Contract versus statute in Internet governance

Lee A. Bygrave


ABSTRACT

The chapter examines the respective role of contract and statute in governance of the Internet along with the reasons for each role. In doing so, it charts the interaction of each type of instrument, particularly the ways in which each is used in the other’s service and the ways in which they are in conflict. The chapter shows that contract is often preferred over statute because it enables flexible micro-management of the digital environment more easily than statute does. However, the chapter also shows that the relative roles played by each instrument are fluid and that in particular contexts statute is assuming an increasingly salient position. Nonetheless, it is argued that the prospects of any new statutory overlay being introduced which dramatically overshadows or reduces the role of contract in the field are generally slim, especially at the international level.

INTRODUCTION

This chapter is concerned with the following issue: what is the respective role of contract and statute in governance of the Internet and what are the reasons for each role? The chief catalyst for addressing the issue is the massive reliance upon contract as the principal legal means for governing much of the Internet and its virtual worlds. Coupled with this contractual predilection is fairly widespread reluctance to develop statutory measures in the field. How and why such a situation has arisen, and what its extent is, are questions worth considering, particularly given the Internet’s centrality to social, economic and political life. The importance of the questions is augmented by ongoing controversy over purported abuses of contractual power by the providers of Internet-based services (see, for example, Fairfield 2008, de Zwart 2010, Suzor 2010a and Suzor 2010b). Any useful discussion over how such abuses ought to be remedied, or over the respective utility of contract and statute more generally, should be informed by a reasonably accurate picture of the roles that contract and statute currently play. This chapter goes a considerable way to providing that picture.

The term ‘statute’ is herein used in its extended sense as denoting more than simply domestic legislation; international codes in the form of treaties, pacts and conventions are embraced as
well. Delegated legislation, such as ordinances and regulations, is embraced too. A key distinguishing feature of a statute for the purposes of this analysis is that it is formally agreed upon by national governments or government agencies acting alone or in concert. Further, a statute typically creates legal rights or obligations for a particular population without each member of the population first specifically assenting to it. Statutes tend accordingly to embody hierarchical, state-dominated power structures. Note, though, that formal differences exist between domestic and international statutes in the way they create and give effect to law. The main difference is that the rights and obligations created by an international statute—that is, a treaty or similar agreement under public international law—apply primarily to the states that are parties to the statute and will often not apply directly to, or be directly enforceable by, the populations of those states. However, the agreement may require each contracting state to transpose those rights and obligations in national law, thus making them (or elements of them) directly applicable to the populace. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe in 1981, is one of numerous instances in point: it is not intended to provide, of itself, a set of rights directly enforceable in national courts (see its Explanatory Report paragraphs 38 and 60), but requires contracting states to incorporate its principles into their national laws (Article 4(1)). Once so incorporated, those principles give rise to rights and obligations that are domestically justiciable.

In contrast to a statute, a contract may be hatched by any person or organisation (not just governments or their agencies) with the capacity to enter into legal relations, and it will only become legally binding upon a person or organisation once they specifically agree to its terms. Linked to the latter characteristic is the doctrine of privity of contract, which means that a contract normally only binds and benefits the contracting parties; a third party will thus be unable to sue on it. While inroads into the doctrine have been made in some jurisdictions, such as France (see, for example, Whittaker 1995) and England (see the UK Contracts (Rights of Third Parties) Act 1999), it remains a general point of departure in both common and civil law systems. Contracts are predominantly used in market and network modes of governance which purportedly embody flatter, less coercive forms of steering than a state-centric hierarchical mode of governance (for elaboration of these various modes as ideal types, see Meuleman 2008: 21ff, 329–350). Yet, as shown further on in this chapter, contract can also be integrated in the latter type of governance mode.

The term ‘Internet governance’ is herein used in line with the recent tendency to give it an expansive compass (see, for example, Mueller 2010: 9–10). While one may query the desirability of that expansion—not least because it compounds the risk of ‘Internet governance’ becoming a ‘weasel’ term—it is probably irreversible. How the term is defined affects assessment of the relative roles played by contract and statute. The preponderance of each type of legal instrument varies from context to context. A definition of Internet governance that forecloses account being taken of a particular context will lead to a different perception of the balance between contract and statute than a definition that does not. In days past, Internet governance was often treated as principally concerned with the setting of technical standards for data transmission networks based on the Transmission Control Protocol and Internet Protocol (TCP/IP) suite, along with the management of their naming and numbering system. As elaborated further below, statute does very little work in that context compared to contract. Nowadays, Internet governance tends to be treated as concerned with a great deal more. Indeed, some would see it as now embracing pretty much ‘the entirety of communication and information policy’ (Mueller 2010: 10). This gives statute law potentially more importance relative to contract.
At the same time, it makes clearly identifying where the relevant corpus of statute ends very difficult. The same goes for identifying the relevant corpus of contract. It means, in principle, that any statute or contract that impinges—however remotely—on provision of, or policy on, electronic communications could be seen as relevant. Adopting such a broad approach is not particularly useful for the purposes of legal categorisation. For those purposes, it seems more useful to restrict the relevant corpus of law to statute or contract which has governance of electronic communications as its central remit or which otherwise affects such governance in a significant, albeit incidental, way. That type of law accordingly forms the focus of the chapter. One could further narrow the relevant corpus of law by restricting electronic communications to those based on TCP/IP networks, but this delimitation seems to be losing popularity as such networks merge with others. Thus, the delimitation is not strictly applied herein. Account is taken of the multiple levels at which the law in point may govern or affect electronic communications. These include the infrastructure for electronic communications, the services facilitated by that infrastructure, and the resultant data flows. In terms of the latter, relevant laws may affect or seek to affect either how data flows or what kind of data flows on the basis of the information content of the data.

Some caveats are necessary at the outset. First, while essentially a work of legal scholarship, the chapter is written for a generalist (though academic) readership with a view to summing up basic regulatory patterns in the field. It accordingly passes over some (but not all!) legal intricacies in the interests of presenting the ‘big picture’.

A second caveat concerns the title of the chapter. While catchy, it is misleading insofar as it suggests that contract is necessarily at loggerheads with statute. While contract and statute can be in tension with each other, they are not intrinsically in conflict and they often work hand in hand—as illustrated further below. Moreover, many of the rules making up the law of contract are statutory. This is especially so in civil law systems where the principal rules of contract law are enshrined in the statutory law of obligations. The Civil Codes of Germany, Italy and France are prime examples in point. Yet also in common law jurisdictions large swathes of contract law that once were the preserve of the contracting parties and judiciary are now regulated by statute. For example, the UK Unfair Terms in Consumer Contracts Regulations 1999 apply mandatory rules to govern contracts between consumers and businesses; and the UK Employment Rights Act 1996 does the same for employment contracts.

