and easy to remember. Their introduction has promoted the ease of use of the network. Originally designed as a coordinative tool, the DNS—especially names in the generic top-level domain '.com'—was increasingly regarded as a valuable business resource which could be used for branding. This transformed the process of allocating domain names from an act of coordination to one of resource allocation, with potentially negative consequences for those who claim a specific domain name (e.g. trademark owners) but find this name already allocated to somebody else (e.g. a competitor).

Just at the time when the significance of the DNS problems increased and an organisation with some regulatory authority was needed to cope with these problems, the US government removed authority over the assignment of numbers and names and some other managerial functions from the Internet Assigned Names and Numbers Authority (IANA), which worked on the basis of government contracts as a comparatively autonomous kind of US government agency, and delegated it to ICANN, the Internet Corporation for Assigned Names and Numbers (Mueller, 2002). ICANN, a private, non-profit corporation incorporated in California, assumed this responsibility in 1998.[2] It was designed as a 'complex multi-stakeholder global institution based on the principles of internationalisation and privatisation of governance' (Cogburn, 2009: 405). But since its inception, it has been overseen by the US government on the basis of contracts with the Department of Commerce, while other countries' governments have been prevented from controlling ICANN. The original intention of the US government to subsequently weaken its central role in this area and grant more influence to other governments and private stakeholders did not fully materialise. Thus, on the one hand the US government delegated authority to ICANN, but on the other hand a hierarchical political element remained in this arrangement. ICANN operates in 'the shadow of the state' from which it derives its authority (Scharpf, 1997). Whether this shadow is needed is an open question (Héritier and Lehmkuhl, 2008).

ICANN has the authority to formulate and implement the substantive and procedural rules within its jurisdiction entirely on its own. This includes the power to authorise new top-level domains such as '.biz' and '.info' and the control of the operation of the so-called root servers, which keep and distribute up-to-date, authorised information about the content of the name space of the top-level

domains. The root servers are consulted as the highest instance of the domain name hierarchy if a data packet otherwise cannot find its destination. ICANN oversees the organisations which run and maintain the top-level domains (registries), including the country code top-level domains such as '.uk' or '.jp'. Registries must agree to ICANN's terms and conditions. Of particular importance is the fact that ICANN has established a dispute resolution mechanism to process conflicts over domain name allocation through approved dispute resolution service providers. ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP), which has been used to resolve thousands of disputes over the rights to domain names, is considered to be efficient and cost effective.

ICANN claims that it does not control content on the Internet, that it is unable to stop spam, and that it does not deal with access to the Internet. It stresses its role as coordinator of the Internet's naming system in order to promote the expansion and evolution of the Internet (cf. Klein, 2002). ICANN has an international board of directors which represents all parts of the world and diverse groups of stakeholders. It is open for input from various advisory committees including a governmental advisory committee. Regardless of all the efforts to keep this particular area 'politics free', criticism has focused in particular on the US's prerogative position in this example of 'regulated self-regulation' (Knill and Lehmkuhl, 2002: 53–5). Many developing countries, along with China, India, and several European countries, have argued that the current legal construction would theoretically allow the US government to 'punish' a country by blocking its country code top-level domain (cf. von Arx and Hagen, 2002). This could have far-reaching negative consequences for the economy and society in the respective country. US government interventions which stopped ICANN's process of approving the implementation of a new '.xxx' (pornography) top-level domain in 2006 appear to justify this concern (Cogburn, 2009: 405). In the shadow of hierarchical control by the US government, ICANN has gained and demonstrated regulatory authority, at least vis-à-vis the registries, when it comes to preserving the stability and integrity of the domain name system. Most stakeholders seem to accept ICANN's de facto regulatory competences in this area as long as ICANN exercises self-restraint (Pisanty, 2005: 52–8; cf. Hofmann, 2007b).

21.3.2 Compatibility

Private self-regulation on the technical layer of the Internet has a long tradition. Given the decentralised structure of the Internet, safeguarding compatibility has high priority. Ever since the US National Science Foundation decommissioned the operation of what was, until 1995, a publicly-funded academic and research network (CSTB, 1999), it has not been possible for a central authority to impose the necessary compatibility requirements (Holznagel and Werle, 2004: 22–5).

Originally, technical design and development was guided by the Internet Engineering Task Force (IETF), formed in 1986 but with roots dating back to the times of ARPANET in the early 1980s. The IETF adopted many standards, i.e. technical rules, to be implemented in the network, and it has been the guardian of the Internet's generic protocol suite TCP/IP. Participation in the IETF and its numerous working groups is open to anyone, and a broad and unrestricted discussion of proposals via electronic mailing lists is possible. Before new Internet standards are approved, two independent implementations have to be completed. The standards are adopted on the basis of consensus and published online in the so-called Request for Comments (RFC) series. Their use cannot be mandated and they are traditionally available for implementation free of charge (open voluntary standards). IETF activists have always stressed the non-hierarchical, non-bureaucratic, voluntary, and consensus-based process of standard-setting. In an IETF meeting in 1992, David Clark, one of the architects of the Internet, voiced an oft-repeated characterisation of the IETF: 'We reject kings, presidents and voting. We believe in rough consensus and running code.'[3] In this meeting, the IETF rejected the adoption of components of the Open Systems Interconnection (OSI) network protocols developed by one of the established international standardisation organisations, which at the time ignored the IETF or questioned its legitimacy (CSTB, 2001: 23–35).

The other decisive standardisation organisation focusing mainly on components and applications of the Web is the World Wide Web Consortium (W3C), founded in 1994. Virtually all Web standards that are of relevance today were developed by the W3C. Like the IETF, the W3C is a non-commercial organisation of volunteers, but in contrast to the IETF, the volunteers are organisations rather than individuals, and they are charged more than a nominal membership fee. As an international industry consortium, the W3C has about 400 member organisations—companies from the industry and service sectors as well as research and education institutions. All stakeholders who are members of the consortium have a voice in the development of W3C standards which are adopted on the basis of consensus and are also available free of charge.

