A Layered Approach to Internet Legal Analysis

Craig McTaggart*

The analysis of Internet legal and policy issues is aided by an understanding of the Internet's unique, layered architecture. This article proposes a conceptual model of the Internet that reflects its layered architecture. The model is offered to decision-makers, policy-makers, and legal analysts, not only as a roadmap or guide to understanding the Internet, but also as a tool for identifying Internet legal issues with the appropriate degree of granularity. Precise identification enables state and legal actors to assess the impact of policy choices in a comprehensive manner by allowing them to consider the implications of those policy choices for the Internet's various elements.

Following an introduction to the Internet's four conceptual layers along with its sublayers and elements, the author offers a typology of representative legal and policy issues for each layer. A number of issues are surveyed with regards to each sublayer. The specific examples of browse-wrap licenses, overlay software, e-mail service, and Internet protocol telephony are discussed in detail in order to illustrate the characteristic features and concerns of each layer of the Internet.

La compréhension de l'architecture unique de l'Internet favorise l'analyse de ses enjeux juridiques et politiques. Cet article propose un modèle conceptuel de l'Internet qui reflète son architecture sous forme de «couches superposées». Ce modèle s'offre aux décideurs politiques et analystes juridiques non seulement à titre de guide leur permettant de comprendre l'Internet, mais également à titre d'outil pour identifier de manière appropriée et précise les enjeux juridiques qui y sont reliés. Une telle identification permet aux acteurs juridiques et étatiques d'évaluer de manière complète et détaillée l'impact des choix de certaines politiques et de considérer les implications de ces choix pour les différents éléments de l'Internet.

Suite à une introduction aux quatre «couches conceptuelles» de l'Internet, de même qu'à ses «sous-couches» et autres éléments, l'auteur nous offre une typologie des enjeux juridiques et politiques associés à chacune de ces «couches» et «sous-couches». Les exemples des «*browse-wrap licenses*», des «*overlay software*», des services de courriels et de la téléphonie IP sont discutés en détails afin d'illustrer les principales caractéristiques et questions que soulève chacune de ces «couches».

* S.J.D. Candidate and Graduate Fellow, Centre for Innovation Law & Policy, Faculty of Law, University of Toronto. E-mail: craig.mctaggart@utoronto.ca.

To be cited as: (2003) 48 McGill L.J. 571
Mode de référence : (2003) 48 R.D. McGill 571

Introduction

The analysis of Internet legal and policy issues is aided by an understanding of the Internet's unique layered architecture. Instead of being viewed as a monolithic whole, the Internet can be thought of as being composed of four different conceptual layers; from the top down these are: the *content*, *application*, *operational*, and *physical* layers. While Internet content (e.g., World Wide Web pages) and transactions (e.g., e-commerce) are its most familiar aspects, there is much more to the Internet than meets the eye. Many different elements within each of its four layers must work together to make Internet content appear on users' computer screens. Briefly, these layers can be defined as follows:

Content Layer	The data available by means of the Internet and transactions enabled by the Internet.
Application Layer	The software applications that make Internet content available and that enable Internet transactions.
Operational Layer	The centralized resources and functions, standards and protocols, and Internet Service Provider (ISP) functions essential to Internet operations.
Physical Layer	The computer equipment and telecommunications networks over which the Internet operates.

Contrary to early popular perceptions, the Internet is not inherently uncontrollable. Rather, each constituent element is subject to varying patterns of control by a variety of different parties. Addressing these patterns of control through Internet legal and policy analysis necessitates a degree of technical precision. This article proposes a layered conceptual model of the Internet that can be used to place a vast range of Internet-related legal and policy issues into their appropriate contexts. Many such issues are canvassed and some are analyzed in detail in order to provide illustrations of this approach.

The purpose of this article is to help decision-makers, policy-makers, and legal analysts better comprehend the Internet, to ensure that they identify, with an appropriate degree of granularity, the precise issue before them and consider its possible links to, and implications for, other elements of the Internet. The layered model is put forward as a particular way of thinking about the Internet, not as a way of solving any particular problem. It is hoped that readers will find this conception useful in their own study of Internet legal and policy issues.

This article is premised on the idea that the Internet is important and will continue to increase in importance as a social phenomenon. In spite of the "dot-com" implosion of early 2000 that followed the Internet's meteoric rise to ubiquity in the late 1990s, Canadian Internet-use rates continue to climb.[1] The disappointment of e-commerce appears to have done nothing, for example, to dampen interest in e-mail, illustrating the importance of distinguishing one Internet application from another. As was the case with other revolutions in communications, such as the telephone and television, the aphorism that people tend to overestimate the short-term impact of new technologies and underestimate their long-term impact may be borne out by the Internet, or at least by Internet technology.[2] If that is the case, then the short-term impact of the Internet on our legal system may only be the beginning of much greater challenges.

Part I of this article provides an introduction to the Internet's four conceptual layers and many of their respective sublayers and elements. Part II offers a typology of representative legal and policy issues organized by the layer and sublayer to which each issue *primarily* (though not exclusively) relates. Issues associated with each sublayer are surveyed, and one example with respect to each layer is discussed in detail. I observe the considerations that typify each layer as well as explore their respective policy implications. In the conclusion I contemplate future applications of the layered approach to Internet legal analysis.

I. A Layered Conceptual Model of Internet Architecture

To appreciate the significance of the Internet's layered architecture, one must first understand how the Internet's architecture differs from that of previous public communications infrastructures.

A. Monolithic vs. Layered Network Architectures

In the classical North American telephone system of the monopoly era, the "phone company" controlled virtually all aspects of telecommunications within its territory. Starting at the bottom, their comprehensive responsibility included digging the trenches, stringing the cable, and connecting network facilities and subscribers. Subscribers could only use devices supplied, if not also manufactured, by the phone company. Phone numbers were assigned by the phone company and listed in the phone company's directory. For most of the history of the telephone, the user could only use it for one purpose—voice telephone calls. While it may seem trite, this

[1] Statistics Canada reports that "[m]ore than 5.8 million households, or 49% of all 12 million households, had at least one member that regularly used the Internet from home in 2001, up 1.1 million (+23%) from 2000. This was somewhat less than the gain of 1.4 million (+42%) from 1999 to 2000" (Statistics Canada, "Household Internet Use Survey: 2001" *The Daily* (25 July 2002), online: Statistics Canada <http://www.statcan.ca/Daily/English/020725/d020725a.htm>).

[2] This maxim is widely credited, without citation, to science fiction writer Arthur C. Clarke.

limitation, and the structural reasons for it, become significant when contrasted with the open, layered data networks of the Internet.

So long as one company was in complete control of all aspects of the telephone network, its use was narrowly defined. The network was very good at carrying voice telephony, whether down the street or around the world. Carriers made physical and operational layer connections with other carriers. Each carrier, however, also controlled that portion of the overall telephone system that was physically located within its territory. So extensive was this control that until 1968 in the United States, and 1982 in Canada, the telephone companies could prohibit the connection of equipment that they did not make or approve of to their networks (referred to as "foreign attachments").[3] In the monopoly era, public telecommunications networks could indeed be thought of in monolithic terms.

This situation was transformed, however, by the sea of change in telecommunications (and its regulation) that followed the replacement of monopoly principles with market principles in Canadian telecommunications policy.[4] With the competitive provision of "enhanced services" such as voice mail, data processing,[5] and long distance services,[6] enterprises unrelated to telephone companies were given greater access to the latter's facilities on regulated terms. In addition, developing alongside (and thanks to) these changes was the lessening of the telephone companies' control over what services could be provided by means of the system. This development was key in the rise of public data networking. Monolithic network control gave way to decentralized control of separate *elements* at separate *layers*.

Once almost anything could be connected to the telephone system, a remarkable era of innovation in telecommunications and information technologies began. The telephone companies continued to hold monopolies (whether de jure or de facto) over many elements of the telephone system such as the physical access infrastructure, but generally they could not restrict the applications using that infrastructure or the content passing over it. Facsimile machines, "speaking" in standardized analog tones, were an early manifestation of this freedom. Private data networks, employing standardized digital protocols, were another. Large enterprises began to interconnect

---

[3] See *Carterphone v. American Tel. & Tel. Co.*, 13 F.C.C. 2d 420 (U.S. Federal Communications Commission 1968); *Attachment of Subscriber-Provided Equipment* (23 November 1982), Telecom Decision CRTC 82-14. Canadian Radio-television and Telecommunications Commission (CRTC) documents from approximately 1996 onward are available online: CRTC <http://www.crtc.gc.ca/>.

[4] For a detailed account of this transition, see John S. Tyhurst, "Monopoly Lost?: The Legal and Regulatory Path to Canadian Telecommunications Competition, 1979-2002" (2001/2002) 33 Ottawa L. Rev. 385.

[5] *Enhanced Services* (12 July 1984), Telecom Decision CRTC 84-18, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/1984/DT84-18.htm>.