Thirdly, the two types of legal instrument under investigation here are far from being the predominant tools of Internet governance. This follows partly from the very concept of Internet governance, which, as elaborated elsewhere in this book, encompasses a vast range of mechanisms for management and control—of which formal legal codes are but one instance. It follows also from the way in which the Internet is actually governed. The bulk of everyday governance is extra-legal in the sense that it occurs without direct application of legal rules. And many of the normative codes in the field are not legally binding in themselves. In other words, neither contract nor statute does the core practical work of Internet governance. Consider, for example, the Internet standards developed by the IETF: such a standard is represented as ‘not imply[ing] any attempt by the IETF to mandate its use, or any attempt to police its usage—only that “if you say that you are doing this according to this standard, do it this way”’ (RFC 3935). This is a far cry from the formal force of contract, statute or a court decision. Moreover, the IETF consciously attempts to work outside the radar screen of lawyers by, for instance, never formally verifying or making claims about the details of patent
agreements (Alvestrand 2009). This is not to say that an IETF standard or any other technical standard is incapable of gaining legal purchase. For instance, a statute might make reference to such a standard (see, for example, the EU Framework Directive on electronic communications (2002/21/EC) Article 17, which refers to certain technical standards and empowers the European Commission to mandate their implementation in particular circumstances). Alternatively, a court might find that adherence to a standard constitutes good business practice, thereby absolving a litigant from liability under a negligence claim. We must further remember that while much Internet governance is extra-legal, it occurs in the shadow of law. Legal principles also constitute necessary (though not exhaustive) benchmarks for what is legitimate governance by both private and public actors.

Fourthly, the instruments considered herein do not constitute the entirety of the legal arsenal. Most notably missing from the following analysis is in-depth consideration of the role of the judiciary (case law) and the role of customary law in Internet governance. Additionally, with its focus on contract and statute, both of which are typically cast as core constituents of ‘hard law’, the chapter does not deal in detail with the many instruments that are typically cast as ‘soft law’—namely, guidelines, declarations, recommendations, codes of practice and the like.

The division between ‘soft’ and ‘hard’ categories of law is usually depicted as a sliding scale based on several variables: obligation, delegation and precision (see, for example, Abbott and others 2000). In short, obligation concerns the degree to which an instrument is (commonly regarded as) binding. Delegation refers to the degree to which a third party, such as a court, is permitted to interpret and apply the instrument and resolve disputes over it. Precision concerns the degree to which the instrument stipulates clear, unambiguous rules. For present purposes, the latter variable is largely irrelevant to distinguishing the instruments that are the focus of this chapter from their ‘softer’ counterparts: numerous contracts and statutes are couched in vague terminology. Rather, the key variable herein is obligation: the more obligatory the instrument, the ‘harder’ it is. That criterion tends to translate into the degree to which the instrument is directly enforceable by a court (thus calling into play the delegation variable). In general, a court will be prepared to enforce contracts or statutes by providing remedies for their breach—assuming it has authority to do so. This will often not be the case with ‘soft law’ instruments. That the latter are nevertheless commonly seen as a type of law (though compare, for instance, Weber and Weber 2010: 24, who claim that such instruments are not law, only ‘a social notion close to law’) is because they are aimed at and capable of having some practical effect on conduct. Indeed, some scholars (for example, Abbott and Snidal 2000; Power and Tobin 2011) argue that their effect may often be greater than that of ‘hard law’. And, as noted above in relation to standards, they may be incorporated into ‘hard law’ or otherwise shape its application and development, through judicial, contractual or legislative processes (see, for example, Senden 2004: chs 8–11).

**THE PROVINCE OF CONTRACT**

The governance structure for the Internet has been formed largely outside a treaty or other legislative framework that is Internet-specific. Contractual mechanisms provide the legal mortar and bricks for much of the present structure, and they do so often without a direct basis in statute. Consider the Internet’s physical infrastructure, its naming and numbering system and the day-to-day provision of Internet-based services: the management of all of these elements, from their construction to their deployment, is legally regulated primarily by way of a sprawling web of contracts. Concomitantly, the governance structure is relatively
unencumbered by dirigiste ideology and has permitted a fairly high degree of self-regulation (Mifsud Bonnici 2008). While tentacles of government control are increasingly visible (Goldsmith and Wu 2006; Bygrave and Michaelsen 2009), private sector bodies have usually been allowed—and often encouraged—to lead the design and management of the Internet. Governments have acted more as facilitative partners of these bodies than as heavy-handed regulators, at least in Western democracies. In other words, governance has been largely exercised by cooperative networks rather than decree.

Contract has been utilized from the Internet’s beginnings. It was the principal legal tool used by US government agencies to fund the efforts of the scientific research community in developing the Internet and its precursor, the ARPANET (see generally Bing 2009). To be sure, the control that government thereby exercised over those efforts was distant and light-touch but it was, in legal terms, contractual at bottom. It was also capable of real bite. This was made clear when the Internet technical community attempted to gain complete control over the Internet naming and numbering system in 1997—the so-called ‘gTLD-MOU’ initiative. The Clinton-Gore Administration effectively killed the initiative by holding that its funding of Internet development under a series of contracts gave it ultimate authority over the network (Mueller 2002: 142–162; Goldsmith and Wu: 36–43).

Contract continued to be the US government’s preferred legal tool when it formulated its general regulatory approach to Internet-based commerce in the late 1990s. In ‘A Framework for Global Electronic Commerce’ (1997), the Clinton-Gore Administration stated that ‘governments should establish a predictable and simple legal environment based on a decentralized, contractual model of law rather than one based on top-down regulation’ (emphasis added).

Management of the Internet’s naming and numbering system is an important manifestation of that model. The legal relationships between the various actors involved in such management have been largely contractual. There are five main categories of contract: (i) agreements between the Internet Corporation for Assigned Names and Numbers (ICANN) and the US Department of Commerce (DOC); (ii) agreements between VeriSign (previously Network Solutions, Incorporated)) and the DOC; (iii) agreements between ICANN and other bodies—domain name registries, domain name registrars and data-escrow providers; (iv) agreements between data-escrow providers and registrars or registries; and (v) agreements between registrars and registrants of domain names (see further Bygrave and Bing 2009: ch 5, section 5.1.3).

The private law character of this governance structure is reinforced by the fact that the central international body charged with managing the naming and numbering system—ICANN—is a private, non-profit corporation registered in California. The bulk of the other involved actors are also from outside the governmental sector. This is not to say that the role of government or of public law in this context is insubstantial (more on that further below). But it is plainly very different from, say, the traditional telecommunications sector where the central international governance body is a treaty-based intergovernmental organisation—the International Telecommunications Union (ITU)—and where there has long been extensive legislative activity. Moreover, much of the law that governs the Internet naming and numbering system is formed outside the classical arenas of public international law. Its primary sources are accordingly found at the periphery of the traditional centres for law-making—namely, national parliaments and intergovernmental bodies, such as the ITU, EU, Council of Europe (COE) and World Trade Organization (WTO).
Much the same can be said for large tracts of the legal governance structure applying to other aspects of the Internet and its transactional dimensions. Contract is used extensively to regulate the building and interconnection of the myriad communications networks that constitute the Internet’s physical layer or ‘backbone’. It is also applied extensively to regulate access to that layer: consider, for example, the numerous access agreements entered into between Internet Service Providers (ISPs) and various types of end-users (persons in domestic households, corporations etc) and between ‘lower-tier’ and ‘upper-tier’ ISPs.