Despite all the differences between the W3C and the IETF, both organisations emphasise the promotional and coordinative character of their work and the voluntary nature of their standards. Formally, no one can be compelled to comply with them. However, such a view is too narrow. Being technical *rules*, all standards carry a cognitive or normative expectation of compliance. Moreover, particularly in network industries such as telecommunications and information technology including the Internet, coordinative standards can attain a quasi-mandatory status as a consequence of network effects (Shapiro and Varian, 1999). If a standard becomes prevalent in such an industry, it may eventually lock in. This means that producers and users of a specific feature or service of the Internet may be compelled to conform to the prevailing standard and stick to it once they have

implemented it. Internet standards are rarely purely technical, but they can obscure commercial interests, political preferences, and moral evaluations at the same time that these underlying interests and choices are brought to bear (Werle and Iversen, 2006).

Thus, the work that the W3C and the IETF engage in has political and regulatory consequences. The new generation of the generic Internet protocol suite offers an impressive case in point. In 1998, the IETF published a new Internet protocol suite as a draft standard, the so-called IP version 6 (or IPv6), also known as IP Next Generation. IPv6 is regarded as a necessary means of enlarging the address space and augmenting Internet functions, including a stronger encryption sequence and the high-quality services needed for sophisticated (real time) applications. In particular, the pressing need to enlarge the address space is generally acknowledged. Internet service providers and users are running out of addresses since the prevailing protocol suite (IPv4) only provides for 4.3 billion addresses. The respective supply offered by IPv6 is virtually infinite. Apart from alleged problems of compatibility between the new protocol and the incumbent one and difficulties which always have to be coped with if users are to migrate collectively from a proven standard to a new one, IPv6 has affected diverse political and business interests (DeNardis, 2009). The US government hesitated to promote a new protocol, a transition to which would require software updates, address reconfiguration, and other costly efforts on the part of the US Internet industry and corporate users. Many in the Internet industry had received large blocks of addresses in the past or had implemented software to mitigate address shortages and therefore saw no immediate benefit in upgrading the protocol suite.

Conversely, in the wake of September 11, 2001, the Department of Defense (DoD) announced it would migrate to IPv6 by 2008, alluding to the protocol's enhanced security features. But due to doubts concerning, among other things, the legitimacy of the IETF to define and administer world standards, the DoD specified that all software and hardware purchased should have 'IPv6 capability' rather than implementation (DeNardis, 2009). In Japan, IPv6 was seen as an opportunity for the domestic information technology industry to catch up to the United States. Based on this protocol suite, an 'Internet of Things' was envisioned with embedded network interfaces and unique addresses for practically every electronic device. Large IT companies and the Japanese government agreed that reaching this goal required the transition to an IPv6 environment by 2005. Likewise, the European Union (EU) gave its support to IPv6 in a move to harmonise network standards in Europe and at the same time provide the huge increase in Internet addresses needed by its prospering mobile telecommunications industry in order to offer high-quality, secure new mobile services (Holznagel and Werle, 2004: 22–5; DeNardis, 2009).

All in all, with its IPv6 standard, the IETF triggered different and partly contradictory political and business strategies. As a result, worldwide adoption has been significantly delayed. The IETF lacks the formal legitimacy and also the resources to enforce the world-wide implementation of the new protocol suite. Here it has reached the limits of private self-regulation because even as an open, consensus-based organisation, it is unable to involve all interested or affected stakeholders in the decision-making process and to accomplish concerted action. But because governments also take diverging stances towards IPv6 as indicated above, regulation by an intergovernmental standardisation organisation such as the standards branch of the International Telecommunications Union (ITU) would very likely fail as well (cf. Schmidt and Werle, 1998).

21.3.3 Interconnectivity

In addition to combining single networks to a network of networks, the operational requirement of interconnectivity encompasses issues of access to and differentiation or fragmentation of the Internet. Unlike the operators of telephone networks and the providers of telephone services, Internet network operators and service providers are not controlled by any industry-specific interconnection regulations in most countries. In this respect, the Internet is an unregulated network.

Social and territorial differences regarding access to the Internet were one of the central concerns tackled at the above-mentioned 'World Summit on the Information Society' (WSIS). 'Digital divide' is the popular metaphor used to describe this issue. While some delegates to WSIS regarded the divide as a transitory phenomenon, others emphasised the need for funds to support the development of information and communication technologies and bridge the divide between developed and developing countries. There can be no doubt that over the last 15 years, the digital divide has been shrinking in terms of numbers of Internet users. But looking only at these numbers conceals the dynamics of the divide which includes Internet usage and usage patterns. Digital divide or digital differentiation tends to reproduce itself in the sense that with highly-innovative Internet technology, ever-newer features and services are developed which turn out to be sources of new lines of differentiation (Werle, 2005) or, as Manuel Castells—with a view to broadband connections—put it: 'As soon as one source of technological inequality seems to be diminishing, another one emerges: differential access to high-speed broadband services' (2001: 256).

Since the Internet's inception, political factors including deliberate abstention from regulation have accounted for the emergence, as well as, the mitigation of differences concerning access to and use of all features of the Internet. Network operators and service providers play an important role in this context. Most of them are private companies. They have agreed to interconnect their networks and services via network access points. Initially, the operational costs of these network access points were shared among those connected to such a point (peering). Later, peering was complemented and in some cases replaced by transit arrangements,

which obliged smaller networks to compensate larger networks for the traffic they send to them because large networks receive much more traffic from small networks than they send to them. Peering and transit arrangements are achieved through commercial negotiations. It is argued that the strong positive network externalities generated by the fast-growing Internet have provided sufficient incentive to enter into interconnection agreements on a voluntary basis. Thus, in principle, interconnection is governed through market processes and voluntary coordination.

The Internet market offers providers not only inducements to interconnect but also incentives to differentiate products into a variety of 'dedicated services' which attract specific user groups and also content providers who are willing to pay a higher price for privileged and faster access to Internet services. Conversely, network and service providers may charge different prices to different content providers for a similar service, block web sites or portals of some providers, or selectively direct users to others. This has raised concerns that the architecture of the Internet will change, losing its traditional openness, and end-to-end character (Lemley and Lessig, 2004; Zittrain, 2008). According to the end-to-end design principle, most of the network's 'intelligence' is located at its ends (servers, work stations, PCs), while the network remains comparatively 'stupid', only providing the 'pipes' through which the bits and bytes are delivered (Isenberg, 1997). In such a best-effort network it would be virtually infeasible to privilege certain providers over others. It can be disputed that the Internet has ever been that 'stupid'. In any case, several architectural changes made for the sake of secure e-commerce and a variety of other reasons have already eroded the original principles. The fragmentation of the network is no longer technologically impossible and it is particularly likely to occur where only one or two providers control local or regional markets for high-speed services.

