7

Internet Policy

Sandra Braman

The Internet is simultaneously a general use tool, communication medium, set of material objects, idea, and factor of economic production. Thus any discussion of Internet policy must begin by looking at what it is, and what it is not. Internet policy is made at every level, from the global to the most local, involving private-sector entities and personal practices as well as governments. The Internet raises a myriad of legal problems, but the "Big Four" – access to the Internet, access to content, property rights, and privacy – stand out because policies in these areas create the conditions under which all Internet activity takes place. This chapter addresses the foundational questions: What is policy? What is Internet policy? Where is Internet policy made? What are the most important issues?

What is Policy?

The word "policy" has many faces. It can refer to general legal principles as articulated in constitutions or constitution-like documents, such as freedom of expression. A policy can be a proposed law still being debated, or a program to implement a law once passed. Organizations, communities, and families create policies that don't apply outside of those contexts but that serve as regulation within them. Policy can be public (governmental) or private (corporate, personal, or generated by civil society groups), and it can be formal or informal. Here the focus is on formal laws and regulations of governments, with the important exception of the Internet Corporation for Assigned Names and Numbers (ICANN). This section introduces the elements of the policy world,[1] critical distinctions among types of policies, and policy convergence.

The policy world

Policymakers hold power in decision-making entities. The *audience* for each law includes those who are affected; for an Internet law or regulation the audience

The Handbook of Internet Studies Edited by Mia Consalvo and Charles Ess

may be specialized (e.g., those who gamble), but often it is society-wide. A policy *issue* is the social problem that the law is asked to address (privacy, or equity), and political scientists group related issues into *issue areas*. Policy *tools* are the legal mechanisms used to achieve given goals. The *target* of a law is the entity to which a law applies; antitrust (competition) law, for example, targets corporations. *Citizens* influence policy through traditional political means such as the vote and work as policy advocates and activists. Because so much Internet policy is still emerging, often appearing in areas in which there are lacunae in the law or in which traditional perspectives must be reconsidered, citizens also play important roles by developing norms and practices that affect, inspire, or actually generate legal innovations.[2]

These various law–society relations are often mixed in policy analysis, and sometimes confused and/or conflated, so an example may be helpful. For copyright in the US, members of Congress and the World Intellectual Property Organization (WIPO) are the policymakers; the audience is society but the nature of the interest can differ (concerns of the music industry are not those of music students); the issue is how to balance motivations for content production with society's need for access to content; tools include education, lawsuits, and digital rights management (DRM) systems; and targets include individual and corporate content users as well as Internet service providers (ISPs) and ISP-like entities such as universities. Citizens affect decision-making and practice in each of these.

Latent versus manifest policy

Whether or not any given policy affects the Internet may not be evident on the surface. We can refer to laws and regulations that clearly and directly affect the Internet and how we use it as "manifest," and those for which the influence is indirect and not necessarily evident "latent." It is easy to identify manifest Internet policy issues, such as privacy. Discerning latent policies can be more difficult, as exemplified by antitrust. In the early 1980s, the US government began to relax antitrust restrictions on the high-speed computer chip industry in response to assertions that closer collaboration among corporations was needed to retain international competitiveness, a matter of deep concern not only economically but also from a military perspective. This was justified publicly by arguing that such chips were needed for high-definition television, a technology that also requires a broadband network like the Internet. Thus changes in antitrust law that on the surface had little to do with the Internet have influenced its development.

Public versus private law

Public law is the law made by geopolitically recognized entities that include states (France, Singapore, Egypt) and legally effective regional bodies (the European Commission). It affects everyone and every entity within its jurisdiction. Private law is created through contractual agreements between individuals and individual

entities, such as corporations, with each contract applying only to signatories. Historically, public law created the environment for private law, but today increasingly the reverse is true. The audience of private contracts can go far beyond signatories, as when environmental damage occurs; these effects are called "externalities." Privatization of former government functions also contributes to the rising importance of private law. In the many areas in which networked digital technologies have presented issues not previously the subject of national or international law, private contracts have set precedent for public law. ICANN, the global organization that manages the Internet, has set up a parallel legal world through a flow-down contract system derived from control over domain names (Mueller, 1999).

Criminal versus civil law

Most countries distinguish between criminal and civil law, though there are national differences in the definitions of each and interactions between the two. In the US, it is a matter of criminal law when an explicit law or regulation has been broken, an action understood to be an attack on society as well as on the victim; Internet examples include sexual predation against children, libel, and some invasions of privacy. Civil law, on the other hand, involves conflicts or harms that do not involve a specific law; these are considered to harm the victim, but not society at large, and are called torts. Providing false information is an example of Internet behavior that might be tortious. Legal systems can expand by turning torts into crimes through new laws and regulations. Criminalizing even unintentional damage to computer systems that costs $5,000 or more to fix (under the USA PATRIOT Act) is an Internet policy example of this process.

Policy convergence

The Internet was made possible by the convergence of computing and communication technologies, and Internet content displays a convergence among genres. In the same way, coping with the Internet has made us aware of at least four forms of convergence processes among previously distinct categories of law.

First, Internet policy appears across silos of the law that have been separated from each other in the past. Internet interfaces – what one attaches to the network in order to use the net, also known as customer premises equipment (CPE) – provide one example of why this makes a difference. In the US, historically two very different bodies of law applied. In constitutional law, interpreted by the courts, the postal provision governs privately owned interfaces with the public message distribution system with an emphasis on equity and ubiquity of access to the system. In administrative law, managed by the Federal Communications Commission (FCC), telecommunications regulation dealt with CPE for the telecommunications network with an emphasis on network efficiency. Extensive discussions about such interfaces have appeared in both environments, and both approaches

must be taken into account for the Internet, but in the past these discussions never referenced each other.

Second, though typically legal practice and scholarship treat legal issues as if each exists in isolation, this is never the case. Anonymous use of the Internet, for example, simultaneously involves privacy, authenticity, free speech, surveillance, and access. Internet policy analysis must thus include attention to "policy precession," interactions between the effects of two or more laws and regulations.

Third, technological convergence has made it impossible to keep previously distinct systems for regulating communication separate. In a highly influential work of enduring value, political scientist Ithiel de Sola Pool (1983) pointed out that the separate frameworks for regulating broadcasting, telecommunications, and expression would themselves converge into a single legal system. His prescient warning that the result would most likely use the most restrictive elements of each approach is worth heeding today.

Fourth, the global nature of the Internet has given it a role in both requiring and facilitating what political scientists and legal scholars refer to as legal "harmonization," the convergence of laws and regulations across states so that they conform with each other. Harmonization comes about through a variety of processes of policy transfer and coordination that have received very little attention from scholars of Internet policy (Braman, 2009).

What Is Internet Policy?

Over the 50-year history of what we currently refer to as the Internet, perceptions of the boundaries of the domain of pertinent law have mutated, and are likely to continue to do so. Here, Internet policy is defined as those laws and regulations that are either specific to Internet infrastructure and its uses (e.g., domain names, or trying to control spam) or apply to long-standing legal issues that have so qualitatively changed in nature in the digital environment that significant changes are required of the legal system (e.g., privacy and copyright). Some of the legal tools in play to regulate the Internet and its uses are familiar from earlier communication law; others are innovations specific to the Internet.

A short history

Since the time of the reinvention of the printing press in Western Europe in the fifteenth century, each new information or communication technology has been followed by changes to the legal system. From the mid-nineteenth century on, governments responded to the telegraph, telephone, and radio with new regulatory systems. Technological innovation was ongoing, triggering essentially constant reconsideration by governments of how those communication systems should operate.[3]

By the mid-1990s, three stages of thinking about what we now refer to as Internet policy were already discernible.[4] The first involved forecasts of legal problems that

would result from digitization such as warnings by cyberneticist Norbert Wiener, detailed analyses of growing threats to privacy by Alan Westin, and inquiries into the regulatory status of new technologies by numerous legal scholars. Government explorations of the legal consequences of digitization in the late 1970s included, notably, the French Nora/Minc report and the Swedish Tengelin report. During the second, sometimes overlapping, stage, attention focused on consequences of the convergence of computing and communication technologies that had taken place during World War II and was quickly diffusing throughout the commercial world. In some cases, regulatory agencies took the lead; in the United States, the FCC, which had responsibilities for both telecommunications and broadcasting, explored the legal status of new forms of communication with characteristics of both in a series of "Computer Inquiries" from the mid-1960s to the mid-1980s. Communication scholars such as Cees Hamelink, Marjorie Ferguson, and Larry Gross began to look ahead. Attorneys at influential law firms often took the lead role in developing new legal approaches to communications in the digital environment.[5]

The third stage saw such an explosion of detailed analyses of very specific legal issues that it rather quickly led to efforts to conceptualize a single umbrella for Internet policy as a distinct legal domain. In the 1990s, Internet-specific courses began to appear in law schools.[6] By the first decade of the twenty-first century, courses, books, and journal articles all take the concept of Internet policy as a given and both the scholarly literature and the legal problems themselves continue to explode in number. But there is still no consensus about what exactly the domain includes. Now that there are Internet dimensions of every area of human activity, it is likely that this period of treating Internet-related legal problems as a special class will, in its turn, also pass.