[6] *Competition in the Provision of Public Long Distance Voice Telephone Services and Related Resale and Sharing Issues* (12 June 1992), Telecom Decision CRTC 92-12, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/1992/DT92-12.htm>.

scattered computing facilities to exchange internal data traffic—an early step towards the user taking control of what public telecommunications networks could do.

The technical architecture of today's Internet was first developed in U.S. government-sponsored research networks during the 1970s and 1980s. These networks included the U.S. Advanced Research Projects Agency Network (ARPANET), under the aegis of the U.S. Department of Defense and the U.S. National Science Foundation Network (NSFNET). Access to these networks was initially restricted to the American defence establishment and the government-funded scientific community, respectively.[7] The rules governing the NSFNET were relaxed in the early 1990s so that public, commercial networks could interconnect with it.[8] This step was the beginning of the Internet's commercial era, in which anyone with an Internet connection could send e-mail or put up a Web site, among other empowering benefits.

The fundamental difference between data networks such as the Internet and the telephone networks that preceded it is the separation of control over the *use* of the network from control over the network *itself*. As will be explained in the next section, control over the physical, operational, and application layers (i.e., those layers below the content layer) is further separated within the Internet's infrastructure. Control over individual elements is sometimes even more dispersed. This fragmentation of control is what lies behind the idea that nobody controls the Internet—no one entity is in a position to control every element of every layer. To put it another way, "nobody can turn it off."[9]

B. Layers and Law

Much like the Internet's potential to "change the rules" of business, the extent to which it could exist outside real-world law was overhyped in the 1990s. The title of Canada's first law journal article on the subject, "Controlling the Uncontrollable: Regulating the Internet" by Dov Wisebrod,[10] expressed the popular notion at the time that the Internet either could not be controlled or would prove particularly resistant to regulation by the state.[11] After offering the view that "King Canute had as much

---

[7] The fascinating history of these early "internetworks" can be easily accessed in Katie Hafner & Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Simon & Schuster, 1996).

[8] See Neil Randall, *The Soul of the Internet: Net Gods, Netizens and the Wiring of the World* (London: International Thomson Computer Press, 1997) at 248-50.

[9] Brian Carpenter, ed., "Request for Comments (RFC) 1958—Architectural Principles of the Internet" (June 1996) at s. 2.4, online: Internet Engineering Task Force <http://www.ietf.org/rfc/rfc1958.txt>.

[10] Dov Wisebrod, "Controlling the Uncontrollable: Regulating the Internet" (1995) 4 Media and Communications Law Review 331.

[11] Perhaps the classic academic expression of this idea is found in David R. Johnson & David Post, "Law and Borders: The Rise of Law in Cyberspace" (1996) 48 Stan. L. Rev. 1367.

success commanding the tides to retreat as a national government will have regulating cyberspace,"[12] Wisebrod argued:

> The very essence of the Internet is anarchy, a diametrical opposite of authority. ... [T]he anarchy of the Internet is a powerful, cooperative, functional force that *cannot* be subjected to centralized control. Thus, while the existence of a normative basis for regulating the Internet would be an interesting subject for debate, the exercise has little practical application. Due to the nature of the Internet, including its history, culture, amorphousness, and universality, it is quite impossible to effectively regulate.[13]

While the Internet may appear anarchical in the context of Usenet,[14] which is the single, text-oriented application that formed the object of Wisebrod's analysis,[15] the physical and operational layers are far from anarchical—indeed, they cannot be if the Internet is to function. The centralized resources and functions must be stable and non-conflicting. Internet Service Providers (ISPs) must carefully control and coordinate the delivery of traffic. Eight years of experience since Wisebrod's ground-breaking article have shown that it is simply not possible to make blanket statements as to whether the Internet is, or can be, controlled and regulated. The answer to that question depends entirely on the specific aspect of the Internet at issue. More precisely, it depends on the specific element of the specific layer and sublayer at issue.

Wisebrod later qualifies the term "anarchy" to mean "co-operative anarchy".[16] That the Internet is a *co-operative* environment is an important insight.[17] One must add to this, however, Lawrence Lessig's insight that, far from being anarchic, the Internet can be regulated as much by the design of software code as by statute and indeed is already regulated in many such ways. In *Code and Other Laws of Cyberspace*[18] Lessig refutes the idea that the Internet has an "essence" or a fixed "nature". Rather, its shape and function are determined by those in control of its architecture:

---

[12] Wisebrod, *supra* note 10 at 332.

[13] *Ibid*. at 332-33.

[14] Usenet (short for USEr NETwork) is defined as follows: "A public access network on the Internet that provides user news and group e-mail. It is a giant, dispersed bulletin board that is maintained by volunteers who provide news and mail feeds to other nodes." Alan Freedman, *Computer Desktop Encyclopedia*, 9th ed. (New York: Osborne/McGraw-Hill, 2001), *s.v.* "Usenet".

[15] Wisebrod explicitly notes, "The remainder of this article assumes the Internet is comprised primarily of Usenet" (*supra* note 10 at 337).

[16] *Ibid*.

[17] While we are beginning to learn more about the nature of the relationships between ISPs and their customers, there has been very little research on the relationships *among* ISPs. So mysterious is this realm that it is often depicted in popular and even technical literature simply as a cloud. Given the Internet's social and economic importance, at least in North America, this obscurity cannot likely continue much longer.

[18] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) [Lessig, *Code*].

> As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones who set its nature. Their decisions, now made in the interstices of how the Net is coded, define what the Net is.
>
> How the code regulates, who the code writers are, and who controls the code writers—these are questions that any practice of justice must focus [on] in the age of cyberspace. The answers reveal how cyberspace is regulated.[19]

In *Future of Ideas*, Lessig develops this theory and argues that commercialization is radically changing the Internet, such that the "commons" it represents is being enclosed in many ways:

> [A]t just the time that the Internet is reminding us about the extraordinary value of freedom, the Internet is being changed to take that freedom away. Just as we are beginning to see the power that free resources produce, changes in the architecture of the Internet—both legal and technical—are sapping the Internet of this power. Fueled by a bias in favor of control, pushed by those whose financial interests favor control, our social and political institutions are ratifying changes to the Internet that will reestablish control and, in turn, reduce innovation on the Internet and in society generally.[20]

Lessig's purpose is much broader than mine. I offer no opinion here on whether control is good or bad, but merely aim to draw attention to the way the Internet's unprecedented architecture gives rise to varied issues of law and policy at each layer. This article will serve its purpose if it assists those dealing with such issues to better understand both the context and implications of their decisions.

With a few notable exceptions, early Internet legal literature focussed on one layer and either played down or completely ignored the rest.[21] Most legal writing and media coverage to date has been related to the content layer. There is, however, much more to the Internet than just its "top" layer. Content and transactions are the "finished product", but they could not exist without the lower layers, the infrastructure.

Canadian Tim Wu was the first scholar to argue for something of an architecture-influenced approach to Internet legal analysis. In a 1999 article, Wu writes:

> For most purposes, I think we ought to discard the old talk of the Internet as a whole, for the whole Internet is rarely an appropriate level on which to generalize. Instead, legal thinking can better focus on where the variation that is apparent to the user is actually found: the application layer above the

---

[19] *Ibid.* at 60.

[20] Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (New York: Random House, 2001) [Lessig, *Future of Ideas*] at 15.

[21] See *e.g.* I. Trotter Hardy, "The Proper Legal Regime for 'Cyberspace'" (1994) U. Pitt. L. Rev. 993; James Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors" (1997) 66 U. Cin. L. Rev. 177; Johnson & Post, *supra* note 11; Wisebrod, *supra* note 10 at 332-33.

> Internet's basic protocols. We need, I think, to focus on the user, not on the network, and that means legal analysis that begins with the application.[22]

Wu suggests that Internet legal analysis proceed on an application-by-application basis (e.g., the Web, e-mail, video streaming). He continues:

> What's the difference? This seemingly technical point matters because the Internet by its design allows—even encourages—great diversity above a few basic standards. The "end-to-end" design of the Internet delegates the power to code function to the point nearest to the user: the application. As a result, nearly everything that "counts" about the Internet from a legal standpoint is a function of the particular application at issue and *not* of the basic Internet protocols. Since applications actually drive Internet usage, they ought also drive legal analysis of the Internet, yielding nuanced rather than stereotyped results.[23]

While I endorse this argument to a point, note that it obscures at least two important aspects of the Internet. First, it omits entirely an account of the physical layer, on which all higher layers "ride". Second, Wu's argument fails to recognize the complexity of issues that arise at the operational layer. There is much more to what makes the Internet work than "a few basic standards". Wu's view either assumes that all the elements of the Internet below applications are uninteresting or uncontroversial or declares that applications, for the purposes of legal analysis, *are* the Internet. In the model proposed in this article, the application layer (further divided into client-side and server-side manifestations) is recognized as a distinct layer for the purposes of legal analysis; however, it is one of four layers and is not the only layer of import.