The spectre of fragmentation has triggered—under the heading of 'network neutrality'—a debate in the US and the EU over the need for regulatory intervention partly akin to the common carrier or universal service regulation of the telephone industry through specialised regulatory agencies (cf. Frieden, 2007). Proponents argue that without regulatory control, the Internet's opportunities will be taken away from users and shifted to network and service providers in the name of efficient network management, and at the expense of the innovative potential of decentralised discretionary use. Opponents contend that market competition between providers will mitigate these problems and also encourage broadband deployment as long as antitrust enforcement agencies monitor providers' behaviour and prevent the abuse of market power. They also stress that the Internet, which up to now has been unregulated with regard to network neutrality regulation, has enabled the era of user-generated content in social networking sites and blogs, potentially breaking the hegemony of traditional content generators as the primary sources of content.

21.3.4 Coordination and regulation of technology

The emergence and development of the Internet can be described as an evolutionary process which, despite the decisive promotional role of the US government, was never guided by a master plan. Voluntary, private self-regulation coordinated the actions of the early architects of the Internet (David, 2001). This tradition has survived particularly in the area of technical standardisation. Also, the administration of the domain name system by ICANN shows strong elements of self-regulation, occasional attempts by the US government to intervene notwithstanding. Organisations such as the IETF and the W3C, and even ICANN, have gained authority and legitimacy through the successful coordination of the global expansion of the Internet, which is in the common interest of most private and public stakeholders (for a more critical view of ICANN, see Murray, 2007: 114–25). IP addresses, domain names, and Internet standards cross national borders and have global validity (cf. Bendrath *et al.*, 2007). In contrast to identification and compatibility, interconnectivity tends to be regulated by governments within the territorial confines of their authority. This description has traditionally characterised telephone regulation, which comes in national and regional variants within a liberal global telecommunications regime.

Whether the existing hybrid constellation regulating the technical infrastructure will endure for the next decade is an open question, given the rapid changes and the increasing commercial importance of the Internet. The regulatory arrangement that has emerged is criticised from two opposite camps. On one side are those who argue that there is too much regulation and propose that functions such as domain name management could be left completely to the market. Network neutrality rules are declared absolutely unnecessary and dispensable. On the other side are those who call for more regulation, particularly for more political leverage for all interested or affected states on all relevant aspects of the technical infrastructure. Intergovernmental organisations or forums might have the legitimacy and the sanctioning power to implement regulations including the new Internet protocol stack (IPv6) which still struggles for acceptance.

21.4 Regulation of Content

While the regulation of the technical infrastructure aims at shaping the general opportunities and constraints of utilising the Internet, the regulation of content touches more explicitly upon values, norms, and rules. It deals, for example, with child pornography, hate speech, and discrimination against minorities and more generally with provisions to enable (or restrain) the free flow of information. In

our understanding, it also includes the regulation of conduct. The latter relates to commercial and other electronic transactions which can be hindered through electronic deception and fraud, infringement of privacy, unsolicited content, and hostile attacks. Compared to the regulation of the infrastructure, content regulation is an extremely broad and heterogeneous policy domain in terms of the issues and actors involved.

21.4.1 Political and private regulation

Cyberspace represents a de-materialised and largely de-territorialised world which challenges national social, political, and legal cultures and traditions. In contrast to proprietary telecommunications networks, the decentralised (end-to-end) technical infrastructure of cyberspace allows for distributed creativity, peer production, and sharing, making it hard to trace and control social, economic, and political action (Benkler, 2006; Lemley and Lessig, 2004). The commercialisation of the Internet and its increasing significance as a global platform for commercial transactions of all kinds have created a pressing need for a reliable and secure environment. Central questions, not only for legal scholars, include whether existing law can be extended into cyberspace in order to provide such an environment—and upon which nation's law this should be modelled—or whether a singular body of cyber law must be developed (Sieber, 2001). Legal regulation is based first and foremost on national law. National law frequently addresses commercial, civil, or criminal action on the Internet because these actions are typically not yet strictly 'cyber'. If, however, the adjustment of existing rules to the cyber environment is necessary or new legal regulations are required, slow political rule-making procedures often reduce their effectiveness (Greenstein, 2000: 183). Traditional legal forms of regulation encounter limits which are felt ever more directly in the context of law enforcement. The validity of national law ends at a country's borders, but Internet transactions can easily cross these borders and escape from national jurisdiction. As soon as more than one political authority is affected by a transaction and the legal rules regulating this transaction differ from one country to the other, a multilateral agreement is needed to reach a common solution and enforce regulation. Only in a limited number of cases can we find internationally shared or accepted rules.

Given these problems and the Internet industry's, and users' fear of what they see as either regulatory failure or political over-regulation, private (self)regulation is often proposed as the preferred policy. Self-regulation originally emerged in areas such as standard-setting and protocol development (see above). But even so-called netiquette had *inter alia* a regulatory purpose, aiming to secure freedom of speech and the free flow of information (Werle, 2002). From there self-regulation diffused into commercial and other areas where profits and specific interests, along with moral values, are at stake.

21.4.2 Areas of content regulation

Everything that happens on the Internet has to do with content, but what is actually targeted through rules and regulations is behaviour or conduct, and its effects. In the following we will briefly review a limited selection of areas and examples of Internet activities, and what they mean for the setting and enforcement of rules, regulation, and control. This review cannot be comprehensive, but it comprises issues such as data protection and privacy; intellectual property and copyright; Wikipedia as an example of Web 2.0 peer production; protection against fraud and the creation of trust in e-commerce with eBay as an example; and finally the protection of specific symbolic values (content control) and of specific groups (child/adolescent pornography).

21.4.3 Privacy and data protection

This issue is not new, but it originally gained prominence and urgency with the computerisation of private organisations and public administrations starting in the 1960s. It was aggravated by the Internet's enormous capacity to collect, store, share, and distribute personal data. Data protection includes protection not only against theft and misuse, but also against their conscious or unconscious distortion by public and private institutions. The right to control the dissemination of one's personal information and to know who possesses which information on which legal grounds has the status of a human right in many liberal democracies. But this does not mean that a common understanding of privacy prevails. Rather, the tension between privacy and other rights or concerns such as freedom of information, freedom of speech, and collective security is balanced differently in different countries (cf. Bennett and Raab, 2006; CSTB, 2001: chapter 6). While in the US, freedom of speech is generally valued more highly than privacy, this is different in many European countries where legal provisions concerning privacy and data protection are more comprehensive and elaborate. In authoritarian countries like China, system security and political and social stability are more important for the government than the protection of privacy or the freedom of speech (Wu, 2008; Kluver, 2005). These differences are the result of policy choices which rest on cultural, political, and juridical legacies. Even in the EU, one of whose basic political and economic aims is to harmonise national legislation, it took more than 20 years of political negotiations and lobbying for two EU Directives and one EU Regulation regarding the governance of Cyberspace to be put into force, in the mid-1990s (Newman, 2008).