When it does, distinctions among legal issues specific to the Internet, those that are traditional and appear in traditional forms on the Internet, and those that are traditional but appear in qualitatively new forms on the Internet will be important. Those in the first category, such as treatment of denial of service (DNS) attacks or the theft of wi-fi signals, will clearly fall within the domain of Internet policy. Those in the second category, such as most forms of fraud that use the Internet as a tool and pornography, may well fold back into their originary legal frames.

Those in the third category, traditional legal problems that are experienced as qualitatively new in the Internet environment, will remain particularly problematic. For these issues, the change in scale and relative ease of socially troublesome activity made possible by networked digital technologies completely shift the experience and the perception of the legality of particular practices. In most democratic societies, for example, we have long had the right to access many types of the personal data of others, such as date of birth, license plate number, and legal records. In the analog environment, however, gathering all of this information about a person required physical travel to diverse locations, working with numerous organizations and individuals to locate the data, and steep costs in money and time. Today, the work can be done within minutes for minimal cost on the

Internet, with the result that it is done so much more frequently that many people believe the information has become publicly available for the first time. As a consequence, laws in this area are undergoing deep reconsideration.

Digitization, expansion of the global information infrastructure, and continuous technological innovation are not the only factors affecting the contours of the domain of Internet policy. Other profound changes in the nature of the law and in law–society–state relations have also been important.[7] These include the privatization, liberalization, and deregulation of communication networks by governments around the world that began in the late 1970s; oligopolization of most communication and information industries and the concomitant growth in size of dominant corporations; and the transition from an industrial to an information economy. The fact that very few policymakers understand the technologies they are regulating, or know anything about their uses and the effects of those uses, is particularly problematic.

The policy subject

Differences in operational definitions of the Internet, whether implicit or explicit, often underlie contradictory legal positions from different venues treating the same problem. When the Internet is seen as a marketing and distribution mechanism, for example, differentially pricing access to various websites (which undermines network neutrality) can seem appropriate. When the Internet is seen as a medium for political and other forms of free speech, however, backing away from network neutrality is highly inappropriate. Several pre-digital distinctions among ways of conceptualizing communications media for legal purposes remain important to Internet policy, though often with a twist. Here we look at two types of technologically driven differences as well as at the distinction between content and conduit (message versus medium) and the variety of issue areas involved.

Wired versus wireless Though digitization has made transitions between wired and wireless communications relatively easy for service providers and seamless for users, in the analog environment the difference between transmission of messages by wire (using the telegraph, and then the telephone, for telecommunications) and through the air, wirelessly (in radio and television broadcasting) was crucial to regulators. In most countries both types of systems were managed under the same regulatory roof, though usually in different work units and with different sets of regulations.

It is possible that techniques for communicating across the wired/wireless border would have developed more quickly had there not also been antitrust (competition law) concerns about organizations that engaged in both types of activities. In the US, the Kingsbury Commitment of 1913 forced corporations to choose one or the other, leaving AT&T with wired communications (and voice) and Western Electric with wireless (and data). Even so, from at least the 1920s on, broadcasters regularly leased telecommunications circuits to transmit program

content from one geographically based station to another. In the digital environment messages and data regularly flow across the wired/wireless divide, but the distinction retains regulatory importance in areas such as network security.

Broadcasting versus telecommunications versus speech There is a wide variety of approaches to regulating communications across states, but even within single societies several different legal frameworks can simultaneously apply to digital technologies even though the rights and responsibilities of each may conflict. In the US, three quite different approaches to regulating communications developed, each put in place to manage a different technology. (1) The First Amendment protects free speech and press, the right of association, and the right to ask for changes in the government. It developed in a print environment and is a matter of constitutional law. (2) Telecommunications regulation, managed by the FCC, was created to deal first with telegraphy, and then with telephony. (3) Broadcasting regulation, which applied first to radio and then to television, is also handled by the FCC, but under a second set of regulations.

Each of these systems started from a different regulatory assumption. For print, the fundamental principle was maximizing the free flow of information. For broadcast, the original approach treated those relatively few speakers with licenses as "trustees" with responsibilities to represent all speakers that justified constraints not applied to print. For telecommunications, the governing principle was common carriage with its two basic rules: service must be provided to all who desire it, and content should be transmitted untouched.

These three approaches yield significant legal differences, as exemplified by treatment of editorial control. Those who publish in print have complete editorial control over the content that is produced. In broadcasting, however, there are some editorial constraints because of trustee responsibilities. In telecommunications, there should be no editorial control at all. On the Internet, a single network provider almost inevitably carries all three types of content, yielding regulatory confusion.

The medium versus the message Since the first decades of the twentieth century, the law has distinguished between medium (the technologies that produce and carry communications) and message (the content of the communications) or, in an alternative phrasing, between conduit and content. Two different types of regulatory tools – structural regulation and content regulation – replicated this distinction in the law. Additional dimensions appear with the Internet.

Traditionally, the medium was managed through structural regulation dealing with matters such as network structure, pricing issues, interconnection, and rules for customer premises equipment. Technical standard setting (detailed specifications for technologies) was largely carried out by the private sector, even when this was accomplished under cover of international organizations. It was assumed that network architecture mapped onto organizational structure; each changed, if at all, slowly and in response to the actions of a relatively small set of players. In the digital environment, however, network structure is also a matter of software

that can change frequently and market entry is achieved through the contractual relations of ICANN's domain-name system. Many more players – potentially all Internet users – are involved in structural issues. Thus there is much greater awareness of the political importance of standard setting and network design as forms of regulation, strengthened by theories of and research on socio-technical development. On the content side, differences of scale rather than kind are so extreme that they qualitatively change the nature of regulated activities as well as the previously discussed perceptions of appropriate legal positions. As a consequence, governments are reconsidering when content regulation should be acceptable for the Internet.

In most countries, communication policy has long been used to regulate behavior, but this motive was rarely at the center of attention and affected relatively few people. Websites, however, often combine speech and action, so that regulation of speech is often a technique for regulating behavior. It is still important not to conflate the two; a gambling website involves both a contract for the website's domain name and, separately, legal permission for the gambling activity. Both types of legal arrangements are necessary, but they involve different processes, each under its own rules, and they can be carried out in different legal jurisdictions.

A final medium/message complexity is that in the digital environment it is often possible to choose whether or not a given set of material should be considered content or conduit. Software, for example, can be treated as a text, covered by copyright and replaceable by other programs in a computer or network. It can also, however, be hardwired into a machine, in which case it would be covered by patent instead of copyright, and it would not be replaceable by other programs in a given computer or network. As text, the program is content, or message; as technology, it is conduit or medium. Competitive factors often influence which form any given program will take.

One way of summarizing the medium/message distinction in the Internet environment, then, is to say that there are three processes through which the Internet is governed. Technical decision-making is conducted through a relatively informal "requests for comments" (RFC) process (http://www.ietf.org/rfc.html), open to anyone anywhere in the world, whether public or private, and through ultimate standard-setting processes that are more formal. ICANN (http://www.icann.org) manages the operations of the Internet. National and regional governments and international organizations make laws and regulations to govern uses of the Internet and the content that flows through it. It is the last subject that is the central focus of this chapter, though it is impossible to completely segregate laws and regulations from the contract system of ICANN and from technical decision-making.