A second model was proposed by Professor Yochai Benkler, who employs a tripartite model comprising a "content layer", a "logical layer", and a "physical layer".[24] While his model goes further to affirm the significance of what I call the operational and physical layers, it nevertheless generalizes too much about the logical layer and neglects to identify the distinct sublayers within the logical layer, such as the centralized resources and functions and the ISP functions. I therefore prefer "operational layer" to "logical layer" as a broader term. Finally, I suggest that Benkler's top layer be subdivided into content and transaction sublayers in order to embrace both static content and interactive e-commerce transactions.

In *Future of Ideas*,[25] Lawrence Lessig adopts Benkler's three-layered model but refers to Benkler's logical layer as the "code" layer, to pick up on the title of his own

---

[22] Timothy Wu, "Application-Centered Internet Analysis" (1999) 85 Va. L. Rev. 1163 at 1164 [Wu, "Internet Analysis"].

[23] *Ibid*.

[24] Yochai Benkler, "From Customers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access" (2000) 52 Fed. Comm. L.J. 561 at 562.

[25] Lessig, *Future of Ideas*, *supra* note 20 at 23-25.

book, *Code and Other Laws of Cyberspace*.[26] By implying that code-layer software "makes the hardware run" on its own, Lessig's model continues the trend of obscuring the critical roles played by the Internet's centralized resources and functions and by its ISPs. Lessig's formulation of Internet layers also conflates the Internet's standards and protocols ("the protocols that define the Internet") with the applications that employ them ("the software upon which those protocols run").[27] In my view, these two types of code perform such different functions and relate to such distinct functional aspects of the Internet that they warrant division into separate layers. As illustrated above by reference to earlier public telecommunications network paradigms, it is the Internet's unique *user-definable* application layer that makes it special among communications networks. This feature is what Wu is referring to when he says that the technical design of the Internet "delegates the power to code function to the point nearest to the user: the application."[28] Code that is user-definable (e.g., application software) is therefore qualitatively different from code that is standardized (e.g., operational standards and protocols).

Another way to distinguish these two types of code is to think of application-layer code as edge code and operational-layer code as core code. It is an Internet industry convention to refer to those parts of the Internet that are closest to users as the network's "edge"[29] and to everything in between these edges as the "core". As such, edge code consists mainly of application software and is user-definable, while core code consists mainly of standards and protocols with which the user normally has almost no interaction. Examples of core code and edge code are provided below in the sections describing the operational and application layers respectively.

C. A Four-Layer Conceptual Model of Internet Architecture

Bearing in mind the way in which the present model is distinguished from previous models, the four conceptual layers of the Internet discussed in this article are, from bottom-up: the physical layer, the operational layer, the application layer, and the content layer.[30] Below is a graphical representation of these four layers, their

---

[26] Lessig, *Code*, *supra* note 18. "Code" is a computer industry term for software or the individual machine instructions of which it is composed.

[27] Lessig, *Future of Ideas*, *supra* note 20 at 23.

[28] Wu, "Internet Analysis", *supra* note 22. Note that "code" is used as both a noun and a verb in the computer industry.

[29] Though there are, of course, no "edges" to the Internet at all, only nodes in a vast mesh.

[30] I note that two unpublished papers have been presented at the annual Telecommunications Policy Research Conference in Washington, D.C. in recent years that apply somewhat similar four-layer models to U.S. cable and telecommunications regulation. See Kevin Werbach, "A Layered Model for Internet Policy" (Paper presented to the 28th Research Conference on Information, Communication, and Internet Policy, September 2000) [unpublished], online: University of Michigan <http://www.tprc.org/abstracts00/layeredpap.pdf>; Douglas C. Sicker, "Further Defining a Layered Model for Telecommunications Policy" (Paper presented to the 30th Research Conference on Information,

respective sublayers, and some examples of their constituent elements. It is important to bear in mind that this model is not intended to be comprehensive. Furthermore, this model is purely conceptual—Internet architecture does not conform exactly to these divisions in reality. The rationale for the model is further explained at the outset of Part II.

Communication, and Internet Policy, September 2002) [unpublished], online: University of Michigan <http://intel.si.umich.edu/tprc/papers/2002/95/LayeredTelecomPolicy.pdf>.

Four-Layer Conceptual Model of Internet Architecture

Layers	*Sublayers*	*Examples of Elements*
Content Layer	Content	Web pages Digital media, software files E-mail messages
	Transactions	E-commerce transactions Interactive transactions
Application Layer	*Client-side Applications*	IP telephony, instant messaging, and e-mail client software Web browser software Peer-to-peer file-sharing applications Multi-player video games
	Server-side Applications	IP telephony, instant messaging, and e-mail server software Web server software Multi-player video game servers
Operational Layer	Centralized Resources *and Functions*	Domain names IP addresses Root server system
	Standards and Protocols	TCP/IP, HTTP, SMTP, BGP*
	ISP Functions	Interconnection and routing Naming and addressing Mail and name server operation
Physical Layer	Equipment	Computers (terminals and servers) Routers
	Networks	Telephone, cable TV networks Wireless networks

* See the glossary at page 625, below, for the meanings of these acronyms.

1. Physical Layer

The physical layer can be defined as: (a) the computer equipment, and; (b) the telecommunications networks over which the Internet operates.

a. Equipment Sublayer

Internet equipment consists mainly of computers functioning as terminals, servers, or routers. Terminals are those computers used at the "edges" by users and today consist largely of Personal Computers (PCs). Servers are the core computers that host data and perform operational functions. Routers are computers as well but with a more specialized function: to deliver "packets", the basic unit of Internet traffic consisting of chopped up messages and data, to other routers.

In the case of terminals, servers, and routers, their physical manifestation is separate from their operational control as a result of their modular design. User terminals and provider servers run applications that are under the control of the user and provider, respectively. Router software is controlled by the ISPs that operate them. Most of these control functions can be performed remotely over the Internet, making physical control of the equipment less important than operational control. The consequences of this modular pattern of control are discussed in the layered typology set out in Part II.

b. Networks Sublayer

It is often forgotten that the Internet operates atop other telecommunications networks, including the Public Switched Telephone Network (known in the telecommunications world as the "PSTN"). Telephone and Internet traffic are often carried over the same physical wires and cables—they are simply encoded using different operational protocols. In the classical North American Internet access model of the 1990s, the humble copper loop PSTN line was the predominant type of "first mile" physical layer link connecting the user with the Internet. But the copper loop is just one type of physical link. Coaxial cable networks and wireless radio frequency networks can also carry data. Wireless local area networks[31] are increasingly being used to provide always-on wireless Internet connectivity. Even electric power transmission lines are capable of serving as the physical layer for communications networks.[32] Fibre optic cable has now replaced metallic wire in the long-haul portions

[31] Based on the Institute of Electrical and Electronics Engineers 802.11 networking standards.

[32] See Julia Scheeres, "Net Access: Socket to Me" *Wired News* (17 April 2001), online: Wired News <http://www.wired.com/news/technology/1,1282,43054,00.html>.

of most telecommunications networks, and there is a push in some quarters to extend the reach of high-capacity (and therefore high-speed) fibre closer to users.[33]

All of this said, it is worth briefly noting some elements below the physical layer (though implicit in it for present purposes), such as rights-of-way, trenches, and support structures (e.g., poles and conduits), which are simply assumed to exist in most discussions of networks, but for which the real-world constraints of space, climate, and distance should not be forgotten. Distance may be dead at the operational layer,[34] but it is still an important consideration at the physical layer.[35]

2. Operational Layer

The operational layer, made up of the Internet's centralized resources and functions, standards and protocols (or "core code"), and ISP functions, is the most obscure part of the Internet from the user's point of view, but it is the essential glue which binds all the other layers together. The physical, application, and content layers could exist separately without the operational layer, but they could not be *interconnected* without it. There are three major sublayers of operational-layer elements, and thus areas in which distinct legal and policy issues arise: (a) the Internet's centralized resources and functions; (b) the standards and protocols to which participating networks adhere; and (c) the operational functions performed by ISPs of all sizes.

a. Centralized Resources and Functions Sublayer

Domain names, and their numerical cognates, Internet Protocol (IP) addresses, are used by ISP facilities to "route" Internet traffic (in packet form) among interconnecting ISP networks from origin to destination, in response to user commands. A hierarchical system of servers, known as the Root Server System (RSS), makes available certain information that "binds" domain names to IP addresses. In this way, routers know where to send packets when the user has requested a Web page with a particular Uniform Resource Locator (URL) or sent an e-mail to a particular e-mail address. Each ISP assigns IP addresses to its Internet-connected equipment and manages the assignment of domain names to its customers' servers. The ISP shares this information with other ISPs in the complex

---

[33] See Canada's Advanced Internet Development Organization ("CANARIE"), "Gigabit Internet to the Home and Schools", online: CANARIE <http://www.canarie.ca/advnet/gitts.html>.