Differences in privacy and data protection between countries can have detrimental effects on international trade. This is especially the case if one country or group of countries—in this case the EU—legally requires foreign companies and countries to respect and enforce the level of protection guaranteed on the partner's

territory. Business itself relies to some degree on the provision of adequate protection in e-commerce, where trust and the reputation of trustworthiness must be actively achieved—either through self-regulation or public policies (Marcus *et al.*, 2007). But, first and foremost, national and not foreign regulation is relevant in the countries concerned, and difficulties arise if regulations abroad are substantially different. Two agreements between the US and the EU are not only of illustrative importance in this respect: The Safe Harbor Agreement and an agreement concerning the transmission to and storage by US security administrations of personal passenger data (PNR data) collected by airlines flying to the US (Farrell, 2003; Busch, 2006). In both cases, the interest behind these treaties was mainly economic, but legally they were the result of stipulations in the EU Directives meant to protect the privacy and data of EU citizens. Legal harmonisation between the US and the EU was not an option. As the two legal cultures were too incompatible, bilateral international treaties have been the solution. Each side accepted the other's legal framework and reassured the other that they essentially fulfilled that side's regulatory requirements—in EU policy terms, mutual recognition agreements. In both cases, the assurance had to come from the US, which had lower privacy and data protection standards and less comprehensive regulations. In addition, the US generally relied on a self-regulatory model of protection more than the EU (Haufler, 2001: chapter 4). In the first case, the Safe Harbor Agreement, it was the US side which made the concessions; in the second case it was the EU which compromised substantially on privacy and data protection standards. Whether the agreements were reached because of deliberative persuasion, as the constructivist position maintains (Farrell, 2003), or were the result of clear economic interests and the negotiation leverage behind them (Busch, 2006) is a matter of dispute. In any case, the result of these processes is a piece of international regulation comprising elements of self-regulation that are based on bilateral treaties signed by political authorities.

Some scholars argue that the Safe Harbor Agreement has been a model, among others, for other international agreements as well as less-legalised measures that facilitated the spread of relatively strong privacy standards and fair information principles (Bennett and Raab, 2006). Other factors that contributed to this development include the OECD Privacy Principles, adopted as recommendations in 1998 (cf. Farrell, 2006) and the occurrence of several data breaches and other scandals which raised public consciousness in these matters. These mobilised civil society groups, who not only put pressure on governments and companies but also developed software to enable users to protect themselves (cf. Holznagel and Werle, 2004). An encompassing global regulatory regime regarding privacy and data protection has not evolved, though, and this is unlikely to happen. Thus, for some observers, self-help strategies are the only viable route to protection (Johnson, Crawford, and Palfrey, 2004). In their view, the importance of self-protective measures is reinforced through the emergence of so-called Web 2.0

peer-to-peer applications including social networking sites of the Facebook type (Zittrain, 2008: 205–16).

21.4.4 Intellectual property protection

The Internet and Web space as a storage device have fundamentally transformed the availability, reproducibility, and circulation of immaterial goods. Production cost and even more so distribution cost decreased enormously. New ways of using and distributing particularly music have emerged (Lessig, 2004). The ease with which digital content can be copied and transmitted has fomented the creation of file sharing networks which argue that free and equal access to music and other cultural goods is a human right which should not be sacrificed for the sake of profits. The traditional copyright industry has seen these developments as a threat and responded with lawsuits and antipiracy campaigns targeting file sharing platforms such as Napster, Kazaa, and Grokster (Dobusch and Quack, 2008), and most recently, The Pirate Bay in 2009. The entertainment industry argues that monetary incentives are needed to stimulate creativity and innovation.

From a socio-cultural perspective, the new technological opportunities have triggered a clash of conflicting values, norms, and ideas concerning the meaning of culture, cultural production, and cultural consumption. Although—backed by most governments of industrialised countries—legal intellectual property protection has been extended and strengthened at the international level, file sharing in ever newer variations cannot be inhibited. On the other side, industry has also reinforced its efforts to deploy protection technologies intended to stop unauthorised copying. This marked only the starting point of a kind of arms race between technological developments which facilitate the circumvention of copy protection and usage control, and innovations, especially digital rights management software, which allow the industry to determine technically the conditions of use of digital products (Goldsmith and Wu, 2006). At the same time, this unresolved arms race indicates that technological self-protection reaches its limits when and if it cannot rely on societal consensus.

21.4.5 Peer production

Wikipedia, 'the free online encyclopedia that everyone can edit' (Zittrain, 2008: 130), impressively shows what the Internet can achieve by way of decentralised peer production. Doing away with real world power differentials concerning the provision and use of this service, Wikipedia appears as a counter model to the incumbent information industry (Benkler, 2006: 70–1). The initial idealistic concept, formulated by its founder Jimmy Wales, rests on a 'trust-your-neighbour' attitude.

Confidence in the discursive and self-correcting capacities of this open participatory system has guided the development of a service with a minimal set of rules prospering without external control.

A closer look reveals that Wikipedia's success rests on self-regulation and an internal hierarchy of influence. Furthermore, one of the general rules stipulates that users must respect the legal environment and avoid legal disputes. Wikipedia content should not, for instance, infringe on copyrights, and infringing material must be eliminated immediately (Zittrain, 2008: 130–6). As the service grew in size, rules became tighter and more constraining. They address a variety of problems which jeopardise the substantive goal of the enterprise: to provide a comprehensive, up-to-date, and reliable encyclopedia. The problems include vandalism, libellous content, misuse of biographical information and attempts to strategically utilise Wikipedia for political or commercial purposes. A recent rule requires that any changes to pages about living people must be approved by one of the site's editors or trusted users before they can be released to the general public. If new rules are to be established, they are discussed as openly as the content of entries in the encyclopedia.