Issue area Governments have always approached communication policy through the lenses of multiple issue areas. While military concerns provided the initial impetus for funding to create the distributed communications network we refer to as the Internet, other issue areas of importance for further Internet development included European concerns about vulnerabilities deriving from over-dependence

on US-based computing capacity and networks, Middle Eastern government desires to attract business to the region, US interest in a network to support scientific research, and African-country eagerness to bring rural areas into the capital-based economy. Corporations believed there were profits to be had in new forms of content distribution and efficiencies to be gained through Internet-based coordination of activities, and civil society groups recognized possibilities for diversifying public discourse and engaging in participatory democracy. Today, support comes from governments that see the Internet as critical for economic viability, international competitiveness, research and development, the delivery of government services, and national-security-related surveillance. Corporations use the Internet for internal operational purposes as well as external marketing and production input functions. Individual and community users perceive the net as an entertainment medium, a means of interpersonal communication, a political tool, and a tool for scanning the environment.

This diversity of issue areas matters because each frames legal issues in its own way. As a result, problems that may be singular from a sociological perspective are often the subject of laws or regulations generated by numerous different entities that put in place mutually exclusive rights and responsibilities. Internet speech involving the sexuality of children, for example, can be seen as an issue of criminal behavior of primary concern to the those in law enforcement; as critical educational content of interest to those in education; as a matter of free speech – whether by corporate producers of such content or by individual communicators – of primary concern from a constitutional law perspective; as an economic issue to vendors concerned about their ability to deliver services across jurisdictions, to be viewed through the lenses of commercial regulation; or as a matter of privacy, also a constitutional matter in the United States. No one of these should stand alone in analysis of the legal issue, as all concerns are legitimate. Rather, the range of interests needs to be taken into account and evaluations made regarding the value hierarchy that should dominate in resolution of any given issue.

Traditional Internet policy tools

Many legal tools available are considered inappropriate for communications because of the intimacy, social functions, and political valence of much content. A number of traditional communication policy tools, however, remain useful for the Internet.

Content regulation Content regulation constrains or forbids communications on the basis of message content. The kinds of content regulated vary across time, from country to country, and in response to shifts in the political, social, and cultural environments. In many countries there is a bias against content regulation because it impedes the free flow of information, but there is no country that absolutely protects free speech. Content that is commonly not protected includes that which is treasonous, libelous, or involves criminal activity. Many governments outlaw hate speech. In Thailand, it is forbidden to criticize the monarchy. In most

Islamic countries, criticism or parody of the Koran is illegal. Aside from these exceptions, policy must, in the language of US law, be "content neutral" – applicable irrespective of message content. Anti-terrorism laws are currently expanding the domains of restricted content in many countries around the world. In 2008, the European Commission criminalized content that suggests intention to promote or commit a terrorist act. Because these are very broad rules, and because they are vague and susceptible to multiple interpretations, it is unclear how far this will go. There have been several efforts in the US to claim that any expression of concern about damage to civil liberties is itself a form of support for the enemy.

Structural regulation When a policy intervenes in how a market, industry, or organization operates, it is referred to as structural regulation. For networks, technological design of the infrastructure is a form of structural regulation. Spectrum allocation – licensing specific types of communications to certain bands of the radiomagnetic spectrum – is an area of structural regulation over which there are intense struggles in the early twenty-first century because service providers would like to use the "white space" between portions of the spectrum given to analog broadcasting in order to expand wi-fi offerings. Antitrust law, regularly used against Microsoft, tries to prevent a single or a few corporations from inappropriately dominating the market. Policy precession in structural regulation can multiply its effects. Changing to a spectrum auction system in the US made it easier for large corporations to dominate the market in a way not traditionally the subject of examination on antitrust grounds. ICANN has put in place a parallel world of global structural regulation specific to the Internet with its division of the world into geographic and top-level-domain material and virtual spaces.

Time, place, and manner regulation Time, place, and manner regulation restricts communication under specific circumstances in a content-neutral way. Laws criminalizing disruption of networks are examples of Internet time, place, and manner regulation.

Contracts as regulation Contractual agreements among private parties can restrict content, legally (Braman & Lynch, 2003). ISPs typically do so in the end-user licensing terms everyone must agree to in order to gain access to the Internet. Sometimes users experience the results as direct censorship, as when even US-based ISPs refuse to transmit messages that take particular political positions. In other cases, those with an interest in civil liberties approve of ISP constraints on content such as hate speech. We are just beginning to see the complexities of where this can lead: provider claims that content must be "throttled" in order to meet service provision commitments that are also contractually based are one technique being used to undermine network neutrality.

Self-regulation Self-regulation takes place when an organization or association of organizations sets up rules regarding content some consider harmful to society.

(This can be a defensive measure undertaken to prevent government intervention.) Self-regulation can involve informal agreements not to distribute certain types of content, as when American newspaper editors agreed in the 1970s not to publish news of terrorist activity because it was understood that doing so stimulated further aggression. It can also involve setting up rating systems to help users or audience members avoid content to which they do not wish to be exposed, as the film and videogame industries have done. The Entertainment Software Rating Board is a self-regulatory organization that provides ratings, advertising guidelines, and online privacy principles for electronic games and other forms of online entertainment.

Balancing It is rare – perhaps never – that a particular legal issue involves only a single constitutional right or regulatory principle. Rather, balancing is an important legal practice that can be considered an Internet policy tool. At least three types of balancing are of concern for Internet law and policy. A content producer's right to property may come into conflict with an artist's right to free speech if the former believes that the latter has used content inappropriately, and these two rights must be balanced against each other. Historically, the First Amendment has been considered to have an acceptably heavy thumb on the balancing scale relative to other constitutional rights because of its importance to democratic practice, but in the twenty-first century national security concerns so far have the heavier thumb. Second, different stakeholders may come into conflict with each other on the basis of the same legal principle; conflicts over which corporation has the right to a particular patent can fall into this category, particularly when resolution of the conflict requires a conceptual distinction rather than matter of fact. Third, the same stakeholder may find him- or herself on different sides of the same issue at different times; university professors have an interest both in expanding fair use so that they can take advantage of the materials of others in the classroom and for research purposes, and an interest in strengthening intellectual property rights, to maximize the benefit from their own work.

Designation as critical infrastructure Defining the Internet as critical infrastructure has justified numerous interventions into network structure, content, and uses. This has a very long history; government uses of the network are always privileged, though often the impact on regulation and practice is not widely perceived. Today, this is at the center of public debate and political struggles over the Internet because of its utility for surveillance and concerns about information warfare.

New Internet policy tools

It should not be surprising that with each innovation, new ways of infusing practice, organizational form, and the material environment with techniques for enforcing the law should become available. Certainly with the Internet this has been so.

Deputization of private sector entities Because of their gateway functions, ISPs and ISP-like entities such as universities and public libraries are under an enormous amount of pressure to essentially serve as policing arms of the government. In the US, the first dramatic example of this came with the statutory requirement that ISPs should cut off users accused of copyright infringement from service. A particularly disturbing feature of this policy tool is that it reverses the assumption of innocence until proven guilty. Under the governing legislation (the Digital Millennium Copyright Act), the mere charge that someone is infringing is all that is required to cut someone off from the net, *before* legal evaluation of the validity of the charge takes place.

Technology design and network architecture Because technology design and network architecture are not only forms of social policy themselves, design features can also serve as policy tools. While those involved in Internet design often took privacy, security, and other policy issues into account, in the past this was often done outside of governmental frameworks and without legal oversight. Today there is deliberate use of such techniques by policymakers for a variety of purposes, including protection of privacy and facilitating use of the Internet for surveillance. One contentious example is the use of digital rights management (DRM) systems to embed particular interpretations of copyright law into technology design so that content cannot be viewed in what vendors believe to be an infringing manner.

Evidence as regulator One of the most fascinating developments in law–society relations has been driven by electronic discovery, subjecting electronic communications and files to the demands of the evidence-gathering process attorneys use to prepare for court cases. Working papers – documents produced in the course of work that are ephemeral in nature, emphasizing speculative, exploratory, partial, and/or intermediary stages of work processes – are typically exempt even when final work products must be produced. However, in most places corporate email is now subject to discovery, whether or not documents being circulated are working papers, final work products, or other types of communication. This has vastly expanded the amount of material subject to discovery, stimulating savvy organizations to redesign knowledge management and communication systems in order to maximize legal protection should a problem ever arise. This procedural matter, too, then, has effectively become a form of structural Internet policy.