Additionally, contract is extensively employed to regulate the dissemination and use of data at the Internet’s application and content layers. This is most salient with data in which intellectual property rights inhere. Software is an obvious example. The distribution and use of computer programs is governed principally by contract in the form of license agreements—originally, ‘shrink-wrap’ licences for physical, off-the-shelf software packages; more recently and now more commonly, ‘click-wrap’, ‘web-wrap’ or ‘browse-wrap’ licenses for purely online software distribution.

The digital environments created by software developers are also governed principally by contract, typically in the form of End-User License Agreements (‘EULAs’). We see this exemplified particularly well with massively multiplayer online games (‘MMOGs’), such as World of Warcraft, and with other popular virtual worlds, such as Second Life. For the millions of people participating in these environments, the formal rights, obligations and benefits attaching to their participation are legally dictated primarily by the respective EULA. The latter is thus a central means of governance in such environments, performing a function akin to the constitutional law of an ordinary country. Like such law, though, the EULA is rarely the sole means of governance. It will usually be one component of a digital rights management system (DRMS)—that is, a technological-organisational infrastructure for managing online dissemination and use of data with the purported aim of protecting intellectual property rights in the data (Bekker and others 2003). The EULA rules will often be replicated and buttressed by technological measures, such as use of encryption and steganography (‘digital watermarking’). In other words, the legal code of the DRMS will be integrated with, and reinforced by, its software code (de Zwart 2010: 608 and references cited therein; on the regulatory role of software more generally, see Reidenberg 1998 and Lessig 1999).

Extensive use of contract is not unique to the field of Internet governance. Summing up recent empirical evidence from a variety of fields, Edgeworth notes that ‘[r]ights are determined increasingly by reference to private contractual agreement rather than public regulation so that contract once more, as in the 19th century, “swallows up” much of the subject matter it was seen to “disgorge”’ (Edgeworth 2003: 150). Indeed, he argues that this (re)ascendancy of contract is a hallmark of the ‘postmodern’ legal paradigm. In the field of Internet governance, though, we need to keep in mind that this development is not so much a case of contract reclaiming lost territory as claiming new.

Care ought to be taken not to overstate the extent of this conquest. If we look more closely at the above-listed contractual frameworks, we find that they tend not to be based exclusively on contract but are also under the sway of statute or various types of ‘soft law’. Although some of the latter resemble contract, they are not formally legally binding in the way that contract ordinarily is.
Governance of the Internet naming and numbering system provides pertinent illustrations of these non-contractual dimensions. To begin with, some ccTLD governance regimes have a statutory footing. Norway is a case in point (Thunem and Lange 2009). Further, the role played by contract in governing the relationships between ICANN and ccTLD managers is more modest than for the relationships between ICANN and gTLD managers. Although ICANN has pushed for the creation of formal contractual agreements between itself and ccTLD managers, few such agreements have been signed. Most ccTLD managers have preferred to formalise their relationship with ICANN by an ‘exchange of letters’. The latter mechanism has been characterised as contractual (Uerpmann-Wittzack 2008: 159 describing the exchange of letters between ICANN and the .de registry, DENIC, as a ‘contract’) but this is misleading. The parties enter into these exchanges in order to formalise their relationship in a way that avoids making them legally liable to each other. For example, ICANN’s letter of 29 March 2006 to DENIC stipulates that ‘nothing contained in this letter shall give rise to any liability, monetary or otherwise for ICANN’. This is hardly typical for an ordinary contract.

Another instrument that is hardly typical for an ordinary contract is the Affirmation of Commitments (AOC) concluded between ICANN and the DOC in late 2009 (for details, see the chapter by Michael Froomkin in this volume and Froomkin 2011). It is worth devoting some space to the legal status of this instrument, partly because it replaced an agreement that was clearly contractual (the Joint Project Agreement (JPA) of September 2006), partly because its own legal status is ambiguous, and partly because it now forms a central plank in the constitutional compact between ICANN and the DOC and, in a broader perspective, between ICANN/DOC on the one side and the rest of the world on the other. The AOC has definite contractual elements. In the first place, it is an agreement, as is made expressly clear in clauses 1 and 11 of it. And despite otherwise using the nomenclature of ‘affirmation’, both the DOC and ICANN are essentially agreeing to commit themselves to a particular course of action; the term ‘affirms’ equates with ‘agrees to remain committed to’. Secondly, both parties make promises. Although ICANN makes far more promises than the DOC, it is wrong to suggest that the latter makes none. The DOC makes at least one fairly concrete promise, which is to keep participating in and support the Governmental Advisory Committee for the ICANN Board (AOC clause 6), and it makes a vaguer promise in terms of commitment to a ‘multi-stakeholder, private sector led, bottom-up policy development model for DNS technical coordination’ (AOC clause 4). Thirdly, a credible argument can be made out that the agreement is supported by proper consideration, which is a basic prerequisite for a valid contract under US law (and other common law systems, though not civil law systems).

The matter of consideration, though, is contestable, with at least one scholar claiming that the AOC probably does not qualify as a valid contract for lack of consideration (Froomkin 2011: 199). Put somewhat simplistically, consideration is some action or thing undertaken or provided by a person (natural or legal) in exchange for, and at least partly because of, a promise by another person (for a classic exposition in terms of US law, see Farnsworth 1982: ch 2). Part of the doctrine of consideration is a rule that consideration cannot be ‘past’, which means that action undertaken prior to a promise being made cannot be valid consideration for the promise as it was not in response to the latter (see further, for example, Farnsworth 1982: 50–51). This rule seems to be the basis for the claim that the AOC is not supported by consideration. In Froomkin’s view, ICANN and the DOC are simply doing what they have previously committed to doing; thus, the AOC is not supported by fresh consideration and thereby falls foul of the rule that consideration must not be ‘past’. However, an argument can be made out that fresh consideration is provided. The argument would be that the lapse of the JPA caused a lapse of each party’s legal commitments (at least as elaborated in the JPA)
towards the other, thereby permitting each some leeway to change tack if they wanted. Through the AOC, the DOC effectively agreed not to change tack. This ‘affirmation’ of (or agreement to remain committed to) previous policy, in a situation in which the DOC was not legally required to do so, was something new and could thereby constitute fresh consideration for ICANN’s promises. And ICANN—the argument would run—provided fresh consideration for the DOC’s promises by agreeing to undertake review processes that go beyond what its Bylaws or Articles of Incorporation already required.

Yet regardless of the outcome of such an argument, any attempt to view the AOC as a valid contract faces more serious difficulties. One problem is lack of clear statutory authority enabling the DOC to bind itself, via contract, to the commitments it makes without violating US administrative and constitutional law—a similar problem has arguably afflicted the older ICANN/DOC contracts too (Froomkin 2000 and Froomkin 2002). Another difficulty concerns the agreement’s probable lack of mutual enforceability given doctrine on sovereign immunity and the vagueness of much of what each party promises. In conclusion, it would be wrong to assume that the AOC is a valid contract.

WHY CONTRACT?