The guiding rule for all discussions is that participants should try to achieve consensus. If this does not work, voting is an option. Generally, Wikipedia follows procrastination and subsidiarity principles. Over the years, an internal hierarchy has developed, ready to step in if decentralised problem solving fails. Administrators can block content and prevent users from editing. Ultimately, administrators report to an elected arbitration committee, the board of Wikipedia's parent, the Wikimedia Foundation, or to the 'God-king' Jimmy Wales himself (Zittrain, 2008: 135–41).

Wikipedia seems to be the prototype of a self-regulated, community-based cyberspace organisation. But this is only half of the truth. It exists and flourishes in a real-world legal environment that must be respected if external intervention is to be avoided. This also holds for the increasing number of language-related sub-communities which organise themselves rather autonomously, again painstakingly respecting external legal constraints.

21.4.6 E-Commerce

The Internet is of increasing importance for economic transactions. As a fast border-crossing technology, it facilitates communication processes which lead to or accompany commercial transactions, most of which are finally executed off-line. As far as digital products are concerned, e-commerce can also be a full-circle online activity. Commercial interaction via the Internet can save transaction costs and increase the frequency and territorial spread of business contacts. But it also has certain drawbacks and poses certain challenges. A crucial one, especially in international commerce, is ensuring that business is done safely and in a secure way over

the Internet, as a precondition for the establishment of trust in business-to-business and, more so, business-to-consumer relations. Commercial contacts can be established in seconds and contracts concluded with a simple click, providing ample opportunities for new forms of crime. Internet crime includes several types of non-fraudulent action, but by far the largest portion of cybercrime is committed in e-commerce. Hierarchical legal regulation is indispensable in the fight against cybercrime. Some regulations are already in place, but they are usually national and they differ substantially from one country to another. Only in a limited number of cases can we find internationally shared or accepted rules. A global criminal-law response with harmonised Internet-specific regulations is unrealistic due to widely differing social, political, and legal cultures (Sieber, 2006).

As a consequence, e-commerce had to develop mechanisms of self-regulation and self-help to create trust, and thereby facilitate commercial transactions. eBay, the online platform for auctions, provides an instructive example. eBay has established an online market between seller and bidder. It charges a fee if exchanges are accomplished. The service started small as a self-regulating community and grew within a few years into a large and highly profitable business (Dingler, 2008: 7). A challenging side effect of growth has been the omnipresent threat of fraudulent behaviour on the part of sellers or buyers. In response, eBay started with a simple 'Feedback Forum' of mutual ratings and a single customer support person in 1996. Nine years later, the company had a full-time security staff of 800 which is charged with catching criminals. For this purpose, in-house monitoring and data-mining software are deployed. For seller–bidder relations, it is even more important that the initially rather simple system of mutual rating by eBay's customers has developed into a sophisticated tool, which enables them to judge the trustworthiness of their potential business partners. The system is continually improved by 'Trust & Safety' teams. It is an instrument of self-regulation that depends on the active input of eBay's customers. It leaves the evaluation of risk and the decision of whether to engage in a specific transaction to the customers, and at the same time it helps the company trace and deter, or penalise fraudulent behaviour in order to protect the integrity of the platform (Goldsmith and Wu, 2006: 136).

21.4.7 Illegal content and conduct

The labelling of content or conduct as illegal or harmful, and policies developed to protect collective symbolic values and specific groups (e.g. minors) are independent of the Internet. As in other areas, national cultural and legal rules determine their definition. Hate speech, extremist propaganda, the glorification of violence, the denial of crimes against humanity or genocide, pornographic or obscene material, etc. can be forbidden in one country and legally protected as free speech in others (CSTB, 2001: chapter 5; Holznagel, 2000). Illegal or harmful conduct

ranges from conventional cybercrimes like hacking for reasons of sabotage, identity and/or data theft to aggressive acts such as cyber shaming, stalking, or bullying which can be very harmful. What the Internet adds in impact is the exponential increase in volume, the speed of dissemination, and the potentially global spread of such content and activities. Their sheer quantity accounts for new qualitative effects on individuals, communities, and organisations. Bullying among schoolchildren, for example, has always been a harmful activity in schoolyards or other physical meeting places. Now that these activities, as well as documents negatively influencing the moral development of children have migrated to social platforms, chat-rooms, and forums in the Internet, they can easily be spread among children and at the same time hidden from the eyes and ears of parents and teachers. Perpetrators in this and other areas often use technical means to hide their identity. In many cases they can also take advantage of national differences in legal regulations and evade what they see as an unfavourable jurisdiction, fleeing into a less rigid one. This holds in particular for many of the highly profitable industries such as Internet-based pornography and gambling, which are legal in some countries and illegal in others. Their business is transnational in character, serving customers and clients, or including participants worldwide.

It is likely that industry self-regulation and codes of conduct in social networks, alone or in conjunction with self-protective measures taken by individual users, fail to fend off undesirable or illegal content and conduct. Therefore, these non-legal forms of regulation are no—or no complete—alternative to legal regulation, which is usually on a national basis and which must be enforced by national authorities. The limits of enforcement in a network that easily crosses borders are obvious. A promising response to these limits would be the international harmonisation of regulation. But here the above-mentioned differing national cultural values and norms, as well as distinct legal traditions, make it extremely difficult to reach international agreements—and they are time-consuming if reached at all. Even in the case of child pornography, where a rather broad international consensus about its unacceptability exists, the European Council had to deal with tedious definitional problems (Sieber, 2006: 198–9). It took many years of negotiation before the European Convention on Cybercrime was signed. This first international treaty on crimes committed via the Internet deals with copyright infringement, computer-related fraud, child pornography, and violations of network security. It was passed in 2001 and went into effect in 2004. The US and other non-European countries signed the Convention, but it contains many exemptions and discretionary possibilities for the countries ratifying it. One cannot say that the Convention has facilitated the coordination of concerted and accountable action against crime on the part of the signatories in a substantial way.

Due to the lack of international legal harmonisation, national law enforcement agencies are still the central institutions investigating and prosecuting conduct which violates the law (Goldsmith and Wu, 2006). In the case of child pornography,

we find rather conventional regulatory approaches of a centralised command and control type. Where content regulation threatens to collide with freedom of information and freedom of speech principles, control agencies in many countries increasingly deploy filtering and blocking software—a form of censorship which is often not even noticed by the average user (Zittrain and Palfrey, 2008).