What Internet policy is *not*

As the short history of Internet policy above suggests, the range of issues perceived to fall within Internet policy has been steadily expanding. Indeed, given that the Internet is involved in all social processes today, this could lead to an equation of Internet policy with all law. At that point the concept would have no utility. Thus it is worth marking boundaries as well.

Internet policy is not laws and regulations that apply to all digital technologies. Digital manufacturing technologies, for example, do not fall within the domain of Internet policy even if networked among themselves to facilitate interoperability. Ambient, or ubiquitous embedded, computing which fills our material and organic environments with communicating sensors and computational devices, would not fall within the domain. And the Internet is a sub-set of – not identical with – the global information infrastructure. There remain many uses of the global telecommunications network that do not involve the publicly available Internet, so Internet policy is not the same thing as telecommunications policy.

Where is Internet Policy Made?

Internet policy is made in numerous venues. This section looks at the jurisdictional problem, briefly introduces sources of Internet policy, and looks at the different types of Internet policymaking by governments.

The jurisdiction problem

Internet law and policy is made at every level of the legal structure, from the most local to the global. A legal jurisdiction is the geographic space within which laws and regulations of a specific government are in force; since the Internet is global, Internet-based activities always involve multiple jurisdictions.[8]

There are many areas of communication law in which multiple jurisdictions have long been possible or probable. Libel law, for example, is a matter of state (provincial) law in the US, so libel cases involving national publications always have a choice of jurisdiction within which to press a case. Satellite broadcasting caused many tensions between national governments over differences in content regulation and treatment of commercial content. Jurisdiction is thus another area in which the problem is not new with the Internet, but our experience of it has changed in the Internet environment because it is now endemic.

This presents several challenges. Interactions across levels of the legal structure can yield differences from one place to another in the legal context for a specific type of Internet-based activity or communication. It is also possible for differences in the stage of the information production chain – the distinction between content creation, processing, flows, and use – to affect the legality of any particular content or activity within a jurisdiction. The prohibition on Nazi content in Germany illustrates both of these. For a long while, Nazi content was being produced in the US (where hate speech is considered a protected form of political expression) and made available over the Internet to German receivers. When the German government turned its attention to a large-scale Internet service provider through whose services the content was being distributed within German territory, the private corporation elected to ban all such content everywhere it operated rather than be subject to the legal process in Germany. Ultimately, the European Court

of Justice determined that the German law could not be upheld in the Internet environment. A recent South African domain-name case presented a different example of how jurisdictional differences affect Internet policy. When the South African government felt that its intellectual property was being infringed by a corporation, it took the case to a US court for resolution, believing – correctly, as it turned out – that this choice would be favorable to its case.

Internet policy across levels of the legal infrastructure

Internet policy is inherently global since it is a global information infrastructure, a network of networks. But the global is experienced only under local conditions; Internet policy is also, therefore, made at the level of municipality as well as within organizations and homes. In this section we look briefly at all of the sources of Internet policy other than those of national governments, the subject of the next section.

Global The desire for a global communications network has long been an important spur to the development of new forms of regulation that cross state borders. It was the telegraph that inspired the formation of the first international organization in the 1860s – what we now know as the International Telecommunications Union (ITU, http://www.itu.org). Similarly, the Internet has lead to the formation of the first global organization, ICANN (http://www.icann.org). An international organization is comprised of representatives of geopolitically recognized governmental entities (states), but in global organizations civil society entities such as non-governmental organizations (NGOs) and corporations also have a voice in decision-making.

ICANN was born in a decision by the US Department of Commerce in 1998 to establish an entity at arm's length from the government. The result was a private not-for-profit organization incorporated under California law. Decision-makers came from the private sector, and decision-making took place in secret until pressure from civil society groups concerned about the public interest succeeded in achieving greater transparency. ICANN has operated under the oversight of the US government, in recent years under terms that made it possible to completely privatize the organization should certain conditions be met. At the time of writing, it is still unclear what form ICANN will ultimately take. Some argue that the time for complete privatization has come, but others claim that the organization has failed to serve the public interest and needs to remain under governmental oversight. Options involving the public sector include remaining under US control, putting the organization under the rubric of the ITU, itself a part of the United Nations (UN) system. Recently, an ITU-sponsored multi-year process – the World Summit on the Information Society (WSIS) – concluded with the creation of a new forum for multi-stakeholder policy discussions, the Internet Governance Forum (IGF), a venue for policy discussions that has no actual authority. Another option is to allow other countries besides the US – Brazil and China

have pursued this with particular eagerness – to become active in ICANN governance mechanisms. Whichever way it goes, many extremely important issues will remain, particularly in the areas of public accountability and democratic representation of the interests of all in decision-making.

Effects of current ICANN rules include constraints on free speech via the end-user licensing agreements (EULAs) contractually required in order to access the Internet by Internet service providers (ISPs) and ISP-like entities; intersections between domain names and other forms of intellectual property rights; and invasions of privacy enabled by the domain-name system. Many believe that the constitutional or constitution-like principles underlying the law in most countries should also apply to ICANN's decisions, particularly in the area of civil liberties (Froomkin, 2000). EULAs give ISPs the rights to prevent users from accessing the system, censor content, or use content for otherwise unauthorized commercial purposes in ways that would be considered unconstitutionally vague and overbroad under US constitutional law. One can legally choose to sign away one's rights by contract, but historically that has been available in contexts in which one can also choose *not* to do so because other types of contractual arrangements are available. EULAs are becoming more and more like each other in content, and more and more restrictive, with the consequence that it is essentially impossible to choose a means of accessing the Internet through an access provider that provides the full range of speech and related protections available in all other communicative contexts under the US Constitution.

International Several international organizations make Internet policy directly and indirectly. Treaties are the basis of these activities, whether multilateral (obligatory for all participants, or members, of the organization), plurilateral (binding only a sub-set of the members of an alliance), or bilateral (two-party).

Long-standing responsibilities of the ITU for technical standard-setting remain key. The ITU is also involved in development activities through efforts such as those of the Applications and Cybersecurity Division, which works with developing countries to improve infrastructure capacity and security; and work in areas such as e-government, Internet multilingualism, and uses of the Internet for healthcare. Regional meetings within the ITU framework provide support for other national- and regional-level Internet policymaking.

The World Trade Organization (WTO) was created in 1995 as a managerial home for the international trade system first created after World War II and significantly changed in the 1990s. Formation of the WTO was very much a product of the transition to an information economy, driven by the need to expand the trade system to cover not only goods (via the General Agreement on Tariffs and Trade, or GATT, in place since the late 1940s) but also information processing and related services (via the General Agreement on Trade in Services, or GATS), and to treat more systematically the trade dimensions of intellectual property rights (via the Trade Related Aspects of Intellectual Property Rights, or TRIPS, agreement). Each country develops its own package of proposals for

consideration by the WTO. These packages include multiple policies, distinguished by industrial sector, type of economic or social vulnerability, and the techniques used to constrain trade. Within each of these areas, there are agreements specific to each service or product. Telecommunications agreements, for example, have an impact on rates that in turn affect the cost of network access to the Internet, and agreements that cover trade in computing and networking equipment affect the cost of equipment used to use the Internet.

Regional When multilateral treaties cover a broad purview they effectively create an additional layer of legal infrastructure between the international and state levels. The most comprehensive of such regional legal entities is, of course, the European Commission (EC). Other regional entities created by multilateral treaties with such features include those of the North American Free Trade Agreement (NAFTA) and the Association of South East Asian Nations (ASEAN). Within the ICANN system, regional groups also establish policies that differ from each other in areas such as which elements of the Internet are deemed to be critical infrastructure. Other regional groups focus more broadly on networking issues. Civil society groups actively contribute to the regionalization of Internet policy efforts. Two examples of regional groups that make Internet policy are briefly introduced here.

The European Commission (EC) has laws and regulations that affect the Internet in three ways. In the area of regulating the market, EC network policies attempt to reduce levels of spam and cybercrime, manage the spectrum, and prevent negative health-related effects of electromagnetic fields. Policies dealing with copyright, web accessibility, and regulation of the audiovisual industry affect Internet content. EC policies that stimulate Internet development include those dealing with taxation of Internet service and e-commerce, research and development, and use of the net to pursue social goals such as improving the quality of healthcare and education. The i2010 Initiative brings many of these policies together under a single rubric, and international dimensions of what the EC is doing in this area are a part of its international relations program.