The growth in reliance on contract has a complex and multifaceted aetiology. It partly reflects dissipation of faith across much of the Western liberal sphere in the efficacy of state-run ‘command and control’ regimes—a tendency particularly salient over the past three decades (see, for example, Jänicke 1990, Moran and Prosser 1994, De Vries 2011). This loss of faith applies across many sectors but is especially acute regarding governance of rapidly changing technological infrastructures, such as the Internet. Its corollary tends to be a belief in the ability of a competitive marketplace to deliver goods and services in the most appropriate manner. This gives relatively great latitude to private fiat and contractual mechanisms.

Thus, the roll out of the Internet concurrently with growing loss of faith in the efficacy of ‘top-down’ regulation contributed to relatively extensive application of contract. This result was reinforced by the network’s origins in the USA, where ‘laissez-faire’ ideology and commitment to freedom of expression have traditionally had a firmer grip on government than in many other countries. In light of that commitment, it is somewhat paradoxical that the USA was home to the first attempt to legislatively censor expression on the Internet through enactment of the federal Communications Decency Act of 1996. That attempt, however, was ultimately thwarted by the strong place given to free speech in the US Constitution as interpreted by the US Supreme Court (see its decision in American Civil Liberties Union v. Reno, 521 US 844 (1997)).

Other aspects of Internet development have also engendered reluctance to apply extensive ‘top-down’ regulatory controls on the network. The informal, open, ‘bottom-up’ decisional culture of the network’s technical pioneers—manifest most famously in their mantra of ‘rough consensus and running code’—rapidly became a benchmark for subsequent governance regimes, such as that established by ICANN (see, for instance, Froomkin 2003). Its apparent embodiment of democratic ideals together with its spectacular success in fostering innovation with broad societal benefits gave such culture a high degree of legitimacy. It thereby placed a question mark against the propriety of more formal, hierarchical regulatory approaches, thus pre-empting knee-jerk recourse to them.
At the same time, governments have generally acknowledged the immense value of the payload created by the cooperative arrangements of the Internet technical community and have been accordingly cautious about upsetting such arrangements. Indeed, one is tempted to suggest that legislators in this context—at least in the Western world—have taken heed of the lesson drawn by Ellickson in his classic account of Order without Law: ‘lawmakers who are unappreciative of the social conditions that foster informal cooperation are likely to create a world in which there is both more law and less order’ (Ellickson 1991: 286). Nonetheless, many governments have responded in relatively dirigistic fashion when the Internet has threatened them or interests that they deem important. The most heavy-handed responses have tended to come from non-Western states, with China a salient case in point (see, for example, Sohmen 2001). Yet, as highlighted further below, Western governments too have been far from averse to attempting to subject aspects of the Internet to legislative control.

The Internet itself, though, poses serious challenges to the efficacy of any state-imposed regulation. As Mueller (2010: 4–5) points out, one set of challenges arises from the global scope of Internet communication and the ‘quantum jump’ in its scale. Another challenge arises from the way in which the Internet distributes and disaggregates control. In particular, the Internet has ‘ensured that the decision-making units over network operations are no longer closely aligned with political units’. Linked to this, the Internet has given birth to new institutions: ‘[d]ecision-making authority over standards and critical Internet resources rests in the hands of a transnational network of actors that emerged organically alongside the Internet, outside of the nation-state system’. Finally, the Internet ‘changes the polity’ by facilitating ‘radical changes in collective action possibilities’.

To this list of challenges one can add more generic problems, not least the slow pace in which legislative processes usually occur and the customary difficulties of reaching meaningful intergovernmental agreement on the details of any international regulatory instrument. The latter difficulties (elaborated further below) are especially problematic when the Internet’s global reach limits the purchase of purely national regulation.

All of the above-described factors have left public law and statute struggling to gain extensive traction in the field of Internet governance. They have thereby helped to leave the field to a large extent the province of private ordering and contract. Yet it would be wrong to cast reliance on contract as simply a by-product of ‘statutory default’. Contract has been actively promoted as a preferred legal tool on account of possessing certain purported strengths. When, as noted above, the Clinton-Gore Administration advocated use of contract in its policy paper ‘A Framework for Global Electronic Commerce’ (1997), it assumed that this would create a ‘predictable, minimalist, consistent and simple legal environment for commerce’. Such assumptions are fairly commonplace. Other commonly assumed strengths of contract are the speed and flexibility with which it can usually be developed and amended, relative to statute. Some of these assumptions are contestable, others less so. For instance, the increasingly dense legalese of many EULAs along with the numerous changes they tend to undergo (Jankowich 2006 and Nino 2010), hardly make for a ‘predictable, minimalist, consistent and simple legal environment’. Broader concerns exist too about the tendency of contract to cater for a narrow range of interests (typically just those of the contracting parties or often simply those of the party who drafted the contract) at the expense of the legitimate interests of others—a matter that is elaborated further below in respect of EULAs and the balance between contract and copyright.

Still, it is difficult to deny that contract is particularly well-suited to governing the digital
Contract can be closely tailored to a particular technology and then quickly amended as the technology develops. It can operate across national jurisdictions relatively independently of them. It can be readily applied in ways that align with the market and network structures of the Internet along with changes in those structures. And it can be applied in hierarchical, ‘command and control’ modes of governance along with more heterarchical modes.

All of these capabilities are nicely illustrated by the contractual web spun for the Internet naming and numbering system. ICANN enters into a set of individual contracts with registries giving the latter rights to manage particular TLDs. The registries contract individually in turn with various registrars, which in turn individually contract with private legal or physical persons who then gain certain rights to the use of domains within the given namespace. The chain of bilateral agreements transmits obligations; the terms set by ICANN filtering down to the last link. The agreements have a dynamic element as they are revised on the adoption of new policies by ICANN. And they are frequently transnational, the parties often being based in different jurisdictions. Moreover, policy is developed and then cemented as law in essentially a legislative process, albeit with different formal outcomes, actors and procedures than in a traditional parliamentary system. ICANN functions as a legislative arena replete with its own set of lobbyists, constituencies and law-making procedures. Given its legal status, the ‘legislation’ ICANN produces must take the form of contract but the latter is employed similarly to the way in which ordinary statute tends to be employed—that is, to set down legally binding norms for an entire community or considerable sections of one.

The legislative role of contract in governance of ccTLDs is admittedly less significant than for gTLDs, with some governments using statute to lay down the ground rules for ccTLD management. Yet contracts are still employed at the lower end of the normative chain where they govern the relationships between registries, registrars and domain name holders. They function, though, as handmaidens of statute since they must faithfully reflect the statutory rules (along with other ‘softer’ norms, such as those documented in RFC 1591) further up the normative chain.

Governance of ccTLDs is but one of numerous areas where contract is integrated in and services a statutory ‘top-down’ regulatory structure—again showing the versatility of contract. Other such areas that are particularly pertinent to the Internet include data protection law and law on provision of electronic communications services. Regarding the latter, statute requires, amongst other things, that the obligations it imposes on ISPs be followed up in contracts with end-users (see, for example, the EU Universal Service Directive (2002/22/EC) Articles 20 and 30(5)). In the area of data protection law, statute mandates use of contract to ensure, for instance, that the outsourcing of data-processing operations remains subject to the relevant statutory rules (see, for example, the EU Data Protection Directive (95/46/EC) Article 17(3)).