[34] Frances Cairncross, *The Death of Distance: How the Communications Revolution Will Change Our Lives* (Boston: Harvard Business School Press, 1997).

[35] As illustrated by several protracted right-of-way disputes between carriers and municipalities in recent years. See *e.g. Ledcor/Vancouver—Construction, Operation and Maintenance of Transmission Lines in Vancouver* (25 January 2001), Decision CRTC 2001-23, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/2001/DT2001-23.htm>.

interconnection and routing process that makes its customers' servers accessible across the Internet.[36]

The nature of digital network identifiers (i.e., domain names, numbers, and addresses) requires that they be globally unique in order to be "resolvable" or useful across the network that employs them. It is an unavoidable technical constraint that there can only be one of each domain name, number, or address on a network. This constraint means that there can only be one of each domain name on the global Internet. The resulting clash between trademarks (which can co-exist on Earth in spite of their similarity) and domain names (which cannot) has resulted in volumes of scholarly writing, court and arbitral decisions, and regulatory activity (mainly in the U.S.). The problem, in the minds of many, has yet to be resolved satisfactorily. I further discuss this problem, along with several other issues related to the centralized resources and functions, in the layered typology below.

This restrictiveness of network identifiers stands in stark contrast to the bountiful diversity of the content layer and renews debates over scarcity that many thought the Internet would render irrelevant. Andeen and King explain the reality as follows:

> Ultimately, the fundamental technical driver of addressing is that Top Level Domains of any addressing scheme must be under the authority of a single, superordinate power if the network is to be globally effective. There is no way to avoid this.[37]

The Internet Domain Name System (DNS) is a hierarchical system of names and databases, and as the quotation above suggests, *someone* has to hold ultimate authority over the top level of this hierarchy.[38] For most of the Internet's history, this power was held by the U.S. government but exercised by a small team of engineers at the University of Southern California under the leadership of computer scientist Jonathan Postel.[39] His role was institutionalized in 1998 with the Internet Corporation for Assigned Names and Numbers (ICANN).[40]

---

[36] More is said about the roles played by ISPs after an explanation of Internet standards and protocols in Part I.C.2.c, below.

[37] Ashley Andeen & John Leslie King, "Addressing and the Future of Communications Competition: Lessons from Telephony and the Internet" in Brian Kahin & James H. Keller, eds., *Coordinating the Internet* (Cambridge: Massachusetts Institute of Technology Press, 1997) 208 at 251.

[38] Despite a preponderance of expert technical opinion in favour of a single Internet DNS hierarchy (see *e.g.* Internet Architecture Board, "RFC 2826: IAB Technical Comment on the Unique DNS Root" (May 2000), online: Internet Engineering Task Force <http://www.ietf.org/rfc/rfc2826.txt>), there are some who believe that multiple hierarchies or "roots", can, and in some circumstances should, coexist. See Milton L. Mueller, "Competing DNS Roots: Creative Destruction or Just Plain Destruction?" (Paper presented to the 29th Research Conference on Information, Communication, and Internet Policy, 28 October 2001) [unpublished], online: Cornell University <http://arxiv.org/abs/cs.CY/0109021>.

[39] As a 25-year-old graduate student at the University of California at Los Angeles, Jon Postel volunteered to maintain the "authoritative" lists of many parameters in use on the ARPANET, which eventually came to include domain names. Postel held various roles (under the semi-official title of the

b. Standards and Protocols Sublayer

Transmission Control Protocol/Internet Protocol (TCP/IP—often abbreviated to simply "IP") is the language or protocol that all computers on the Internet speak. TCP/IP is the most important element of the Internet's core code, though it is not the only one. TCP/IP is an end-to-end protocol suite, meaning that any Internet-connected computer is capable of "speaking" directly with any other connected computer and by means of any one of a number of different protocols. By contrast, telephones exist in a "master/slave" relationship with the switch to which they are connected. Internet packets need to be "switched" too, but a dedicated circuit between sender and receiver is not required: the packets merely join the rivers of other packets traversing the multitude of interconnected networks that comprise the Internet. TCP/IP makes sure that, eventually, they all get to where they are supposed to go.[41]

The TCP/IP suite consists of three general protocols (TCP, IP, and User Datagram Protocol) in addition to many others with specific functions.[42] Each protocol provides a simple, standardized way to participate in the global Internet. The protocols are voluntary—that is, no one *requires* any Internet-connected network to use any particular protocol—but the price of non-compliance is isolation. In another stark contrast to the diverse content layer, standards and protocols require absolute conformity. The question of who sets these powerful standards and on what basis is one of the most important public policy questions relating to the Internet.

c. ISP Functions Sublayer

Simply having a physical link to a telephone or cable TV network is not enough to connect to the Internet. One needs to enter into a relationship with a specialized intermediary—commonly known as an Internet Service Provider (ISP). In the classical North American dial-up Internet access model, the user's modem dials a telephone number that an ISP has designated to receive incoming calls to its own modems. The devices "shake hands" and "speak" to each other in order to establish a two-way TCP/IP connection over which packets can pass. With broadband connections, slightly different hardware performs the same functions. ISPs also provide other services such as the operation of domain name resolution software and the hosting of e-mail, Web, and application servers. Some provide extra security

---

Internet Assigned Numbers Authority (IANA)) under U.S. government contracts until his untimely death on 16 October 1998. See V. Cerf, "Request for Comments (RFC) 2468: I Remember IANA" (17 October 1998), online: Internet Engineering Task Force <http://www.ietf.org/rfc/rfc2468.txt>.

[40] The ICANN Web site is found at <http://www.icann.org/>.

[41] A more detailed explanation of TCP/IP and its origins is found in Randall, *supra* note 8, c. 4, "Vint Knows Protocol: The Birth of TCP/IP". See also Freedman, *supra* note 14, *s.v.* "TCP/IP".

[42] Examples listed in the table at page 582, above, include routing protocols such as Border Gateway Protocol (BGP) and application-supporting protocols such as Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP).

services such as "spam filtering", a server-side measure intended to keep junk e-mail out of customers' inboxes.

3. Application Layer

The application layer consists of the software applications that make Internet content available and that enable Internet transactions. Such software allows users to "post", send, and receive information of all kinds via the Internet. These applications underlie the content layer and rely on the availability of the operational layer below. The malleability of edge code allows any two (or more) users to communicate over the Internet by means of any software application they wish, be it commercial or homemade. Instead of just taking part in telephone calls, as with the classical telephone network, users can define what the network does for them. As suggested above, this development is truly revolutionary in public communications networking.

Almost all Internet applications have "client-side" and "server-side" manifestations;[43] that is, it takes software on both a user terminal and a provider server to effect a two-way exchange of data.[44] Common examples of application layer software include Web browser and server software, multi-player video games, and client and server software for IP telephony, instant messaging, and e-mail. There are literally hundreds of other applications that support such Internet-based functions as software upgrades, video conferencing, and remote equipment monitoring.

4. Content Layer

The content layer is the layer the user sees: it is the reason he or she uses the Internet in the first place. It comprises the data available by means of, and transactions enabled by, the Internet.

a. Content Sublayer

Technically speaking, all Internet content exists in the form of computer data stored on servers until it is called up by a client-side application and arranged for display on a user's screen. The more common meaning of content, and the one used in this article, is simply the information that the user can access via the Internet. The range of such information is, of course, incomprehensibly vast. Internet content can be anything digitizable: any information that is convertible into digital form, or, as with most modern media, information that is created in digital form. The most

---

[43] "Client/server" is "[a]n architecture in which the user's PC (the client) is the requesting machine and the server is the supplying machine, both of which are connected via a Local Area Network (LAN) or Wide Area Network (WAN)." Freedman, *supra* note 14, *s.v.* "client/server".

[44] The fascinating exception is second-generation "server-less" peer-to-peer file-sharing applications, introduced in Part II.B, below.

common forms of content include Web sites, audiovisual media, software, and e-mail messages.

b. Transactions Sublayer

Internet transactions include electronic interactions of all kinds—whether commercial, non-commercial, human, or machine—over the Internet (e.g., gambling, buying and selling goods and services, submitting a job application). Internet transactions can be instantaneous or they can result, for example, in the delivery of a good, either in digitized form over the Internet or in physical form by some real-world means of delivery. Following a typological exposition of Internet issues, I will return to transaction issues and specifically to the example of "browse-wrap licences".

II. A Layered Typology of Internet Legal and Policy Issues

This section offers a typology of representative Internet legal and policy issues. The issues are organized according to the conceptual layers and sublayers to which they *primarily* (though not exclusively) relate. In order to create this typology, I survey a number of issues associated with each sublayer, and one example per layer is discussed in depth. Some of the considerations that typify each layer are noted. The descriptions and discussions of each layer and sublayer are intended to place well-known issues in context and to illuminate some of the many lesser-known issues that may require attention in the future.