In 2003, ASEAN brought together diverse regulations dealing with Internet-related matters in the Singapore Declaration, an action agenda devoted to using ICTs to promote digital opportunities within ASEAN countries and enhancing their competitiveness. Issues such as network interoperability and interconnectivity, security, and data integrity are key. Harmonization of Internet-related laws across ASEAN countries, reduction in tariffs on trade in the technologies involved, and collaboration on cyber-security issues are seen as major ways of improving the environment for users. Stated goals include reducing the digital divide within ASEAN countries as well as improving the infrastructure.

Sub-state policy In most countries, there are several layers of additional decision-making about Internet-related matters below the level of the national government. In many cases, laws and regulations dealing with a specific subject may exist at multiple levels of government and governance within a single state. The

provincial, municipal, organizational, and domestic environments are of particular importance.

Most countries have laws and regulations at the provincial level that pertain to the Internet. In Canada, for example, provinces have data protection laws in addition to those of the federal government. In Germany, the Länder (states) are responsible for the research and development that results in innovations in Internet technologies. In some cases these are laws that are put in place only at the provincial level, while in others the same laws can be found at the national level as well. Access to government information laws, for example, are found at both the state and national levels in the US.

Municipalities (legally defined urban areas) are sources of Internet policy in multiple ways. Municipalities have regulations (in the US these are called ordinances) regarding protection of personal data about citizens and their activities, access to information, and other e-government issues. In many countries, municipalities support public libraries through which citizens can gain Internet access. The municipal issue currently receiving the most attention is the establishment of community-wide free public access to the Internet through a wireless network.

Community wi-fi access provides a good example of ways in which contemporary debates over Internet policy often repeat battles that have come before and from which we can learn, as municipal wi-fi struggles echo those over municipal control over cable networks of several decades ago. In the case of cable, municipalities had a deep interest because putting in the network involved changes to existing infrastructure – streets had to be dug up and new equipment was installed on existing buildings themselves subject to zoning and other regulation. For the same infrastructure reason, it was long argued – as it had been with telephony and telegraphy – that cable was a "natural" monopoly, and licensing cable systems was a source of revenue for municipal governments. Challenges to municipally governed cable networks came from vendors who saw themselves as possible competitors to licensees but who were forbidden market entry in monopolistic city environments. First Amendment challenges were pressed against municipal limitations on access to television content and the inevitable sole-sourcing of televised government proceedings that was a concomitant of the public service channel requirements of municipal cable franchises. Ultimately, the municipal cable issue was made moot by the appearance of competition from satellite television and, with digitization, the ability to transmit cable content via the telecommunications network rather than a second, cable-specific network.

Given the technical nature of wireless networking, infrastructure issues remain important, but in a different way. Nothing needs to be dug up, but a system of transmitters does need to be put in place, and concerns over such matters as the health impact of these transmitters (10 percent of the population is extremely sensitive to the wavelengths involved) also suggest that municipal regulation remains important. The larger issue at the center of debate, however, is again the competitive matter. Opposition from telecommunications providers who see in free or low-cost municipal wi-fi a loss of ISP subscribers has so emphasized

the cost of building such networks that decision-makers in many cities have become shy of the process. Institutions such as universities that consider offering community-wide access are often scared away by attendant legal responsibilities for uses and content. Meanwhile many businesses see offering free or low-cost access to wireless networking as a competitive attraction, community groups sometimes make access available in service to other aspects of their mission, and many individuals are happy to leave their personal wireless transmitters unprotected so that others can take advantage of the signal. After a period of widespread enthusiasm, and a shorter one of dismay and reluctance, it is still too early to know the extent to which we will see municipal wireless networks in future.

National governments and Internet policy

Within each country there are many different ways in which laws are made, ranging from executive fiat at one extreme to votes of the entire population in plebiscites at the other. Within the US, the four most important ways of making law each bring a different type of knowledge, decision-making process, and perspective into the legal system.

Constitutional law Fundamental policy principles are put forward in constitutions, or constitution-like documents. These go under many different names. In Germany, for example, it is the Basic Law, interpreted by the Federal Constitutional Court in response to petitions from federal bodies, government officials, or citizens. In Britain there is no written constitution *per se*, but an unwritten constitution is comprised of fundamental principles of enduring importance and consensual acknowledgment.

Law at the constitutional level is based on philosophy, social theory, and beliefs about the nature of society and of democracy. While other types of law deal with existing social categories and relations within and between them, it is the job at the level of constitutional law to define the very categories through which we will relate to each other and to establish the constraints and responsibilities for just how those relationships unfold. Because communication law creates the conditions under which all other types of decision-making take place, it can be argued that all Internet policy is of constitutional status.

The US Constitution includes 20 principles that should underlie Internet policy (see Table 7.1). Constitutional law changes via court interpretations of the law (in the US, any court can deal with constitutional issues, though in many other countries this can only be done in special constitutional courts), and through amendments to the Constitution. The First Amendment to the US Constitution, which provides the foundation for freedom of expression in that country, requires "state action" – governmental responsibility for laws, regulations, or activities affecting freedom of expression. If the government is not involved in a particular activity or restriction, the First Amendment provides no protections.

Table 7.1 Internet Policy Principles in the US Constitution

Principle	*Location*
Information collection by the government	Art. 1, sec. 2
Open government	Art. 1, sec. 5; art. 2, sec. 3
Free speech within government	Art. 1, sec. 6
Federal government control over currency	Art. 1, sec. 8
Universal access to an information distribution system	Art. 1, sec. 8, cl. 7
Intellectual property rights	Art. 1, sec. 8, cl. 8
Restriction of civil liberties during time of war	Art. 1, sec. 9, cl. 2
Treason	Art. 3, sec. 3
Freedom of opinion	1st Amend.
Freedom of speech	1st Amend.
Freedom of the press	1st Amend.
Freedom of assembly and association	1st Amend.
Freedom to petition the government for change	1st Amend.
Privacy	1st Amend.; 4th Amend.
Right to receive information	Art. 1, sec. 8, cl. 7; 1st Amend.
Protection against unlawful search	4th Amend.
Protection against self-incrimination	5th Amend.
Due process	5th Amend.
Rights beyond those enumerated	9th Amend.
Incorporation of federal constitution into state constitutions	14th Amend.

Statutory law Statutory law translates general constitutional principles into laws, or statutes. Statutory law is created by parliamentary entities such as the US Congress (the Senate and the House of Representatives, at the federal level) and by legislatures (at the state level) or, in Germany, the Bundestag (representatives of the people) and Bundesrat (representatives of states). Statutory law is considered the product of representative democracy because it is created by representatives who have been elected to serve as lawmakers, though of course many forces in addition to popular opinion influence statutes. Statutory law changes through amendments to existing laws, replacements of existing laws, addition of new laws, development of programs or institutions through which to implement the law, or as a result of interpretations of the law made by judges in court cases. The USA PATRIOT Act, passed after the terrorist attacks of September 11, 2001, is an example of statutory law that has had enormous impact on Internet policy. There are many other recent examples of statutory Internet policy, including those that are manifest (such as the spam-fighting CAN-SPAM Act of 2003) and those that are latent (such as the Central America Free Trade Agreement, which requires countries to bring their laws into line with US laws requiring ISPs to withdraw Internet access from those accused by rights holders of infringing copyright).

Regulatory, or administrative, law When decision-making in a particular area requires detailed technical knowledge and must be made over and over again, Congress uses statutory law to set up a regulatory, or administrative, agency to put in place regulations that have the force of law. Regulatory law brings technical expertise into the legal system. These agencies bridge all three branches of government, for they report to the White House and those in conflict submit to decisions by courts, if resolution cannot be reached through internal agency processes. When very large issues appear – such as in the current debate over media concentration – Congress can step in and assert its will.

A number of agencies regulate certain kinds of content; the Food and Drug Administration (FDA), for example, requires publication of specific information about things we take into or put onto our bodies, and has rules for how such things are described in the media. The FCC has already been mentioned. Other administrative agencies in the US key to Internet policy include the Securities and Exchange Commission (SEC), which regulates financial information of publicly held corporations (corporations that sell their stock to the public); and the Federal Trade Commission (FTC), which regulates advertising and marketing practices.