Statute also sometimes services contract. In an Internet context, this is evidenced particularly well by the recent round of legislative reform to promote electronic forms of commerce. An important element in that reform has been to give contractual transactions that are carried out electronically similar legal status to non-electronic transactions (see, for example, the 2006 UN Convention on the Use of Electronic Communications in International Contracts, the E-Commerce Directive and Electronic Signatures Directive (1999/93/EC)).

At the same time as contract is well-suited to governing the digital world, the latter is
particularly conducive to use of contract. In the words of Hugenholtz (1999: 308–309):

The structure of the Internet facilitates the establishment of a multitude of contractual relationships between information producers and end users, either directly or through intermediaries. The Internet (or more precisely, the World Wide Web) is uniquely suited for this purpose. Both its “textual” environment and its interactive nature are ideal conditions for a contractual culture to grow and flourish.

The burgeoning use of EULAs to govern interactive virtual worlds illustrates this point well.

Yet EULA proliferation highlights another important reason for the popularity of contract. This is that contract is an excellent means of control. It is particularly suited to micro-management and can be closely fitted to the particular needs of a virtual world provider. It can also be used to marginalise, if not lock out, norms that threaten those needs. These control possibilities become even greater when combined with technological measures. Not surprisingly, then, we find a considerable number of virtual worlds operating in effect as feudal fiefdoms (Jankowich 2006, Mayer-Schönberger and Crowley 2006, Fairfield 2008, Fairfield 2009, de Zwart 2010).

THE PROVINCE OF STATUTE

Despite the popularity of contract, statute is far from absent in Internet governance. Indeed, the range of legislation that we must regard as pertinent to the field has grown greatly as conceptions of what constitutes ‘Internet governance’ have expanded. When Internet governance is now (rightly or wrongly) treated as basically concerned with ‘the entirety of communication and information policy’ (Mueller 2010: 10), a large body of statute law becomes relevant. Such law can be seen as providing numerous ground rules for the provision of Internet-related infrastructure and services, and for the resultant data flows. It does this for the most part through both international and national instruments. The regulatory intensity, though, varies considerably from context to context as does the degree to which the rules are Internet-specific.

An exhaustive presentation of all relevant statute law would burst the boundaries of this chapter. Hence, the following paragraphs provide only examples of matters that have been the subject of relatively intensive statutory regulation and focus only upon relevant international agreements. Keep in mind, however, that most of the requirements laid down by those agreements have been or will be transposed into national laws. The actual number of statutory instruments is thus far greater than the number of instruments listed in the following.

Protection of intellectual property rights (IPR) is one matter that has long been singled out for energetic legislative effort. The Clinton-Gore administration signalled concern about the matter early on, stating already in its 1993 policy paper, ‘The National Information Infrastructure: Agenda for Action’, that it would ‘investigate how to strengthen domestic copyright laws and international intellectual property treaties to prevent piracy and to protect the integrity of intellectual property’ (principle 7). The plan thus constituted one exception to the ‘decentralized, contractual model of law’ otherwise championed by the administration. It helped give birth to several international agreements (most notably, the WTO TRIPS (Trade-Related Aspects of Intellectual Property Rights) Agreement of 1995 and two treaties under the auspices of the World Intellectual Property Organisation (WIPO)—the Copyright Treaty and
Performances and Phonograms Treaty, both of 1996) along with domestic legislation (primarily in the form of the Digital Millenium Copyright Act of 1998). These efforts were duplicated by governments elsewhere. The EU, for example, has enacted a raft of Directives with the aim of strengthening and harmonising European IPR regimes as they apply to the digital environment (see particularly the Database Directive (96/9/EC), Software Directive (2009/24/EC), Copyright Directive (2001/29/EC) and IPR Enforcement Directive (2004/48/EC)). The impact of some of these instruments is dealt with further below.

Cybercrime and information security are other matters attracting relatively intensive statutory regulation both nationally and internationally (for overviews focusing on international efforts, see Rutkowski 2011 and Williams 2010). The chief international legal instrument on point is the COE Cybercrime Convention adopted in 2001. The Convention requires contracting states to make provision in their national laws not just for hacking and other standard ‘CIA’ offences (that is, activities impinging upon the confidentiality, integrity and availability of computer data and systems; see Articles 2–6) but certain content-related offences as well, namely dissemination of child pornography (Article 9), dissemination of racist and xenophobic material (Additional Protocol of 2003) and breach of IPR (Article 10). It is thus manifestation of a growing tendency for legislative measures on cybercrime to dovetail with legislative measures for protecting IPR, thereby helping to criminalise IPR violations. This is but one of many controversial sides to the agreement (see further, for example, Williams 2010: 480–483). The Convention is otherwise noteworthy not just for being a rare instance of a treaty regime attempting to deal directly with Internet-related activity but also for its impact beyond the circle of COE member states. It was prepared with assistance of states from outside that circle and is the only COE Convention to have been signed and ratified by the USA. It continues to constitute a significant point of departure for legal developments in other non-European states. Australia, for instance, is in the process of passing legislation which will allow it to accede to the Convention (see Cybercrime Legislation Amendment Bill of 2011). As yet, though, the Convention hardly qualifies as a global agreement. It has been ratified by just 32 countries, the USA being the only non-European state in that group. A significant number of COE member states, including Austria, Belgium, Italy and Sweden, have not yet ratified.

Cybercrime and IPR aside, governments have shown much legislative zeal in the area of privacy and data protection (see further the chapter by Greenleaf in this volume). Even in the USA, where government has traditionally eschewed enacting comprehensive data protection legislation along the lines typical for Europe, we find a surprisingly great number of statutes on point. These tend to be narrowly circumscribed, and the coverage they offer, particularly with respect to processing of personal data by private sector bodies, is haphazard and incomplete (Schwartz and Reidenberg 1996: chs 9–14; Solove, Rotenberg and Schwartz 2006: chs 2 and 7). Yet when viewed in their entirety, they make up a hefty corpus of code. While some of the recent legislation on privacy and data protection takes specific account of the Internet or digital environment (see, for example, the EU Directive 2002/58/EC on privacy and electronic communications), much of the seminal legislation does not and was adopted before the Internet became widely used. This is especially the case with key international agreements (Bygrave 2008), such as the 1981 COE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the EU Data Protection Directive (95/46/EC). That does not mean the codes in question fail to apply to Internet-related activity; they do apply, though not always with sensible results or a desirable degree of prescriptive guidance (Bygrave 2002: ch 18; Bygrave and Michaelsen 2009: 120–121).
Academic discourse dealing specifically with Internet governance now tends to devote considerable attention to legislation on cybercrime, IPR and privacy (see, for example, Wu and Goldsmith 2006; Mueller 2010). There is, however, a large body of other legislation which remains much less salient in that discourse but must now be regarded as fairly central to Internet governance. The most glaring instance is legislation on deployment of electronic communications infrastructure and services. At the same time, discourse that does focus on such legislation has tended to pay scant attention to Internet governance as such (see, for example, Walden 2009 and previous editions of that work). The disconnect has both technological and legal roots, the legislation in point being originally pitched at networks for ‘telecommunication’ which were not TCP/IP-based. It thus mirrors the gap that previously existed between the policy spheres of the ITU and the early governors of the Internet, such as the IETF, ISOC and ICANN. The factual basis for the disconnect is now greatly weakened: the technological-organisational lines dividing TCP/IP networks from other forms of electronic communication have become less distinct; conceptions about the scope of the ‘Internet’ and ‘Internet governance’ have broadened; and much of the legislation previously dealing with telecommunication has been updated to cover TCP/IP networks. The EU regulatory framework on electronic communications, for instance, has undergone successive revisions partly in order to take better account of the Internet environment.