There are three caveats. First, this typology is suggested as *one way* of conceptually organizing Internet legal and policy issues; it is certainly not the only way. One could also classify these issues by dominant legal regime (e.g., commercial law, intellectual property law), issue area (e.g., digital media, gambling, telecommunications), or even by jurisdiction. The classification of issues by layer, however, is intended to demonstrate the degree to which the architectural and legal circumstances of each layer can differ and to show how control of elements at one layer can have an impact on the elements at other layers.

Second, in an article of this length it is not feasible to attempt to identify every aspect of every issue. Indeed, each sublayer gives rise to such a wide range of issues that the relevant sections below can only refer to a few. This approach is not intended to downplay the importance of issues that are not mentioned. I have endeavoured to provide references to further material on those Internet-specific topics that are raised but that cannot be addressed in detail. In some cases, there have not been any legal or regulatory proceedings to date, a state of affairs that highlights potential public policy problems. The Internet will likely continue to give rise to interesting policy issues that we cannot yet imagine, precisely because we cannot know how people will use the Internet in the future. This model therefore may be useful as a way of placing such future questions in context, but does not claim to provide answers to them.

Third, the choice of which layer to advert to when considering a particular issue is not meant to imply that it does not engage other layers—quite the opposite. The examples discussed in the sections below illustrate the remarkable degree to which issues cut across layers: they can implicate many different layers and legal regimes in different ways. Indeed, while it may be possible to make generalizations about some legal regimes, for example, that copyright law is primarily relevant to the upper two layers (content and application), and telecommunications law relates to the bottom two layers (operational and physical), some regimes are so far-reaching that they have an impact on almost all of the layers.

Privacy issues, for example, are implicated at each sublayer: *content*—the text of e-mail messages; *transactions*—health information disclosed in an on-line pharmaceutical purchase; *client-side applications*—"cookies",[45] which track Web browsing patterns; *server-side applications*—Webmail[46] e-mail account information on provider servers; *centralized resources and functions*—one's identity as expressed in a domain name; *standards and protocols*—the presence or absence of privacy-enhancing features in Internet core code; *ISP functions*—customer information such as logon and logoff times; *equipment*—unique identifiers on computer hardware;[47] and *networks*—wireless network eavesdropping.

Jurisdiction is constantly relevant as an analytical consideration. The Internet's challenge to territorial sovereignty is well known,[48] but the examples below illustrate how jurisdictional patterns can vary not only across layers but even within sublayers. As Michael Geist has noted, "Lurking behind virtually every Internet law issue is the question of jurisdiction ... "[49] As such, jurisdiction is not examined on its own here[50] but is adverted to in the context of several issues below.

Beginning with the content layer and proceeding back down through the application, operational, and physical layers, I discuss four specific examples as follows: *content layer*—browse-wrap licences; *application layer*—overlay software;

---

[45] A "cookie" is "[d]ata created by a Web server that is stored on a user's computer. It provides a way for the Web site to keep track of a user's patterns and preferences and, with the cooperation of the Web browser, to store them on the user's own hard disk." Freedman, *supra* note 14, *s.v.* "cookie".

[46] "Webmail" refers to Web-based e-mail services such as canada.com and hotmail.com where the user's messages are stored on the Webmail provider's servers and not on the ISP's servers as with ordinary Internet e-mail.

[47] For example, all ethernet Network Interface Cards (NICs) (the most common means by which PCs are connected to networks) carry a unique serial number that prevents any two NICs from bearing the exact same network address.

[48] This topic is influentially explored in Johnson & Post, *supra* note 11.

[49] Michael A. Geist, "iCraveTV and the New Rules of Internet Broadcasting" (2000) 23 U. Ark. Little Rock L. Rev. 223 at 239 [Geist, "iCraveTV"].

[50] See Michael A. Geist, "Is There a There There?: Toward Greater Certainty for Internet Jurisdiction" (2001) 16 Berkeley Tech. L.J. 1345; Vaughan Black & Mike Deturbide, "*Braintech, Inc. v. Kostiuk*: Adjudicatory Jurisdiction for Internet Torts", Case Comment (2000) 33 Can. Bus. L.J. 427; Chris Gosnell, "Hate Speech on the Internet: A Question of Context" (1998) 23 Queen's L.J. 369.

operational layer—e-mail service; and *physical layer*—IP telephony. References are made primarily to Canadian materials where possible, and to those in the English-language common law tradition in particular.[51]

A. Content Layer

It is appropriate to begin with the content layer, since it is the aspect of the Internet that is the most familiar to users. The range of Internet content-related legal issues is limited only by the content that people are willing to put on the World Wide Web. As in other Internet policy areas,[52] the Canadian government led the world in initiating a comprehensive study of "legal issues of liability for content circulating on the Internet" in 1996.[53] The excellent discussion of content-related issues in that study has since been supplemented by a rich array of Canadian legal scholarship on, for example, hate speech,[54] child pornography,[55] freedom of expression,[56] defamation,[57] and broadcasting.[58]

---

[51] The most comprehensive general resources are: Michael A. Geist, *Internet Law in Canada*, 3d ed. (Concord, Ont.: Captus Press, 2002) (casebook) [Geist, *Internet Law in Canada*]; Barry B. Sookman, *Computer, Internet and Electronic Commerce Law*, looseleaf (Toronto: Carswell, 2002) [Sookman, *Electronic Commerce Law*]; and George S. Takach, *Computer Law* (Toronto: Irwin Law, 1998) [Takach, *Computer Law*].

[52] Such as clarifying the regulatory status of IP telephony (see Part II.D.3, below).

[53] Michel Racicot *et al.*, "The Cyberspace is not a 'No Law Land': A Study of the Issues of Liability for Content Circulating on the Internet" (Paper prepared for Industry Canada, February 1997) at 1, online: Industry Canada <http://strategis.ic.gc.ca/epic/internet/insmt-gst.nsf/vwGenerated InterE/h_sf03117e.html>.

[54] Francine Aumueller, "Hate Propaganda Law and Internet-Based Hate" (2001) 44 Crim. L.Q. 92; Gosnell, *supra* note 50. Note that the *Anti-terrorism Act* (S.C. 2001, c. 41, s. 88) amended the hate messages provision of the *Canadian Human Rights Act* (R.S.C. 1985, c. H-6) to specifically include Internet-based speech, a result that had already been achieved somewhat awkwardly under the old provision in *Citron v. Zündel* ((2002), 41 C.H.R.R. D/274 (CHRT)).

[55] Sanjeev Anand, "A Case for Upholding the Child Pornography Law" (1999) 25 C.R. (5th) 312; Tanya Scharbach, "Child Pornography in Cyberspace" (1996) 2 Appeal 58.

[56] Robert Dawkins, "Online Liberty: Freedom of Expression in the Information Age" (2001) 10 Dal. J. Leg. Stud. 102; Frank Iacobucci, "Recent Developments Concerning Freedom of Speech and Privacy in the Context of Global Communications Technology" (1999) 48 U.N.B.L.J. 189; Gordon Scott Campbell, "Emerging Issues of the Internet and Canadian Criminal Law" (1998) 3 Can. Crim. L. Rev. 101.

[57] Randy A. Pepper, "Internet Defamation: Canadian vs. American Perspectives" (2002) 25 Advocates' Q. 190; Jonathon T. Feasby, "Who Was That Masked Man?: Online Defamation, Freedom of Expression, and the Right to Speak Anonymously" (2002) 1:1 C.J.L.T., online: Dalhousie University Electronic Text Centre <http://cjit.dal.ca/>; Kim von Arx, "LitOral: A New Form of Defamation Consciousness" (2002) 1:2 C.J.L.T., online: Dalhousie University Electronic Text Centre <http://cjit.dal/ca/>; Jacquelyn Burkell & Ian R. Kerr, "Electronic Miscommunication and the Defamatory Sense" (2000) 15:1 C.J.L.S. 81; Black & Deturbide, *supra* note 50; George S. Takach, "Internet Law: Dynamics, Themes and Skill Sets" (1999) 32 Can. Bus. L.J. 1 at 19ff.; Craig Martin,

For the most part, the kinds of legal and policy issues that have arisen in the Internet content and transaction realm to date resemble old wine in new bottles. When social phenomena such as home taping of recorded music and gambling "went on-line", following a period of adjustment, the off-line regimes of copyright and criminal law generally caught up. Indeed, in the area of electronic signatures, it may be the marketplace that now lags behind the law, as e-commerce has failed to become as pervasive as many had predicted.

The incredible diversity of content and transactions on the Internet can be expected to produce diverse legal and policy responses. This diversity can be contrasted with the operational and physical layers, where uniformity and scarcity are the hallmarks. At these levels, public law regimes such as telecommunications regulation and the new Internet governance laws are more prominent. Most users are only familiar with the Internet's content layer. The layered approach suggested here is designed to highlight the aspects of the on-line network and its related legal and policy issues that lie "below the surface".