Common, or case, law Common law is the history of decisions made by judges when legal issues cannot be resolved outside of a courtroom. The impact of decisions in lawsuits extends beyond parties to the case because court opinions provide precedent that must be taken into account in future when conflicts involving related issues arise. Case law has been extremely important to the protection of civil liberties in the Internet environment, and in recent years has been key to pushing back against unconstitutionally repressive statutes. Public interest non-profit organizations concerned about Internet policy, such as the Electronic Frontier Foundation (EFF, www.eff.org) and the Electronic Privacy Information Center (EPIC, www.epic.org), devote a great deal of their energy to participating in such lawsuits.[9]

The "Big Four" Issues

A few policy issues deserve special attention because they create the conditions for all Internet activity and must be addressed by every country. Because these are such complex issues, each can be framed in many different ways and is addressed by numerous policymaking entities. All affect freedom of expression and access to information.

Access to the Internet

The phrase "digital divide" refers to problems generated by unequal access to the Internet; the divide appears both within and across societies. This metaphor

involves one dimension of what sociologists have for many decades referred to as the "knowledge gap," the mutual reinforcement among lack of access to knowledge, lack of political efficacy, and low socioeconomic status.[10] The dimensions of access are multiple; in most countries separate laws and regulations are needed to address each facet separately.

Physical access Physical access involves access both to the network itself and to the interface through which one accesses the Internet. This is often an economic issue as well as a geographic one.

Access to network infrastructure falls under the purview of governments and/or of large-scale corporate vendors as they operate within the regulatory parameters of governments. "Reach" is the extent to which the network is available across space, and "penetration" is the extent to which the population in an area in which the network is available actually does access it. Where the network is under government control, both can be accomplished with particular effectiveness, as in South Korea. Under the more common competitive conditions, governments intervene to encourage widespread diffusion of geographic access to the network through techniques such as establishing conditions for a license, pricing mechanisms, and laws requiring public access at the community level.

Governments and vendors are also involved in access to network interfaces, but because such interfaces may be available at the community or household level as well as the individual level, other types of groups can also have an impact. In both developed societies and developing societies governments support community-level access, whether through libraries, schools, or "tele-centers," to ensure that those who do not have personal access can still use the Internet. Many different kinds of technologies can serve as the Internet interface. In Italy, for example, use of the Internet did not become widespread until it was available through cell phones and that technology itself had become fashionable. "One laptop per child" initiatives seek to expand access to the network interface in developing societies by producing very inexpensive laptop computers, with governments signing contracts to purchase these in large numbers for their schoolchildren.

Those with physical disabilities face additional access barriers. Internet policies to address this problem include establishing usability standards for websites and support for research and development to create technologies that serve those with specific disabilities.

Education Several types of literacy are also key to Internet access. *Traditional literacy* is the ability to make sense out of messages communicated and to create meaningful messages. Because the concept of literacy arose in the print era, it historically referred to reading and writing. Today, however, the importance of images is also acknowledged, leading to *media literacy* as a distinct category. *Information literacy* is the ability to locate, evaluate, and use information in diverse forms, and to create and communicate valid and reliable information. And *technology literacy* is the ability to use technologies to achieve one's goals, including learning

how to do new things with those technologies. All of these are necessary for full use of the Internet.

Historically we have distinguished various levels of traditional literacy. Functional literacy – the ability to read and write as necessary to get through the activities of daily life, including reading signs, locating items one needs to buy, and filling out employment and government forms – is one end of a spectrum. At the other, *avant garde* writers have such mastery that they push language and narrative form forward into new realms. The functional end of the media literacy spectrum involves being able to not only understand mass media programming, but also to discern motives behind such messages and their political economic implications. At the most sophisticated end of the media literacy spectrum are those who produce content that achieves a mass audience, though increasingly the ability to produce at least simple media content is being defined as necessary for all. At one end of the spectrum of information literacy is the ability to locate and evaluate information, and to manage information of importance to oneself; at the other end of this spectrum are those who design and manage large-scale information architectures for large populations and multiple uses. In the world of technological literacy, the functional end of the spectrum would include being able to engage in basic functions such as word processing, surfing the web, and managing email, while at the other end of the spectrum are those who are writing their own code for specific purposes.

All these forms of literacy become the subjects of Internet policy when standards for at least functional levels of mastery are included in education systems and training is provided at government-supported public access centers. Traditional literacy has long been the focus of primary, secondary, and tertiary education, but today media, information, and technology literacy are also increasingly taught at all three levels. Technology transfer programs can serve this Internet policy goal as well when they include knowledge transfer elements.

Cultural access Cultural preferences can generate barriers to Internet use that, in many societies, become the subject of Internet policy. It is a complex area for Internet policy, because regulations intended to break down one barrier can raise others. In South Africa, for example, the government required two managers for each publicly supported tele-center, one of whom had to be a woman, but in many tribal areas gender differentiation is so powerful that the presence of a woman prevented men from using the tele-centers. Successful examples of government policies to reduce cultural barriers to access include support for the creation of web content from marginalized communities, ensuring that culturally based geographic isolation does not prevent access, and efforts to make it easier to use the Internet across languages and alphabets.

Access to content

Once access to the Internet has been achieved, access to content becomes important. Conditions of access, the issue currently popularly labeled "network neutrality," and censorship are key Internet policy issues in this area.

Conditions of access Governments place a variety of types of constraints on the conditions of access in pursuit of diverse goals, beginning with the limits to freedom of expression in any medium discussed above. Some constraints are Internet-specific; China, for example, limits the amount of time one can spend online per day in an attempt to fight Internet addiction. Organizational and public sites for access to the Internet can forbid certain types of activity (e.g., gambling) or access to particular categories of content (e.g., pornography). Parents may insist on devotion of a certain percentage of time on the Internet to educational activities.

While these are all highly variable, conditions of access established by the terms of service, acceptable use, and licensing agreements now collectively referred to as end-user licensing agreements (EULAs) are ubiquitous and contain many features that are uniform across countries and access sites. The conditions of access these put in place, discussed in more detail above in the description of ICANN's law-like impact, can run directly counter to national law and constitutional principles. These, too, are slowly being tested in the courts, with transnational courts playing particularly important roles.

Network neutrality Basic common carriage principles, combined with the value to the network of expanding the network itself, have up until this point ensured that all websites could be reached with the same ease and speed whether they were associated with the world's largest corporation, a retail store, a non-profit organization, or an individual artist or political activist. The phrase "network neutrality" is used to describe this situation.[11] While everyone has experienced delays in reaching certain sites, or at times found them unavailable, these time differentials have resulted from technical difficulties. There can be too much traffic on the network, or a portion of it, slowing everyone down, or the server hosting a particular website may be down.

In the US, however, there is currently a very tense debate over legislation proposing an end to network neutrality. Network providers are seeking the right to slow down your access to websites that have not paid special fees to ensure favorable treatment. There are fears that in some cases ISPs might make it altogether impossible to reach certain websites. If network neutrality is lost, ISPs in essence have the legal right to censor Internet content. The extraordinary diversity of voices and information available – the most important characteristic of the Internet for many – will have been destroyed. Even when it may still be possible to access websites of small, independent, or politically marginal groups more slowly than other websites, research on surfing habits suggests that the time difference is experienced as a difference in ease by users and it is likely that traffic to those websites would go down. There are already numerous well-documented reports of these types of activities by ISPs in countries around the world, including the US; often these ISPs admit to such activities when they are made public, either explicitly or implicitly by stopping the practices about which complaints have been received.

Users set up their own conditions of access to content when they use filtering software to prevent access to categories of websites considered undesirable. Most such software programs base their decision-making rules on computerized

analysis of texts, leading to the problem that perfectly safe – even highly desirable proactive content – may also become unavailable. Software that tries to prevent access to pornographic websites, for example, may also bar access to sites dealing with adult education or support for those with breast cancer. Some filtering software uses decision rules put in place by individuals who examine sites for their acceptability from a particular perspective such as those of specific religions.

Property rights

One of the most fascinating Internet developments has been the creation of entirely new forms of property that expand the boundaries of the economy itself. The transition from an industrial to an information economy has also brought very old forms of intellectual property rights to the center of the economic system and stimulated transformations in how those rights are managed. This issue is so important that it is worth separately thinking about expansion of these rights and about current efforts to correspondingly restrict them through fair use when doing so serves other social goals. A third set of changes to property rights occurs where intensification and expansion of interest in previously existing non-intellectual forms of property has altered how such property is conceptualized and treated.