National regulators also involve service providers in their strategies of control (Goldsmith and Wu, 2006). This opens up additional opportunities to target border-crossing content denounced as illegal by national authorities. If service providers from abroad have affiliates in the respective countries, these firms can be charged with breaching national law if they do not stop unwanted content from flowing in (Frydman and Rorive, 2002). Even if it is hotly debated in many countries whether service providers are legally responsible for content which they have not created but only transmitted (with eyes closed and ears covered), regulatory agencies increasingly seek the 'cooperation' of those service providers, often on a contractual basis (cf. Deibert, 2009).

21.4.8 Varieties of content regulation

The selected areas and examples above show that cyberspace is not characterised by anarchic openness and unregulability. Rather, different national and international institutional arrangements and a large variety of intervention tools geared to specific Internet applications govern the so-called content and social layer of the Internet. Public authority and private actor responsibility often combine in hybrid arrangements. The tools of regulation range from more conventional instruments of governmental command and control policies to non-intervention and reliance on self-protection; between these two extremes are other tools such as 'soft' information and persuasion policies, comparative reporting and evaluations, and procedural regulation or regulation of self-regulation.

Although Internet activities are not as de-territorialised as one might assume, leaving territorial governments some leverage for control, border-crossing Internet activities are difficult and sometimes impossible to regulate. This is mainly due to international differences in legal and enforcement systems, but another important factor stems from technical opportunities to hide or change the identity of Internet users, which makes it difficult to trace illegal or hostile action (Brunst, 2009). International agreements which harmonise legal regulations are scarce, limited in scope and not of global reach. Only the supranational potential of the EU opens a realistic chance for legal harmonisation, even though EU efforts are also still rather limited (for a more optimistic view see Mendez, 2005). But legal harmonisation always comes at a cost, and some scholars argue that international regulatory conflict is often preferable to a strategy of harmonisation which obscures unbridgeable national differences and in effect generates only an illusion of effective

regulation (cf. Goldsmith, 2000). These potential de facto regulatory failures may reinforce the demand for self-regulatory solutions at the international level. But international agreements among firms and associations are not necessarily easier to achieve than intergovernmental treaties. They can be regarded by some affected firms as even more constraining than intergovernmental regulation because some global players may use their strong position to attempt to set the rules.

Seen from this perspective, self-protection or self-help appears to be a viable option once again. Self-regulatory arrangements which are often based on technical solutions such as filtering software and services provided by the market are favoured mainly by those who want to preserve the Internet as a space of individual liberty. Technologically designed regulation should help leave peer-to-peer communication and transaction as unhindered as possible and thereby render other forms of regulation unnecessary (Johnson, Crawford, and Palfrey, 2004). However, these approaches—as useful as they can be under appropriate circumstances—can have serious drawbacks. To be effective, they require knowledgeable users, and it is unlikely that the majority will ever be able to adequately judge all risks and possible counter-measures in a rapidly changing technological environment. Thus, Internet regulation will remain a patchwork of different regulatory approaches in continuous flux, no model being superior to any other.

21.5 Conclusion

In this chapter we have dealt with the regulation of cyberspace and its challenges. They are partly reminiscent of those in other regulatory domains, but they are also partly new. This newness is due to the opportunities which the new technologies provide to actors, opportunities which they can use in very different ways—as regulators or as regulatory targets. We have shown above that the distinction between those who regulate and those who are regulated can become blurred because public regulators increasingly, and probably more so in this regulatory domain than in others, must rely on the cooperation of regulatees or regulatory intermediaries if public intervention is to be effective. Regulation, in the wider understanding, must even be left party to end-users or providers of services, because public authorities' reach is not far or unerring enough or because effective public intervention would jeopardise the public values, e.g. civil liberties, that it is supposed to defend—at least in open societies. Therefore, an astonishing mix of governance modes and regulatory forms characterises the regulation of cyberspace. This includes a rather high degree of self-regulatory arrangements which might be 'state-free' but, nevertheless, can imply strongly constraining rules and also provide unequal levels of protection.

We have not dealt, or if so only superficially, with possible effects cyberspace regulation might have on other regulatory domains. This is a very complex subject which would deserve a discussion of its own. Therefore, just a few remarks: In health care regulation, for example, some countries prohibit advertisement for prescription drugs to the general public. Whatever the rationale for this regulation, the Internet's in this case de-territorialising effect renders such regulation practically unenforceable. The pharmaceutical industry, and in fact any other actor, can now target potential patients directly from abroad and confront them with information, or commercial propaganda, which is completely opaque, and which can put enormous, publicly objectionable pressure on health care providers. This is only a marginal example indicating the important opportunities which this technology provides for territorial law evasion. This technology also facilitates what one might call identity evasion, i.e. hiding behind anonymity. If we consider, additionally, the speed with which communicative interactions occur, the speed with which the locations and addresses of senders can be changed, and the masses of people who can be reached at the same time, then the problems which law enforcement authorities face are evident—especially as enforcement administrations are mostly nationally confined. We have discussed some of these problems above with respect to the protection of minors, for example.

Of course, modern information and communication technologies are also tools in the hands of regulators. The detection of exchange networks for child pornography would not have been possible without the respective technology and technically able personnel. In areas such as cyber crime, there is a technical 'arms race' going on between rule enforcers and rule evaders. As we have discussed in the preceding paragraphs, law making procedures and law enforcement institutions are relatively slow—not only in comparison to the dynamics of the technological development but also with respect to the technological capacities of potential wrongdoers. Law enforcement needs not be successful in one hundred percent of cases to be effective. Nevertheless, cyberspace technologies can seriously reduce the chances of effective law enforcement.

Norms, rules, and regulations governing this complex and dynamic space are influenced by a variety of factors and forces. From the perspective of the policy process and of political influence, the specificities of perceived problem situations and the availability of technological options, as well as cultural, institutional, and policy legacies are shaping the discourse and political competition of stakeholders, policy makers, and concerned or interested parties. All of them are trying to influence developments in cyberspace on the basis of their interests and preferences, utilising the unequally-distributed power resources which are available to them. Demand and the active involvement of end-users—however imperfect the respective markets might be—are also not a negligible factor of influence. All this takes place in an internationalised environment, a fact which further complicates

rule making and rule enforcement. In the end it is a 'battle over the institutional ecology of the digital development' (Benkler, 2006, chapter 11), whose outcome will be the result not of rational planning or rational strategic games but of complex, largely unforeseeable interactions of mutually amplifying and countervailing forces.