1. Content Sublayer

By far the most commercially significant legal regime at the content sublayer is copyright law, perhaps because the Internet may be the ultimate information distribution (read: copying) machine. While many fascinating copyright issues are presented at the content sublayer, my purposes are more circumscribed, so I refer interested readers to some of the many general works,[59] articles,[60] and policy proceedings[61] relating to copyright and Internet content in Canada.

"*Tolofson* and Flames in Cyberspace: The Changing Landscape of Multistate Defamation" (1997) 31 U.B.C.L. Rev. 127.

[58] Jonathan A. Blakey & Justine Whitehead, "Approaching a Regulatory Crossroad: Internet Retransmission Activities in Canada" (2002/2003) 3 Internet and E-Commerce Law in Canada 41; Howard P. Knopf, "Internet Copyright Reform Initiatives from Canadian Government" (2000/2001) 2 Internet and E-Commerce Law in Canada 33; Geist, "iCraveTV", *supra* note 49. See also Canadian Heritage (Copyright Policy Branch) & Industry Canada (Intellectual Property Policy Directorate), "Consultation Paper on the Application of the Copyright Act's Compulsory Retransmission Licence to the Internet" (22 June 2001), online: Industry Canada <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01103e.html>.

[59] Sunny Handa, *Copyright Law in Canada* (Markham, Ont.: Butterworths, 2002) [Handa, *Copyright Law in Canada*]; John S. McKeown, *Fox Canadian Law of Copyright and Industrial Designs*, 3d ed. (Scarborough, Ont.: Carswell, 2000); David Vaver, *Copyright Law* (Toronto: Irwin Law, 2000).

[60] See *e.g.* Jeremy F. deBeer, "Canadian Copyright Law in Cyberspace: An Examination of the Copyright Act in the Context of the Internet" (2000) 63 Sask. L. Rev. 503; Lisa Anne Katz Jones, "Is Viewing a Web Page Copyright Infringement?" (1998) 4 Appeal 60; C. Paul Spurgeon, "Digital Networks and Copyright. Licensing and Accounting for Use: The Role of Copyright Collectives—Evolution or Revolution? (1998) 12 I.P.J. 225; Barry B. Sookman, "Copyright and the Information Superhighway: Some Issues to Think About" (1997) 11 I.P.J. 123 & 265; Donald M. Cameron, Tom

2. Transactions Sublayer

While first-generation e-commerce did not differ significantly from "tele-sales" or even catalogue sales before that, the spectre of large volumes of consumer and commercial transactions moving to the Web has sparked a great deal of interest in the rules governing on-line transactions. As the Web has matured, more powerful transactional environments have been enabled, such as auction sites (e.g., ebay.ca), sophisticated retail storefronts (e.g., chapters.indigo.ca), and government "service windows" (e.g., the one that facilitates "e-filing" of income tax returns in Canada: netfile.gc.ca). A wide variety of transactions can now be executed over the Internet; that is, by means of a combination of client-side and server-side application software. These Web-based systems can inexpensively substitute for specialized, proprietary networks operated by Electronic Data Interchange (EDI) firms over dedicated telecommunications networks.[62]

Today, ordinary browser software and an Internet connection can be used in conjunction with specialized, but relatively inexpensive, server software to enable electronic transactions protected by highly secure encryption tools. Even the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the system used internationally by major financial institutions for instantaneous fund transfers, is moving towards an Internet model.[63] SWIFT, however, is a private organization, and the repeated interactions among its members are governed by sophisticated commercial contracts. This is a very different situation from one-off consumer contracting over the open Internet, which will be discussed below in the context of browse-wrap licences.

E-commerce law is that branch of consumer and commercial law relating to transactions enabled by the Internet and other electronic networks. E-commerce legal issues[64] might be grouped into three areas: (1) the requirements for electronic documents and on-line contracts,[65] (2) consumer protection,[66] and (3) the protection

---

S. Onyshko & W. David Castell, "IP on the I-Way" (1997) 13 C.I.P.R. 311; Mark B. Eisen, "Copyright and the World Wide Web" (1996) 12 C.I.P.R. 405.

[61] Industry Canada (Intellectual Property Policy Directorate) & Canadian Heritage (Copyright Policy Branch), "Consultation Paper on Digital Copyright Issues" (22 June 2001), online: Industry Canada <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01102e.html> [Industry Canada & Canadian Heritage, "Digital Copyright"]. See also Knopf, *supra* note 58.

[62] See Brian D. Grayton, "Canadian Legal Issues Arising from Electronic Data Interchange" (1993) 27 U.B.C. L. Rev. 257.

[63] Albeit via a secure virtual private network. See SWIFT, "SWIFT's Secure IP Network (SIPN)", online: SWIFT <http://www.swift.com/index.cfm?item_id=2304>.

[64] An introduction to the full range of issues and regimes engaged by e-commerce can be found in Barry B. Sookman, "Electronic Commerce, Internet and the Law: A Survey of the Legal Issues" (1999) 48 U.N.B.L.J. 119.

[65] John D. Gregory, "Canadian Electronic Commerce Legislation" (2002) 17 B.F.L.R. 277; Richard Weiland, "The *Uniform Electronic Commerce Act*: Removing Barriers to Expanding E-Commerce" (2001) 7 Appeal 6; John D. Gregory, "Receiving Electronic Messages: *Eastern Power v. Azienda Communale & Ambiente*" (2000) 15 B.F.L.R. 473; Mark J. Selick, "E-Contract Issues and

of individual privacy.[67] Certain types of on-line transactions are subject to existing regulatory regimes. These transactions include gambling,[68] sales of pharmaceutical products,[69] securities transactions,[70] and the use of electronic money.[71] The *Competition Act*[72] governs on-line advertising, promotions, contests, and arrangements among competitors, just as it does off-line.[73] The realm of taxation constitutes yet another major field of transaction-related issues that cannot be explored in depth here.[74]

Opportunities for the Commercial Lawyer" (2001) 16 B.F.L.R. 1; Ian R. Kerr, "Spirits in the Material World: Intelligent Agents as Intermediaries in Electronic Commerce" (1999) 22:2 Dal. L.J. 190; Amy-Lynne Williams, "Electronic Commerce: 'Cutting Edge' Changes and Challenges to Commercial Law and Practice" (1999) 48 U.N.B.L.J. 217; Michael Erdle, "Legal Issues in Electronic Commerce" (1996) 12 C.I.P.R. 251; Alfred A. Macchione, "Overview of the Law of Commercial Transactions and Information Exchanges in Cyberspace: Canadian Common Law and Civil Law Perspectives" (1996) 13 C.I.P.R. 129.

[66] Roger Tassé & Kathleen Lemieux, "Consumer Protection Rights in Canada in the Context of Electronic Commerce", online: Industry Canada <http://strategis.ic.gc.ca/SSG/ca01031e.html>; Roger Tassé & Maxime Faille, "Online Consumer Protection in Canada: The Problem of Regulatory Jurisdiction" (2000/2001) 2 Internet and E-Commerce Law in Canada 41; Bradley J. Freedman, "Canadian Provincial Internet Consumer Protection Laws" (2001/2002) 2 Internet and E-Commerce Law in Canada 6; John D. Gregory, "Solving Legal Issues in Electronic Commerce" (1999) 32 Can. Bus. L.J. 84; David Waite, "Consumer Protection Issues in Internet Commerce" (1999) 32 Can. Bus. L.J. 132.

[67] Christopher Berzins, "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building" (2002) 27 Queen's L.J. 609; Michael A. Geist, "When Dot-Coms Die: The E-commerce Challenge to Canada's Bankruptcy Law" (2002) 37 Can. Bus. L.J. 34; Piero Iannuzzi, "Protecting Transborder Data Flows: A Privacy Model for the 21st Century" (2001) 18 C.I.P.R. 337; John MacDonnell, "Exporting Trust: Does E-Commerce need a Canadian Privacy Seal of Approval?" (2001) 39 Alta. L. Rev. 346. See also the resources cited *infra* note 155.

[68] C. Ian Kyer & Danielle Hough, "Is Internet Gaming Legal in Canada: A Look at Star Net" (2002) 1:1 C.J.L.T., online: Dalhousie University Electronic Text Centre <http://cjit.dal.ca/>; Valerie Jepson, "Internet Gambling and the Canadian Conundrum" (2000) 6 Appeal 6.

[69] Andrea Faith Russell, "Internet Pharmacy: Options for Canadian Regulation" (2001) 21 Health L. Can. 90.