Expansion of the property system This is not the first time in history that new forms of property have appeared, but the process is relatively rare and always accompanies significant change in the nature of society. Two examples of this with import for Internet policy are the domain-name system and property in virtual worlds.

We don't buy the street addresses for our homes and businesses, but the domain names that are the addresses for our sites in cyberspace are bought and sold. Creation of the domain-name system managed by ICANN generated billions of dollars, and the amount is still growing. Numerous policy issues have arisen in association with domain names. Those resolved by ICANN include identifying which organizations within regions and countries will be allowed to generate funds through domain-name related transactions. Domain-name issues resolved in national courts include struggles over the use of trademarks in domain names and efforts to stop cybersquatting, the practice of purchasing domain names incorporating the names of others with the hope of then reselling the domains at a profit.

Complex interactions between virtual property, capital within virtual games and worlds, and capital in the offline world raise a number of legal issues that governments have yet to resolve. Should national laws and regulations regarding financial matters be applied to operations within virtual worlds? How is offline income generated through virtual-world activity to be treated for taxation purposes? Should employment laws be applied to those who engage in virtual-world activity to generate either in-world or offline capital for their employers? Should the law intervene in the industry of cheating in electronic games?

Transformations of intellectual property rights There are four types of intellectual property rights – copyright, patent, trademark, and trade secrets – and all four have undergone changes. Copyright establishes a bundle of separable property rights in symbolic expressions such as texts and images; this bundle includes the rights to reproduce the work, to prepare derivative works based upon the original, to distribute the work, to perform the work publicly, and to display the work publicly. In recent years the duration of copyright has greatly lengthened; in the US, instead of the original 17 years owners can now control uses of copyrighted materials for almost 100 years. Techniques for enforcing copyright have become embedded in digital rights management (DRM) technologies, and it is relatively easy to track who is downloading what content over the Internet. Associations of copyright owners, such as the Recording Industry Association of America (RIAA) have become extremely aggressive about pursuing those whom they believe are infringing copyright. All of these are Internet policy issues because they affect what we can access over the Internet, and what we can do with material once we find it.

Patents establish property rights in three categories, two of which are pertinent to the Internet: utility patents protect processes, machines, articles of manufacture, compositions of matter, and genetic manipulations of animals; and design patents protect the ornamental appearance of objects. Internet technologies each involve numerous patents, almost always under the control of different corporations. Disputes over patents, some claim, slow innovation, and we are increasingly seeing corporations trying to assert that entire classes of activity such as one-click shopping have been patented. Many believe that software underlying ways of conducting business or communicating with each other should not be patentable, but under current law this is possible. The number of patents sought, the lack of pertinent expertise within patent offices, and massive confusion over whether or not there is "prior art" – previously existing patents on aspects of products or services being presented as new – have lead to calls for reform of the patent system altogether. Meanwhile, the open-source software movement has inspired experimentation with public opportunities to contribute to evaluation of whether or not there is prior art for any given new product or service.

Trademarks protect the name or image associated with the product to which they are attached; service marks do the same for services. Legal issues involving trademarks arise in the Internet environment when trademarks are incorporated into domain names or used for avatars or other creations within virtual worlds.

Trade secrets are types of information owners try to prevent others from using through non-disclosure practices. Historically corporations have had the legal right to try to protect trade secrets, but today's electronic discovery practices make it much more difficult to do so.

Fair use Fair use is the concept that there are limits to the extent to which owners can prevent others from using their intellectual property when, under certain conditions, the use of that property serves social goals of particular importance.

Historically, fair use has been central to copyright law, though today there is also discussion of developing fair use principles for patents. In the US, to qualify, uses of copyrighted material must actively transform the material, serve social goals such as education or promoting public discourse about political affairs via the news, and not damage the market for the copyrighted work. Because it is often difficult to determine whether many of the new Internet-based genres and communicative practices meet these criteria, currently there are efforts underway to establish consensual norms among communities of practice to serve as guidelines for courts.

Privacy

Privacy laws have always been sensitive to technological innovation, with each stage of the development of new information and communication technologies triggering evolution in pertinent regulation. Privacy is considered a fundamental human right because it is essential to many of our most profoundly human activities as well as to our ability to exercise many other rights, including free speech, association with others, and property ownership. In many countries legal protections for various forms of privacy are spread across many different laws and regulations in addition to appreciation of privacy torts. Both governments and private sector entities (most often, corporations) threaten privacy on the Internet. Among the many forms of privacy, those involving communications, anonymity, and data protections are particularly important for Internet policy.

Communications privacy Communications privacy involves the right to protect interpersonal communications from being accessed by people who are not intended parties to the conversation. Historically, democratic countries have protected the privacy of face-to-face conversations in the home and other places in which there is a legitimate expectation of privacy; in letters and phone calls; and in conversations with professional advisors such as physicians, religious confessors, and attorneys. When governments have felt the need to access such communications to pursue criminal activity or behavior that threatens national security, evidence of probable cause – sufficient evidence-supported reasons to suspect the individuals involved – was required in order to gain permission to access such interpersonal communications. Repressive governments, on the other hand, used techniques such as opening mail, listening to telephone conversations, and encouraging citizen reports on the conversations of others as a means of invading communications privacy. In many countries, citizens were even required to register their typewriters, each of which produces a uniquely identifiable text, making it impossible to communicate interpersonally in an anonymous manner. (Today unique identifiers for digital printers can serve this function.)

The digitized and networked information flows of the Internet make it much easier than ever before not only to access interpersonal communications efficiently, but also to analyze them for the appearance of particular words, phrases,

concepts, and interpersonal relationship networks. While in the past interpersonal communications were targeted for governmental surveillance only after an individual's behavior raised suspicion, in the Internet environment the reverse is the case: it is possible to collect all communications and identify individuals of interest through data analysis rather than behavior. Despite the ease with which such activities can be undertaken, the law stood in the way of massive surveillance of interpersonal web-based communications until 2001, when anti-terrorism concerns came to the fore. As is always the case in any country, national security concerns can be used by governments to reduce the scope of civil liberties as a means of defense. Though civil libertarians continue to push back against this development, at the time of writing in 2009 anti-terrorism laws support government surveillance of email and other forms of web-based communication. Policy tools used to accomplish this include such techniques as requiring ISPs to keep all traffic that flows through them for periods of six months to two years and dropping any requirement that specific permission should be needed to surveil the communications of any specific individual or group.

Corporations are also interested in reducing the scope of communications privacy because information about what people are saying to each other has marketing value. Emails are a medium for "viral" marketing, reveal clusters of consumption preferences, alert marketers to social networks of demographic importance, and enable the refinement of niche marketing. Interpersonal communications also provide ISPs with salable content, since end-user licensing agreements can give ISPs the right to use content of anything sent through their systems, including personal emails, for commercial purposes. One of the first examples of this was a website charging for access to salacious emails sent by a particular ISP's users.

Anonymity Anonymity protects the privacy of a communicator's identity. In the United States, anonymity is constitutionally protected because it is believed necessary for free and open discourse about political issues that may include strong critique. It is also considered necessary to protect "whistleblowers," individuals who want to report wrongdoing by either public or private sector entities the activities of which are damaging to society.

The Internet has created new types of pressures to forbid anonymity, including most importantly the need to authenticate identity for e-commerce and e-government purposes, and to identify those involved in criminal activity using the net. Internet users actively give up anonymity when they sign into their ISP accounts, and passively when the network acquires the "IP address," an address for the computer being used to access the Internet, in order to complete a connection. Cookies, which gather user data – including personal data entered into website forms – that is often shared across websites, also reduce anonymity unwittingly. The political and whistleblowing arguments for permitting anonymity remain, however. The ease with which web-surfing habits can be observed has added another – people should be free to learn about issues such as mental illness and sexually

transmitted diseases without suggesting to authorities that they themselves have such problems or are engaged in activities that might lead to them.

There are both legal and technological approaches to protecting anonymity online. Techniques such as encrypting your email and directing your web traffic through anonymizing websites, search engines, or software are available to the average user and can increase anonymity. Legally, debates over whether or not all Internet communication, or at minimum communication of particular types, should be permitted to be anonymous, continue. Legal and technical approaches to anonymity come together in the development of networking technologies that create trust relationships, authenticate identity when necessary, and permit anonymous communication in all other circumstances.