The scope of that framework is worthwhile elaborating in detail as it demonstrates the considerable breadth of the impact it may have on Internet governance. The framework is both extensive and dense. Its core alone comprises five Directives (2002/21/EC, 2002/19/EC, 2002/20/EC, 2002/22/EC and 2002/58/EC) and a Regulation ((EC) 1211/2009). These are supplemented by sector-specific recommendations, guidelines and notices along with rules of more general application (see generally Nihoul and Rodford 2011; Walden 2009). The immensity of the framework is testament to the fact that legal reform in the name of ‘competition’ and ‘deregulation’—a central aim of the framework being to privatise and break up monopolized services in the telecommunications sector—some times does not so much decrease regulation as to reconfigure and augment it by establishing comprehensive legislative and policing schemes in order to ensure that competition actually occurs (see too Edgeworth, 2003: 155).

The framework covers a wide range of matters. They include the obligations that state regulators may impose on ISPs and other providers of electronic communications services, use of radio spectrum, conditions for providing network access and interconnection, protection of personal data and end-user freedoms. An important limitation in coverage—at least in principle—is that the framework concerns only communications infrastructure, not the information content of the transmitted data (see Recital 5 in the preamble to the Framework Directive (FD) for electronic communications), though maintaining a strict separation between content and transmission is obviously difficult in practice. Content regulation is dealt with more directly by other sets of rules, including the E-Commerce Directive (2000/31/EC) and legislation on IPR, data protection and cybercrime as outlined above.

The severity of the framework’s bite depends largely on the state of market competition. The most stringent regulation is reserved for actors who exercise ‘significant market power’—that is, actors who are able ‘to behave to an appreciable extent independently of competitors, customers and ultimately consumers’ (FD Article 14(2)). Thus, ‘ex ante regulatory obligations should only be imposed where there is not effective competition, i.e. in markets where there are one or more undertakings with significant market power, and where national and Community competition law remedies are not sufficient to address the problem’ (FD Recital
For the most part, the provisions of the framework are pitched at a high level of generality. They also have little to say specifically about TCP/IP networks. Governance of the Internet naming and numbering system, for example, is addressed obliquely. Aspects of that system may nonetheless fall within the framework if references therein to ‘number translation’ and ‘numbering resources’ extend to IP numbers. The framework fails to clearly define what it means by ‘numbers’; it also fails to clearly address the extent to which IP numbers are embraced. It defines ‘number translation or systems offering equivalent functionality’ simply as elements of an ‘associated service’ and thereby ‘associated facility’ (FD Article 2(ea) and (e)), such services/facilities being covered by the framework. Further, it covers use of ‘geographic numbers’ and ‘non-geographic numbers’, defining these in ways that link them to the ‘national telephone numbering plan’ (Universal Service Directive (2002/22/EC) Article 2(d) and (f)) but without excluding the possibility of IP numbers forming their basis. The framework also deals more generally with ‘numbering resources’ and ‘numbering plans’ (see below) though again fails to define these. On their face, these terms are broad enough to encompass both IP numbers as such and translations of IP numbers in the form of domain name addresses—a view shared by UK legislators and reflected in the broad definition given to ‘telephone numbers’ in the UK Communications Act 2003 (see section 56(5) and (10)). Such coverage may have long-term consequences for the use of IP numbers and domain name addresses, particularly as the most recent round of reform of the framework provides the European Commission and national regulatory authorities with more explicit responsibility over numbering schemes than existed previously. Whether it has also increased the extent of their competence in the field is a matter of debate.

Prior to the reform, the Framework Directive stated that its provisions ‘do not establish any new areas of responsibility for the national regulatory authorities in the field of Internet naming and addressing’ (Recital 20 in its preamble). It went on simply to encourage EU member states, ‘where ... appropriate in order to ensure full global interoperability of services, to coordinate their positions in international organisations and forums in which decisions are taken on issues relating to the numbering, naming and addressing of electronic communications networks and services’ (Article 10(5)). Now the legislation requires member states to ensure that national regulatory authorities (NRAs) ‘control the granting of rights of use of all national numbering resources and the management of the national numbering plans’ (FD Article 10(1); see too Recital 20 in the preamble: ‘All elements of national numbering plans should be managed by national regulatory authorities, including point codes used in network addressing’ (emphasis added)), and that NRAs ‘establish objective, transparent and non-discriminatory procedures for granting rights of use for national numbering resources’ (FD Article 10(1)). Moreover, the Commission is now empowered to ‘take technical implementing measures using its executive powers’ in situations where ‘there is a need for harmonisation of numbering resources in the Community to support the development of pan-European services’ (FD Recital 20; see too Article 19(3)(b)). And, following up FD Article 10(1), the Authorisation Directive (2002/20/EC) now lays down parameters for the procedures and conditions that member states may apply in authorising rights to use ‘numbers’. Basically, authorisation procedures shall be ‘open, objective, transparent, non-discriminatory and proportionate’ (Article 5(2); see too Article 6(1)). They shall also be fairly prompt (Article 5(3)). Permissible conditions that may be attached to authorisations are set out in the Annex to the Directive.

As already indicated, whether these provisions are intended to apply to IP numbers or domain
names is not clear. But if they do apply, they place—at least on paper—those parts of the traditional Internet naming and numbering system which can be singled out as falling within the jurisdiction of the EU (and European Economic Area) under ultimate control of the public sector. Whether that control will lead to greater top-down regulation of the system remains, of course, to be seen. In some states, any push from, say, the European Commission for greater regulation will be met with resistance. The UK is one such state. While its central legislation on point extends to IP numbers and domain names (see the Communications Act 2003 section 56(5) and (10)), these have been removed from the jurisdiction of the main NRA (Ofcom) by secondary regulations (see The Telephone Number Exclusion (Domain Names and Internet Addresses) Order 2003 (SI No. 3281)). This was in line with the government’s ‘aim of promoting self-regulation and not applying additional regulation to cover the internet’, along with its view that use of Internet-related identifiers was subject ‘to evidently effective self-regulation’ (Timms 2003).

CONTRACTUAL SUPREMACY IN GOVERNANCE OF INTELLECTUAL PROPERTY?