[70] Anita I. Anand, "Securities Law in the Internet Age: Is 'Regulating by Analogy' the Right Approach?" (2001) 27 Queen's L.J. 129; Stéphane Rousseau, "Internet-Based Securities Offerings by Small and Medium-Sized Enterprises: Attractions and Challenges" (2001) 35 Can. Bus. L.J. 226; Anita I. Anand, "A Comment on 'Internet-Based Securities Offerings by Small and Medium-Sized Enterprises: Attractions and Challenges'" (2001) 35 Can. Bus. L.J. 274; Gavin Sinclair, "Internet Direct Public Offerings: New Opportunities for Small Business Capital Finance" (2000) 27 Man. L.J. 297.

[71] Muharem Kianieff, "Show Me the Money!: A Critical Evaluation of Laissez-Faire Internet Currencies" (2002) 17 B.F.L.R. 215.

[72] R.S.C. 1985, c. C-34.

[73] Peter Franklyn & Kevin Ackhurst, "Competition Law Issues in the New Economy: The Emergence of B2B Marketplaces" (2000/2001) 2 Internet and E-Commerce Law in Canada 49.

[74] See Arthur J. Cockfield, "Canada's GST E-Commerce Policy (Or How to Catch the Big Fish)" (2002/2003) 3 Internet and E-Commerce Law in Canada 1; Jinyan Li, "Rethinking Canada's Source Rules in the Age of Electronic Commerce" (1999) 47 Can. Tax J. 1077 & 1411; Pierre J. Bourgeois &

3. Example: Browse-Wrap Licences

Can merely visiting a Web site place the user in a contractual relationship with the Web site publisher? Many of the latter (or at least their solicitors) seem to think so; they often post detailed licence "agreements" on their sites purporting to bind visitors to any number of terms of use. A hyperlink to the terms of these agreements is often provided at the bottom of Web pages, taking the user to a separate page where presumably few people other than lawyers or law students ever go. For example, on the first page of Bell Canada's Ontario region English language residential site, there are hyperlinks at the bottom labelled "Legal", "Privacy", and "Terms".[75] Clicking on the first hyperlink brings up a ten-section document in the form of a contract. The first section reads as follows:

> 1. *WEB SITE TERMS AND CONDITIONS*. The materials on BELL CANADA's Website (the "*Site*"), which may include text, images, audio clips, video clips, software and other materials (the "*Content*"), are provided by BELL CANADA for informational purposes only. By accessing the Site or downloading any Content, you agree to be bound by the terms and conditions set out below ("*Terms and Conditions*"). If you do not agree to these terms and conditions, do not access the Site or download any Content.[76]

The remainder of the terms and conditions are representative of this common type of Web-based document: disclaimers of liability relating to the site's content and use; a disclaimer of responsibility for, or endorsement of, non-Bell sites to which links are provided; restrictions on the use of the site; copyright and trademark notices; incorporation of the privacy policy; an indemnity in favour of Bell in case of the user's violation of the terms and conditions; notice that the site originates in Canada; reservation of the right to make changes to the site; and miscellaneous provisions, including the somewhat presumptuous assertion that "[t]he parties have required that these Terms and Conditions and all related documents be drawn up in English."

These documents generally have two purposes: to put users on notice that certain uses of a site and its contents are not permitted, and to attempt to shield the Web site publisher from liability relating to that use. The documents go by several common names, including terms of use, terms of service, disclaimers, Web-wrap licences, and browse-wrap licences. Recent judicial decisions in Ontario and the U.S. provide guidance on the enforceability of these browse-wrap licences.

The browse-wrap concept has its origin in the software industry's shrink-wrap licence. Except for custom software, commercial software is not sold, but licenced. Retail copies of commodity software products are licenced on standardized terms.

Luc Blanchette, "Income_taxes.ca.com: The Internet, Electronic Commerce, and Taxes—Some Reflections" (1997) 45 Can. Tax J. 1127 & 1378.

[75] Online: Bell Canada <http://www.bell.ca/>.

[76] Bell Canada, "Customer Care: Legal Notice", online: Bell Canada <http://www.bell.ca/>.

George Takach expresses the prevailing view on the enforceability of shrink-wrap licences:

> [S]ome software companies indicate on the outside of the box that a full licence agreement is contained within the box. This sort of notice given to the purchaser prior to or at the time of sale should be sufficient to legally bind the purchaser to the terms of the full licence inside the box. This is particularly true given that today these licences have become so standard and ubiquitous that the average user would be hard-pressed to argue that he did not know about them or the various terms contained within them.[77]

Shrink wrap licences are most likely enforceable in Canada, subject to the same caveat given by the court in the leading American case, *ProCD, Inc. v. Zeidenberg*: "Shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general (for example, if they violate a rule of positive law, or if they are unconscionable)."[78]

Today it is just as common for retail software to be delivered in digital form over the Internet, in which case there is no box or envelope sealed with a sticker that says: "Your use of this software is subject to a licence agreement." Instead, a dialog box is usually presented to the user during installation asking the user to click on an "I agree" icon to signify his or her acceptance of the applicable licence terms. This evolution became known as the "click-wrap" licence, and Justice Winkler of the Ontario Superior Court of Justice confirmed its enforceability in strong terms in *Rudder v. Microsoft*.[79]

Any doubts as to whether a mouse click can satisfy the technical requirements for contract formation have been removed by the enactment in most Canadian jurisdictions of statutes based on the Uniform Law Conference of Canada's *Uniform Electronic Commerce Act*.[80] Subsection 19(1) of the Ontario version, for example, provides (in part) that:

> An offer, the acceptance of an offer or any other matter that is material to the formation or operation of a contract may be expressed … (b) by an act that is intended to result in electronic communication, such as, (i) touching or clicking on an appropriate icon or other place on a computer screen …[81]

But what about browse-wrap licences, such as Bell Canada's, which states: "By accessing the Site or downloading any Content, you agree to be bound by the terms

---

[77] Takach, *Computer Law*, *supra* note 51 at 283.

[78] 86 F.3d 1447 at 1449 (7th Cir. 1996).

[79] (1999), 2 C.P.R. (4th) 474, 40 C.P.C. (4th) 394 (Ont. S.C.J.) [*Rudder*]. In this decision, Winkler J. ruled that a mandatory arbitration clause contained in a "Member Agreement" was binding on representative plaintiffs in a prospective class proceeding despite the fact that they had not read that portion of the agreement.

[80] (1999), s. 20(1)(b), online: Uniform Law Conference of Canada <http://www.chlc.ca/en/us/index.cfm?sec=1&sub=1u1>.

[81] *Electronic Commerce Act*, S.O. 2000, c. 17, s. 19(1).

and conditions set out below"? This kind of unilateral imposition of licence terms is probably not enforceable. A recent American appellate decision provides the most current statement of U.S. browse-wrap law. Sotomayor J. set out the facts and reasoning in *Specht v. Netscape Communications*[82] as follows:

> In order to resolve the central question of arbitrability presented here, we must address issues of contract formation in cyberspace. Principally, we are asked to determine whether plaintiffs-appellees ("plaintiffs"), by acting upon defendants' invitation to download free software made available on defendants' webpage, agreed to be bound by the software's license terms (which included the arbitration clause at issue), even though plaintiffs could not have learned of the existence of those terms unless, prior to executing the download, they had scrolled down the webpage to a screen located below the download button. We agree with the district court that a reasonably prudent Internet user in circumstances such as these would not have known or learned of the existence of the license terms before responding to defendants' invitation to download the free software, and that defendants therefore did not provide reasonable notice of the license terms. In consequence, plaintiffs' bare act of downloading the software did not unambiguously manifest assent to the arbitration provision contained in the license terms.[83]

While this lesson has surely been learned in the case of sites offering downloads of software subject to licences (which normally impose a requirement to click on an "I Agree" button or the like), the reasoning likely also applies to the browse-wrap situation, where one can use a Web site without having notice or unequivocally assenting to any governing terms. Barry Sookman's view, which is supported by the *Specht* decision, is:

> It is unlikely that a web-wrap agreement will be enforced under Canadian law unless the user takes an action that manifests assent to the terms of the agreement or unless the web site operator has made a reasonable attempt to bring the terms and conditions posted at the site to the attention of the user and the user has had a reasonable opportunity to read such terms.[84]

The Ontario Superior Court of Justice decision in *Kanitz v. Rogers Cable Inc.*[85] appears at first glance to run counter to this line of thinking, but on closer inspection there is a key distinguishing factor. At issue in the case was an arbitration clause dispute between an on-line service provider and unhappy customers seeking to begin a class proceeding (as in *Rudder*). Nordheimer J. upheld the validity of unilateral amendments to an Internet service agreement, amendments which the plaintiffs claimed they were not notified about and that removed their ability to seek redress in

---

[82] 306 F.3d 17 (2d Cir. 2002).

[83] *Ibid.* at 20.

[84] Sookman, *Electronic Commerce Law*, *supra* note 51 at 10-18.1 to 10-18.2.