Data privacy The phrase "data privacy" refers to information about individuals, whether that is data about finances, health, transactions, or reading and surfing habits. The EU has lead the way in developing umbrella data privacy directives that cover all types of personal data; at the other extreme, in the US there are different data privacy regulations for each type of personal information. Invasions of data privacy may merely be embarrassing, but they can also have far-ranging consequences. Access to the personal data of others facilitates identity theft and a variety of types of fraud. Misuse or falsification of personal data may make it impossible for the victim to buy a home, get credit, graduate college, or take a particular job. The ability to identify groups of people with particular medical problems makes it possible to "redline," or refuse to offer services of specific types to those perceived to have raised risk levels. Illegal access to personal data can have free speech implications when surveillance agencies treat as suspect anyone who reads particular texts or websites. Corporate access to personal data can target victims as subjects of marketing campaigns that may be unwelcome.

Data privacy is an area in which organizational, community, and personal practice are particularly important. Sometimes data privacy is invaded deliberately, but often it happens accidentally, through loss of a laptop or memory stick, mistakes in hardware and software system design, and inadequate training on the part of users. Responsibility for implementing practices to protect data privacy is incumbent upon every individual and organization.

Conclusions

Today it is hard to imagine an activity, social process, or type of communicative content that does not involve the Internet, so from one perspective the domain of Internet policy is co-extensive with the entire legal system. More practicably, we can define Internet policy as those laws and regulations that are either specific to Internet infrastructure and its uses or apply to long-standing legal issues that have so qualitatively changed in nature in the digital environment that significant changes are required of the legal system.

The impact of the Internet on the law is enormous and profound. It is an important stimulus to and facilitator of changes in law–society–state relations so fundamental that many legal scholars and political scientists believe a complete transformation is underway. More immediately, the functions of particular elements of the legal system are changing places. The subjects of regulation (technologies) are now being used as policy tools. The digitization of possible evidence that might be considered in the resolution of legal disputes has reoriented organizations away from the front end (laws themselves) and towards the back end (dispute resolution) of the legal process in terms of design of practices and information systems. Private sector entities such as ISPs are being deputized to serve law enforcement functions. And private law, through the flow-down contract system of ICANN, now provides precedent for and the vessel within which public law around the world operates and is evolving.

The multiplicity and variety of decision-making venues of importance present enormous challenges to those who seek to protect civil liberties and human rights in the Internet environment. For many issues, long-standing practices of participatory democracy are irrelevant at worst, or ineffective at best. One of the points of greatest leverage in these areas may be including an understanding of the basics of Internet policy in information/media/technology literacy courses that should be required of all students.

Still, there are key battles to be fought at the state level through familiar political processes. The "Big Four" Internet policy issues – those that shape the context for all other pertinent activity and policymaking – are access to the Internet itself, access to content and activities on the Internet, intellectual property rights, and surveillance and privacy.

Notes

1 For an excellent introduction to the range of types of policy analysis, from cost-benefit calculations to examination of discourse frames, see Schön and Rein (1994).
2 *Command Lines: The Emergence of Governance in Global Cyberspace* (Braman & Malaby, 2006) examines some of the ways in which practices within virtual worlds interact with and affect the law.
3 For the history of this process in the United States, and discussion of the various ways in which the boundaries of the domain of communications policy have been conceptualized, see Braman (2004).
4 For detailed discussion of the pre-history and early years of Internet policy, see Braman (1995).
5 For a well-written, accessible, rich, and still useful discussion of the various regulatory frameworks under consideration for digital networks by countries around the world during the 1980s, written by attorneys who were particularly influential, see Bruce, Cunard, & Director (1986).
6 The first book with "Internet law" in its title was Chissick's *Internet Law: A Practical Guide for Business* (1997). Most of the first wave of such books was, like this one,

aimed at business users. The second wave of books with the phrase in the title was comprised of coursebooks for continuing legal education seminars. The first casebook for law schools with the phrase in the title was Chris Reed's *Internet Law: Text and Materials* (2000). Internet issues, however, appeared in casebooks on topics such as telecommunications regulation and freedom of expression much earlier as units dealing with "electronic media," "new media," and "new technologies," and casebooks appeared earlier dealing with electronic commerce, software, etc. Influential contemporary casebooks on Internet law and policy include Radin, Rothchild, & Silverman (2006); Lemley, Merges, Samuelson, & Menell (2006); and Maggs, Soma, & Sprowl (2005). For legal analyses from the perspective of mutual interactions between law and society, see Berman (2007).

7 Robert Horwitz's *The Irony of Regulatory Reform* (1989) provides the essential history of network regulation in the United States that is the context within which Internet policy has developed. Historians of technology Mowery and Simcoe (2002) explain why US law has been particularly important even though technical development of the Internet began in the UK and many innovations critical to its success have come from and continue to be developed in other countries.

8 A succinct introduction to jurisdictional issues can be found in Zittrain (2005).

9 The websites of these and other non-profit organizations are particularly valuable sources of information on Internet policy issues – what they are about, what arguments are being put forward, what the technological foundations of these issues are, etc.

10 A good introduction to the knowledge gap literature can be found in Vishwanath & Finnegan (1996) and Kwak (1999).

11 Legal scholar Timothy Wu, who coined the phrase "network neutrality," has a particularly useful webpage that explains the basics of the issue and provides links to a selection of scholarly articles presenting diverse perspectives about it, on his website at http://www.timwu.org/network_neutrality.ht.

References

Berman, P. S. (ed.) (2007). *Law and Society Approaches to Cyberspace*. Aldershot, UK: Ashgate.

Braman, S. (2009). Globalizing media law and policy. In D. Thussu (ed.), *Internationalizing Media Studies* (93–115). New York: Routledge.

Braman, S. (2004). Where has media policy gone? Defining the field in the twenty-first century. *Communication Law and Policy*, 9(2), 153–82.

Braman, S. (1995). Policy for the net and the Internet. *Annual Review of Information Science and Technology*, 30, 5–75.

Braman, S., & Lynch, S. (2003). Advantage ISP: Terms of service as media law. *New Media & Society*, 5(3), 422–48.

Braman, S., & Malaby, T. (eds.) (2006). *Command Lines: The Emergence of Governance in Global Cyberspace*, *First Monday*, special issue no. 7, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.phph/fm/issue/view/223.

Bruce, R. R., Cunard, J. P., & Director, M. D. (1986). *From Telecommunications to Information Services: A Global Spectrum of Definitions, Boundary Lines, and Structures*. London: Butterworths.

Chissick, M. (1997). *Internet Law: A Practical Guide for Business*. London: Financial Times Media and Telecoms.

Froomkin, M. (2000). Wrong turn in cyberspace: Using ICANN to route around the APA and the Constitution. *Duke Law Journal*, 50, 17–184.

Horwitz, R. (1989). *The Irony of Regulatory Reform*. New York: Oxford University Press.

Kwak, N. (1999). Revisiting the knowledge gap hypothesis. *Communication Research*, 26(4), 385–413.

Lemley, M., Merges, R., Samuelson, P., & Menell, P. (2006). *Software and Internet Law*. Gaithersburg, MD: Aspen Law & Business.

Maggs, P. B., Soma, J. T., & Sprowl, J. A. (2005). *Internet and Computer Law: Cases, Comments, Questions*, 2nd edn. St Paul, MN: Thomson West.

Mowery, D. C., & Simcoe, T. (2002). Is the Internet a US Invention? An Economic and Technological History of Computer Networking. *Research Policy*, 31(8–9), 1369–87.

Mueller, M. (1999). *Ruling the Root*. Cambridge, MA: MIT Press.

Pool, I. de Sola (1983). *Technologies of Freedom*. Cambridge, MA: Belknap Press.

Radin, M. J., Rothchild, J. A., & Silverman, G. M. (2006). *Internet Commerce: The Emerging Legal Framework*, 2nd edn. New York: Foundation Press.

Reed, C. (2000). *Internet Law: Text and Materials*. London: Butterworths.

Schön, D. A., & Rein, M. (1994). *Frame Reflection*. New York: Basic Books.

Vishwanath, K., & Finnegan, J. R. (1996). The knowledge gap hypothesis: 25 years later. *Communication Yearbook*, 19, 187–227.

Zittrain, J. L. (2005). *Jurisdiction*. St Paul, MN: Thomson West.