While contract and statute often work hand in hand, their relationship is not always friendly. This is the case when the one is used in an attempt to cancel out application of the other. The conflict arises typically when private fiat masquerading as freedom of contract threatens to trump statutory-based public interests or to otherwise sideline use of statute. Protection of IPR is perhaps the most highly charged case in point. Conflict in that context occurs chiefly over how IPR is to be apportioned (between, say, original and subsequent developers of software) and the extent to which statutory limitations on IPR are to be respected.

Both types of conflict are present in the EULA-based governance regimes of particular virtual worlds due to systematic attempts by the providers of those worlds to supplant statutory rules on IPR through contract and software code (see, for instance, Fairfield 2008 and de Zwart 2010). Such attempts add credence to older fears that the ability of copyright legislation to meaningfully govern the exploitation of digital data risks redundancy due to a more potent regulatory combination of contract and technology (see, for example, Hugenholtz 1999 and references cited therein). In an early vision proffered by one scholar, ‘[t]here may be nothing for copyright to do, except perhaps to serve as a kind of deus ex machina justifying the use of technological and contractual means for protecting works in digital form’ (Samuelson 1995: 125). Of greater concern, though, is the potential mental marginalisation of copyright and related public interests through extensive recourse to licensing. As Madison (2003: 277) has observed, ‘there is the possibility that the licensing norm itself is internalized by the reader, listener, and user communities such that the world of information production and consumption is regulated informally, even in the absence of formal “legal” enforcement of particular licenses and of norms exogenous to the license itself’.

Fortunately, copyright legislation has not yet reached the point where it functions purely as symbolic code, and to claim that it definitely will reach that point would be overly presumptuous. It would also be overly presumptuous to regard copyright as lightweight law that contract can bowl over without resistance. There exist a large range of actual and potential legal restrictions on the ability to contractually derogate from particular end-user rights or freedoms for which copyright or neighbouring rights typically cater.

Some such restrictions are fairly concrete but narrowly tailored. For instance, the EU
Software Directive stipulates that contract may not prevent a person having a right to use a computer program to make a back-up copy of the program (Article 5(2)). Users are given equivalent protection of their ability to analyse and decompile the software (Articles 5(3) and 6), with any contractual provisions to the contrary being deemed null and void (Article 8).

Similarly, the EU Database Directive provides that contract may not prevent a database user from making normal usage of the database (Article 6(1)) or from re-utilising non-substantial parts of it (Article 8(1)), with contractual provisions to the contrary again being rendered nugatory (Article 15).

More general limits on contractual disposition over intellectual property exist too. For instance, restrictive licenses giving rise to anti-competitive practices may be remedied through the imposition of compulsory licensing schemes whereby a holder of intellectual property is forced to grant individual licenses for its use, at a price and under conditions that are determined jointly with the user or by the relevant state authorities when agreement cannot be reached. This involves, in effect, the state imposing and enforcing an involuntary contract between a willing buyer and an unwilling seller (Gorecki 1981). Provision for such schemes is made, for example, in the 1886 Berne Convention for the Protection of Literary and Artistic Works with respect to sound recordings and lyrics (Article 13) and broadcasting (Article 11bis (2)). For patented products, such schemes are permitted under the TRIPS Agreement (see Article 31; see too Article 40) and, more distantly, under the 1883 Paris Convention for the Protection of Industrial Property (see Article 5A(2)).

Courts in some jurisdictions have also applied similar sorts of remedies pursuant to general statutory rules on competition. Case law of the EU Court of Justice under Article 102 of the Treaty on the Functioning of the European Union (formerly Article 82 of the Treaty establishing the European Community) is perhaps the most ambitious in point (see especially Cases C-241/91P & 242/91P Radio Telefis Eirean (RTE) and Independent Television Publication Ltd (ITP) v Commission [1995] ECR I-0743, Case C-418/01 IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG [2004] ECR I-5039 and Case T-201/04 Microsoft v Commission [2007] ECR II-03601; for discussion, see, for instance, Houdijk 2005 and Pereira 2011). That case law deals in part with the ability to access digital data (IMS Health and Microsoft) and thereby points to further potential use of compulsory licensing or equivalent remedies as a tool of Internet governance. The flexibility and reach of such remedies under general competition law is augmented by their apparent ability to apply, at least in principle, independently of whether or not the undesired digital ‘lock-up’ is due to patent or other forms of IPR—a barrier created simply by contractual license might well be sufficient in certain circumstances. Some scholars have even broached the possibility of using such remedies to break up ICANN’s control over the Internet naming and numbering system (Meyer and Utz 2007), but this would be an extremely long shot.

Restrictions on contractual freedom may be derived from other fields of law besides those dealing specifically with IPR and competition. These include rules on protection of fundamental human rights, consumer protection, abuse of rights and even rules in contract law itself. However, the purchase of many of these restrictions is blunted by uncertainty or dispute over the scope of their application (see generally Guibault 2002). Compulsory licenses, for example, are frequently regarded as controversial remedies and their application is typically subject to stringent preconditions (see further, for instance, Harris 2004: 134–136, 144–156 and Cotropia 2008 discussing restrictions on use of compulsory licensing under the TRIPS Agreement). Moreover, the strength and availability of the restrictions varies greatly from jurisdiction to jurisdiction. For example, doctrines on good faith and abuse of rights are most
developed and readily applied in civil law systems (though rough equivalents are found elsewhere—see, for instance, Reid 2004 pointing to manifestation of doctrine on abuse of rights in Scots and English law). And common law systems seem generally most conducive to ‘hard-headed’ contractual freedom. This is indirectly evidenced by commercial actors’ frequent preference for applying English or US law to govern transnational contracting.

All up, serious doubts must attach to the ability of statutory IPR regimes and more general law to prevent a combination of contract and technology from unilaterally dictating how intellectual property shall be used in the digital environment. The sway of the contract/technology combination over statutory IPR regimes is exacerbated by the general failure of such regimes to clearly establish the normative priority of their rules—including the statutory limitations they place on IPR—vis-à-vis contract (Guibault 2002 and Guibault 2006). It is further exacerbated by the fact that the contract/technology combination is no longer purely exogenous to such regimes but incorporated into them through the introduction of provisions on protection of ‘technological measures’ and ‘rights management information’ (see, for example, the 1996 WIPO Copyright Treaty Articles 11–12; EU Copyright Directive 2001/29/EC Articles 6–7). The ambiguity of those provisions, particularly over whether the protection they give technological measures must respect traditional end-user rights and freedoms (see further, for example, Bygrave 2003), compounds the above problems.

FUTURE STATUTORY OVERLAY?