Notes

1. http://homes.eff.org/~barlow/Declaration-Final.html
2. http://www.icann.org.
3. See 'The Tao of IETF' at http://www.ietf.org.tao.html.

References

Baldwin, R. & Cave, M. (1999). *Understanding Regulation; Theory, Strategy and Practice*, Oxford: Oxford University Press.

Bendrath, R., Hofmann, J., Leib, V., Mayer, P., & Zürn, M. (2007). 'Governing the Internet: The Quest for Legitimacy and Effective Rules', in A. Hurrelmann, S. Leibfried, K. Martens and P. Mayer (eds.), *Transforming the Golden-Age Nation State*, Houndmills: Palgrave Macmillan.

Benkler, Y. (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*, New Haven and London: Yale University Press.

Bennett, C. J. & Raab, C. D. (2006). *The Governance of Privacy. Policy Instruments in Global Perspective*, Cambridge, MA: MIT Press.

Brunst, P. (2009). *Anonymität im Internet*, Berlin: Duncker & Humblot.

Busch, A. (2006). 'From Safe Harbour to the Rough Sea? Privacy Disputes Across the Atlantic', *SCRIPT-ed*, 3(4): 304–21.

Castells, M. (2001). *The Internet Galaxy*, Oxford: Oxford University Press.

Cogburn, D. L. (2009). 'Enabling Effective Multi-Stakeholder Participation in Global Internet Governance through Accessible Cyber-Infrastructure', in A. Chadwick and P. N. Howard (eds.), *Routledge Handbook of Internet Politics*, London and New York: Routledge.

Computer Science and Telecommunications Board (CSTB) (1999). *Funding a Revolution: Government Support for Computing Research*, Washington, DC: National Academy Press.

——(2001). *Global Networks and Local Values: A Comparative Look at Germany and the United States*, Washington, DC: National Academy Press.

David, P. (2001). 'The Evolving Accidental Information Super-Highway', *Oxford Review of Economic Policy*, 17(2): 159–87.

Deibert, R. J. (2009). 'The Geopolitics of Internet Control. Censorship, Sovereignty, and Cyberspace', in A. Chadwick and P. N. Howard (eds.), *Routledge Handbook of Internet Politics*, London and New York: Routledge.

DeNardis, L. (2009). *Protocol Politics. The Globalisation of Internet Governance*, Cambridge, MA: The MIT Press.

Dingler, A. (2008). *Betrug bei Online-Auktionen*, Aachen: Shaker Verlag.

Dobusch, L. & Quack, S. (2008). *Epistemic Communities and Social Movements. Transnational Dynamics in the Case of Creative Commons*, MPIfG Discussion Paper 08/8, Cologne: Max Planck Institute for the Study of Societies.

Dutton, W. H. & Peltu, M. (2009). 'The New Politics of the Internet. Multi-Stakeholder Policy-Making and the Internet Technocracy', in A. Chadwick and P. N. Howard (eds.), *Routledge Handbook of Internet Politics*, London and New York: Routledge.

Elmer, G. (2009). 'Exclusionary Rules? The Politics of Protocols', in A. Chadwick and P. N. Howard (eds.), *Routledge Handbook of Internet Politics*, London and New York: Routledge.

Farrell, H. (2003). 'Constructing the International Foundations of E-Commerce—The EU–U.S. Safe Harbour Arrangement', *International Organisation*, 57(2): 277–306.

——(2006). 'Regulating Information Flows: States, Private Actors, and E-Commerce', *Annual Review of Political Science*, 9: 353–74.

Frieden, R. (2007). 'A Primer on Network Neutrality', Working Paper, University Park, PA: Pennsylvania State University—College of Communications.

Frydman, B. & I. Rorive (2002). 'Regulating Internet Content through Intermediaries', *Zeitschrift für Rechtssoziologie*, 23(1): 41–59.

Goldsmith, J. (2000). 'The Internet, Conflicts of Regulation, and International Harmonisation', in C. Engel and K. H. Keller (eds.), *Governance of Global Networks in the Light of Differing Local Values*, Baden-Baden: Nomos.

——& Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press.

Greenstein, S. (2000). 'Commercialisation of the Internet: The Interaction of Public Policy and Private Choices or Why Introducing the Market Worked so Well', in A. B. Jaffe, J. Lerner, and S. Stern (eds.), *Innovation Policy and the Economy 1*, Cambridge, MA: The MIT Press.

Haufler, V. (2001). *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*, Washington, DC: Carnegie Endowment for International Peace.

Héritier, A. & Lehmkuhl, D. (2008). 'Introduction: The Shadow of Hierarchy and New Modes of Governance', *Journal of Public Policy*, 28(1): 1–17.

Hofmann, J. (2007a). 'Internet Governance: A Regulative Idea in Flux', in R. K. J. Bandamutha (ed.), *Internet Governance: An Introduction*, Hyderabad: The Icfai University Press.

——(2007b). 'Internet Corporation for Assigned Names and Numbers (ICANN)', *Global Information Society Watch*, 39–47.

Holznagel, B. (2000). 'Responsibility for Harmful and Illegal Content as well as Free Speech on the Internet in the United States of America and Germany', in C. Engel and K. H. Keller (eds.), *Governance of Global Networks in the Light of Differing Local Values*, Baden-Baden: Nomos.

——& R. Werle (2004). 'Sectors and Strategies of Global Communications Regulation', *Knowledge, Technology & Policy*, 17(2): 19–37.

Hood, C. (2006). 'The Tools of Government in the Information Age', in M. Moran, M. Rein, and R. E. Goodin (eds.), *The Oxford Handbook of Public Policy*, Oxford: Oxford University Press.

Isenberg, D. (1997). 'Rise of the Stupid Network'. <http://www.hyperorg.com/misc/stupidnet.html>.

JOHNSON, D. R., CRAWFORD, S. P. & PALFREY, J. G. (2004). 'The Accountable Internet: Peer Production of Internet Governance', *Virginia Journal of Law & Technology*, 9(9): 1–33.

KING, R. (2007). *The Regulatory State in an Age of Governance. Soft Words and Big Sticks*, Houndmills: Palgrave Macmillan.

KLEIN, H. (2002). 'ICANN and Internet Governance: Leveraging Technical Coordination to Realise Global Public Policy', *The Information Society*, 18(3): 193–207.

KLUVER, R. (2005). 'The Architecture of Control: A Chinese Strategy for e-Governance', *Journal of Public Policy*, 25: 75–97.

KNILL, C. & LEHMKUHL, D. (2002). 'Private Actors and the State: Internationalisation and Changing Patterns of Governance', *Governance*, 15(1): 41–63.

LEMLEY, M. A. & LESSIG, L. (2004). 'The End of End-To-End. Preserving the Architecture of the Internet in the Broadband Era', in M. N. Cooper (ed.), *Open Architecture as Communications Policy*, Stanford: Centre for Internet and Society.

LESSIG, L. (1999). *CODE and Other Laws of Cyberspace*, New York: Basic Books.

——(2001). *The Future of Ideas. The Fate of the Commons in a Connected World*, New York: Random House.

——(2004). *Free Culture. How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, New York: Penguin Press.

MARCUS, J. S. *et al.* (2007). *Comparison of Privacy and Trust Policies in the Area of Electronic Communication*, Bad Honnef: wik-Consult; Cambridge: RAND Europe.

MAYNTZ, R. (2009). 'The Changing Governance of Large Technical Infrastructure Systems', in R. Mayntz (ed.), *Über Governance: Institutionen und Prozesse politischer Regelung*, Frankfurt: Campus Verlag.

MENDEZ, F. (2005). 'The European Union and Cybercrime: Insights from Comparative Federalism', *Journal of European Public Policy*, 12: 509–27.

MUELLER, M. C. (2002). *Ruling the Root: Internet Govenance and the Taming of Cyberspace*, Cambridge, MA: The MIT Press.

MURRAY, A. D. (2007). *The Regulation of Cyberspace. Control in the Online Environment*, Abingdon: Routledge-Cavendish.

NEWMAN, A. L. (2008). 'Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive', *International Organisation*, 62(1): 103–30.

PISANTY, A. (2005). 'Internet Names and Numbers in WGIG and WSIS: Perils and Pitfalls', in W. J. Drake (ed.), *Reforming Internet Governance*, New York: The United Nations Information and Communication Technologies Task Force.

POOL, I. (1983). *Technologies of Freedom*, Cambridge, MA: Belknap Press.

REIDENBERG, J. R. (1998). 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', *Texas Law Review*, 76(3): 553–84.

RESNICK, D. (1998). 'Politics on the Internet: The Normalisation of Cyberspace', in C. Toulouse and T. W. Luke (eds.), *The Politics of Cyberspace*, New York and London: Routledge.

SCHARPF, F. W. (1997). *Games Real Actors Play: Actor-Centered Institutionalism in Policy Research*, Boulder, CO: Westview Press.

SCHMIDT, S. K. & WERLE, R. (1998). *Coordinating Technology: Studies in the International Standardisation of Telecommunications*, Cambridge, MA: The MIT Press.

SHAPIRO, C. & VARIAN, H. R. (1999). *Information Rules: A Strategic Guide to the Network Economy*, Boston, MA: Harvard Business School Press.

SIEBER, U. (2001). 'The Emergence of Information Law: Object and Characteristics of a New Legal Area', in E. Lederman and R. Shapira (eds.), *Law, Information and Information Technology*, The Hague and London: Kluwer Law International.

——(2006). 'Cybercrime and Jurisdiction in Germany', in: B. J. Koops & S. W. Brenner (eds.), *Cybercrime and Jurisdiction: A Global Survey*, The Hague: TMC Asser Press.

SOLUM, L. & CHUNG, M. (2003). 'The Layers Principle: Internet Architecture and the Law', Loyola-LA Public Law Research Paper No. 15. <http://ssrn.com/abstract=416263>.

VON ARX, K. G. & HAGEN, G. R. (2002). 'Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control', *The Richmond Journal of Law and Technology*, 9(1): 1–26.

WERLE, R. (2002). 'Internet and Culture: The Dynamics of Interdependence', in G. Banse, A. Grunwald, and M. Rader (eds.), *Innovations for an e-Society: Challenges for Technology Assessment*, Berlin: edition sigma.

——(2005). 'The Dynamics of Digital Divide', in A. Bammé, G. Getzinger, and B. Wieser (eds.), *Yearbook 2005 of the Institute for Advanced Studies on Science, Technology & Society*, München and Wien: Profil Verlag.

——& IVERSEN, E. J. (2006). 'Promoting Legitimacy in Technical Standardisation', *Science, Technology & Innovation Studies*, 2(1): 19–39. <http://www.sti-studies.de/articles/2006-01/werle-iversen/Werle-Iversen-180306.pdf>.

WHITT, R. S. (2004). 'Formulating a New Public Policy Framework Based on the Network Layers Model', in M. N. Cooper (ed.), *Open Architecture as Communications Policy*, Stanford: Centre for Internet and Society.

WU, T. (2008). 'The International Privacy Regime', in A. Chander, L. Gelman, and M. J. Radin (eds.), *Securing Privacy in the Internet Age*, Stanford: Stanford Law Books.

ZITTRAIN, J. (2008). *The Future of the Internet and How to Stop It*, New Haven: Yale University Press.

——& PALFREY, J. (2008). 'Internet Filtering: The Politics and Mechanisms of Control', in R. Deibert, J. G. Palfrey, R. Rohozinski, and G. Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: The MIT Press.

THE OXFORD HANDBOOK OF

REGULATION

Edited by

ROBERT BALDWIN

MARTIN CAVE

MARTIN LODGE

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford OX2 6DP

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide in

Oxford New York

Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in

Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trade mark of Oxford University Press
in the UK and in certain other countries

Published in the United States
by Oxford University Press Inc., New York

© Oxford University Press 2010

The moral rights of the authors have been asserted
Database right Oxford University Press (maker)

First published 2010

All rights reserved. No part of this publication may be reproduced,
stored in a retrieval system, or transmitted, in any form or by any means,
without the prior permission in writing of Oxford University Press,
or as expressly permitted by law, or under terms agreed with the appropriate
reprographics rights organization. Enquiries concerning reproduction
outside the scope of the above should be sent to the Rights Department,
Oxford University Press, at the address above

You must not circulate this book in any other binding or cover
and you must impose the same condition on any acquirer

British Library Cataloguing in Publication Data
Data available

Library of Congress Cataloging in Publication Data
Data available

Typeset by SPI Publisher Services, Pondicherry, India
Printed in Great Britain
on acid-free paper by the
MPG Books Group, Bodmin and King's Lynn

ISBN 978–0–19–956021–9

1 3 5 7 9 10 8 6 4 2

CONTENTS