The final matter to be canvassed concerns the prospect of statute being accorded a significantly larger role in governance of the Internet: will legislation be introduced in the field which dramatically overshadows or reduces the role of contract? The question is particularly pertinent in light of calls to develop new statutory schemes along a variety of fronts. At the domestic level, proposals for legislation establishing general principles, rights and obligations specific to Internet use are being drafted in some countries. Brazil has perhaps come furthest in this regard with an expansively formulated draft Bill for a civil rights framework for the Internet currently being considered by the national Congress (see Marco Civil da Internet; Bill no. 2126/2011). At the international level, there are proposals to develop a broad treaty-based regime to govern the Internet generally (see, for example, Mueller, Mathiason and Klein 2007 arguing the merits of introducing a framework convention for Internet governance akin to the 1992 UN Framework Convention on Climate Change). There are also proposals for international conventions of more limited scope (see, for example, Weber and Weber 2010 arguing in favour of a convention to govern the nascent ‘Internet of Things’; Svantesson 2006 proposing a model convention to regulate cross-border Internet defamation arising out of mass communication). And there are calls for greater government regulation of virtual worlds (see, for instance, De Zwart 2010 arguing that governments ought to develop a baseline of light-touch, internationally coordinated, regulatory standards for virtual world providers; Balkin 2004 proposing use of ‘statutes of internation’ to govern the legal relationships between providers and users of virtual worlds).

Much can be said in favour of the propriety of such proposals and they may find particularly fertile ground in some countries, such as Brazil. In other countries, however, their prospects of success are probably rather slim. Some of their proponents admit as much. Weber and Weber, for instance, state that the ‘Internet of Things’ is most likely to be subject to an industry-based self-regulatory regime due to the relative ease with which such a regime can be set up and subsequently adjusted to keep pace with technological developments (Weber...
Proposals for international conventions—especially multilateral initiatives—face particularly serious obstacles. One obstacle is the sheer clutter of the ideological landscape in which conventions must now be brokered. The horizons for regulatory policy are filled by cross-cutting sets of norms and interests—human rights, trade, national security, law enforcement, etc.—about which it is increasingly difficult to reach global consensus. Commitment to ‘multistakeholderism’ adds to these problems as does the lack of a sufficiently strong, dynamic and representative body to negotiate any multilateral convention let alone one with bite. The outcomes of the World Summit on the Information Society (see further Hubbard and Bygrave 2009) are testimony to this. And the ITU still seems to have a long way to go in repairing its tattered reputation for potentially brokering a meaningful framework convention on Internet governance—as MacLean (2008: 84) notes, ‘[i]f it continues on its present course, it now seems clear that progressive marginalization is the most the ITU can hope for, and that eventual disappearance “not with a bang but a whimper” its most likely fate’. It is hard to identify another organisation that is both able and willing to drive negotiations for a multilateral treaty forward. The World Trade Organisation (WTO) is occasionally touted as such a body. Yet its ability to broker a broadly acceptable convention will be hampered by its commercial agenda. Its ability to broker such an agreement quickly and efficiently is also in doubt given its tardiness in crystallising policy on e-commerce (Wunsch-Vincent 2005). Another possible candidate is the Organisation for Economic Cooperation and Development (OECD) yet it seeks generally to generate guidelines and other instruments of ‘soft law’ rather than ‘hard law’. The EU and COE are other possible candidates, and they are not averse to creating international ‘hard law’, but their ability to foster global consensus will be handicapped by their regional status and bias. The COE has recently sponsored development of a fairly comprehensive set of general principles on Internet governance which could form the basis for a framework convention in the field (COE Ad Hoc Advisory Group on Cross-border Internet 2011) but has not (yet) taken concrete steps to initiate work on such an instrument and seems reluctant to do so. As for the EU, the current Vice-President of the European Commission who is responsible for the EU’s Digital Agenda has aired the need for general governance principles in the form of a ‘Compact for the Internet’, yet emphasises at the same time that ‘this is not about regulation’ (Kroes 2011).

As for proposals to subject virtual worlds to greater statutory regulation, whether these will get off the ground will greatly depend on market dynamics. And it is very difficult to accurately predict how the market for virtual worlds will develop. As Mayer-Schönberger and Crowley (2006) show, the variables are numerous as are the possible trajectories. Two important variables are the degree to which EULAs affront the wishes of end users and the broader community, and the degree to which end users agitate for their wishes to prevail over EULA rules, thereby mobilising government to take action on their behalf.

It would be premature to assume that either variable is likely to play out strongly in ways that would favour legislative intervention. Although Fairfield (2008: 433) labels EULAs ‘antisocial’ because ‘they create confusion and litigation’, it is remarkable that such contracts have rarely been the subject of litigation or vehement protest on a large scale, despite their massive deployment. While end users are not oblivious to the existence of EULAs—end users must usually formally accept such agreements prior to being admitted to the online service or platform in question—they are probably indifferent to the agreements’ actual terms and, in the absence of untoward behaviour, they can generally enjoy the proffered service(s) without significant interference from the EULA drafter. The above-mentioned ‘internalisation’
problem identified by Madison (2003) might also contribute to end-user passivity. The increasingly dense legalese of EULAs no doubt contributes also to their marginal role for the bulk of end users: to paraphrase one commentator, EULAs appear not just to be written by lawyers but also for lawyers (Nino 2010; see too Jankowich 2006). It is instructive that in one of the few instances of EULA-focused litigation, the plaintiff was both a lawyer and an end user who got into trouble with the online community provider (Linden Labs) for allegedly purchasing virtual real estate in Second Life by improper means (Bragg v. Linden Research Inc., 487 F. Supp. 2d 593 (E.D. Pa., 2007); the case was ultimately settled out of court). Further, virtual world providers are not entirely free to make up and change the rules of their worlds at whim. If they are to survive commercially, they must go some way to respecting the wishes of the majority of end users (Grimmelmann 2006; Mayer-Schönberger and Crowley 2006). This blunts their ability to ride roughshod over end users and the broader public interest, thus helping to take some of the steam out of any possible end user or legislative objections.

CONCLUSION

This chapter shows when and why contract enjoys a privileged position relative to statute in governing the Internet. That position is due essentially to the fact that contract enables flexible micro-management of the digital world more easily than statute does. Whenever Internet governors, particularly in the private sector, need ‘hard law’ to exercise fine-grained control which is tailored to the particular needs of a technological platform, service or online community and yet can be quickly adjusted as those needs change, contract will tend to be the tool of choice. Exacerbating this tendency is a fairly general ideological bias against developing new statutory forms of control except as measures of ‘last resort’.

If we are to attempt to sum up in a single sentence the respective role of contract and statute in Internet governance it is that the latter tends to play second fiddle to the former. Yet, like most such attempts, this is an oversimplification of reality. We can see from the foregoing analysis of copyright that contract may in some instances be threatening to relegate statute to a more marginal spot in the orchestra. In other instances, though, statute and public law may be jostling for a spot amongst the first violins—the case, for example, with EU legislation on electronic communications networks and services.

Indeed, the most important insight delivered by the chapter is that the relative roles played by contract and statute in Internet governance are not frozen but fluid. How those roles change depends on numerous factors. They may change, for example, as conceptions of the parameters of Internet governance change. They may change depending on the degree to which the Internet facilitates behaviour posing a major threat to, say, established revenue streams (consider, for example, legislation on IPR) or basic human rights (consider, for example, legislation on privacy and data protection). They may change as political constellations change (consider, for instance, the replacement of the JPA by the AOC). Or they may change as conceptions of their respective degrees of legitimacy change in light of market behaviour (consider, for example, evolving views of the (un)fairness of EULA-based governance).
REFERENCES