[85] (2002), 58 O.R. (3d) 299, 21 B.L.R. (3d) 104 (S.C.J.) [*Kanitz*]. See also Bradley J. Freedman, "Website Notices of Contract Amendments: *Kanitz v. Rogers Cable Inc*." (2002/2003) 3 Internet and E-Commerce Law in Canada 17.

the courts. The service provider posted notice of the changes on its Web site but did not directly contact the plaintiffs to notify them.

The distinguishing factor in *Kanitz*, of course, is that there was an existing contractual relationship—the users had signed a paper contract before their service was installed. That contract allowed the service provider to amend the agreement from time to time, notice of which could be given by posting notice on the Rogers@Home Web site. The contract urged users to check the Web site periodically to obtain the latest version of the agreement. A notice indicating that amendments had been made (but not the nature of the amendments) was found to have been displayed on the service provider's "customer support site" for a reasonable period of time. While the *Kanitz* decision at least signals the Ontario courts' willingness to recognize and enforce Web-based contractual communication, it does not go so far as to make ordinary browse-wrap terms any more enforceable.

The click-wrap and browse-wrap cases suggest that if Web site publishers want to subject their visitors to any kind of licence agreement, that agreement must be brought to the visitors' attention. Furthermore, visitors must be provided with a way to signify their unequivocal assent before gaining access to the material to which the licence applies. This step would normally be taken when the user wants to interact with the site beyond mere browsing (e.g., by downloading content or querying a database).

B. Application Layer

The application layer is the realm of edge code, the limitlessly diverse set of programmes that define what the Internet does for its users. Edge code may be contrasted with core code, the rigidly uniform standards and protocols facilitating the exchange of information between and among applications. Edge code can be conceptually divided further into client-side and server-side applications. Generally, both a client-side and server-side application are necessary to complete an Internet communication (e.g., sending an e-mail or calling up a Web page). Nevertheless, each type of application plays a very different role, and their control is similarly separated. Client-side software is normally under the control of users, who can configure it according to their liking. Server-side software is under the control of service providers or Web site publishers. Peer-to-peer file-sharing applications present a challenging exception to this paradigm, as noted below, by essentially making every client a potential server.

Internet content and transactions have attracted the most attention to date, but it is useful to consider the role that the supporting applications play in some of these disputes. In this section, after brief note is made of encryption tools, patentability of e-commerce systems, and peer-to-peer file-sharing applications, the specific case of "overlay software" is examined in more detail. While these types of issues are

commonly analyzed as content matters, thinking about them at the application layer and in the light of the Internet's architecture can add a useful new perspective.

On the topic of client-side application software, the case of encryption is particularly illuminating. Given the inherent insecurity of communications across the open Internet[86] (as opposed to, for example, the closed EDI environments referred to above), users must take special measures if they want to protect the privacy and security of their information exchanges. Encryption technology (to oversimplify greatly) scrambles and selectively unscrambles data and allows as few as two users to access a particular communication (be it an e-mail message or a Web banking deposit). Encryption can therefore be thought of as an edge-based measure to foil attempts at intercepting communications in the core.[87]

Yet while encryption can empower users, it can also limit the use of Internet-based content by curtailing users' control over the applications running on their own terminals. For example, Adobe's Acrobat software facilitates the creation of "e-books",[88] electronic versions of books that can be viewed on a computer screen. While this technology can make books more accessible, copyright activists have charged that it can also attenuate citizens' rights of access to information by reducing or eliminating "fair dealing"[89] rights.

Such rights have historically been relatively easy to exercise (e.g., photocopying by students) without prior restraint or self-enforcing limitations. Lawyers for copyright holders might draft licensing terms that attempt to prohibit any non-revenue-generating use of a work, but fair dealing rights override such terms. Lessig contrasts the "over-reaching of lawyers" with self-enforcing rules like e-book settings:

> Now the over-reaching of an e-book that says, "You can read this on a Windows machine, but not on a Macintosh," is something more than bluster. It is a set of controls with the power of mathematics behind it—we call that encryption—and now these controls have the power of law to defend them—we call that the Digital Millennium Copyright Act.[90]

The American *Digital Millennium Copyright Act*[91] contains anti-circumvention provisions that make tinkering with such applications a criminal offence.[92] Industry

---

[86] Bruce W. Stratton, "Data Security and Privilege on the Internet" (1996) 12 C.I.P.R. 303.

[87] A topic to which we return in Part II.C.3 in the context of ISPs and lawful interception.

[88] See Adobe Systems Incorporated, "eBooks Central", online: Adobe <http://www.adobe.com/epaper/ebooks/main.html>.

[89] Or "fair use" in American legal parlance. See Handa, *Copyright Law in Canada*, *supra* note 59 at 285ff.

[90] Lawrence Lessig, "The Architecture of Innovation" (2002) 51 Duke L.J. 1783 at 1797.

[91] Pub. L. No. 105-304, 112 Stat. 2860 (1998) [*DMCA*].

[92] See Pamela Samuelson & Suzanne Scotchmer, "The Law and Economics of Reverse Engineering" (2002) 111 Yale L.J. 1575 at 1647. An interesting introduction to this important area, which engages core values of copyright and freedom of expression, is an article by Jonathan Zittrain,

Canada's 2001 public consultation on digital copyright issues included the subject of digital rights management systems,[93] leaving Canadian anti-copyright activists concerned that Canada might adopt its own *DMCA*-like regime.[94]

On the topic of server-side applications, another debate is raging over the extent to which e-commerce business processes (which are generally embodied in server software) can be patented.[95] Perhaps the most controversial server-side issue, however, is that of peer-to-peer media (primarily music) file-sharing. While rights management mechanisms may be attenuating user freedom at the application layer, peer-to-peer software has the potential to expand it—though this potential has not gone unnoticed by what the peer-to-peer community calls the "copyright industry". The enormously popular Napster system was successfully destroyed by the Recording Industry Association of America,[96] and even its decentralized progeny (such as Morpheus, KaZaA, and Gnutella),[97] which do not feature centralized servers[98] and whose operators are obvious targets for litigation, are now being pursued.[99] Nonetheless, client-side, peer-to-peer applications may represent the ultimate in user empowerment. These applications can give file-sharers access to all the free music they can download and turn each terminal into a mini-server.

Ironically, the compulsory tariff for the communication of musical works over the Internet, which Canadian copyright collective—the Society of Composers, Authors,

---

"What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication" (2000) 52 Stan. L. Rev. 1201.

[93] Industry Canada & Canadian Heritage, "Digital Copyright", *supra* note 61. In response to the consultation, the Minister of Industry tabled "Supporting Culture and Innovation: Report on the Provisions and Operation of the Copyright Act" (3 October 2002), online: Industry Canada <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/vwGeneratedInterE/h_rp01106e.html>.

[94] For instance, see the e-mail archives of the "Canada DMCA Opponents Forum", online: Digital Copyright Canada <http://www.digital-copyright.ca/discuss/>.

[95] Stephen J. Ferance, "Debunking Canada's Business Method Exclusion from Patentability" (2001) 17 C.I.P.R. 493; Richard Naiberg, "Patent Protection for E-Commerce Inventions" (2000/2001) Internet and E-Commerce Law in Canada 17.

[96] Napster and the much larger issue of copyright in music on the Internet are the topics of Alex Colangelo, "Copyright Infringement in the Internet Era: The Challenge of MP3s" (2002) 39 Alta. L. Rev. 891; W. Victor Tuomi, "Music, Copyrights, and the Internet: The Copyright Board Chimes In" (2001) 18 C.I.P.R. 69. See also Michael D. Mehta, Don Best & Nancy Poon, "Peer-to-Peer Sharing on the Internet: An Analysis of How Gnutella Networks are Used to Distribute Pornographic Material" (2002) 1:1 C.J.L.T., online: Dalhousie University Electronic Text Centre <http://cjit.dal.ca/>.

[97] Online: StreamCast Networks <http://www.morpheus.com/>; Sharman Networks <http://www.kazaa.com>; and OSMB <http://www.gnutella.com/>, respectively.

[98] For a detailed discussion of the many incarnations of peer-to-peer file-sharing applications and their legal status, see Tim Wu, "When Code Isn't Law" (2003) 89 Va. L. Rev. 679. Wu argues that each successive design was a conscious response to copyright enforcement strategies.

[99] See John Borland, "U.S. Liability Looms over Kazaa" *CNet News.com* (25 November 2002), online: CNet News.com <http://news.com.com/2102-1023-971086.html>; John Borland, "File Traders, Studios Spar in Court" *CNet News.com* (2 December 2002), online: CNet News.com <http://news.com.com/2102-1023-975801.html>.

and Music Publishers of Canada (SOCAN)—has been pursuing for several years before the Copyright Board, might be ineffective against peer-to-peer networks.[100] The proposed tariff's scope has been shaped by two important decisions, one of which was made by the Copyright Board and the other by the Federal Court of Appeal.[101] As it now stands, the tariff would apply to persons who post music files on a server thereby making them available over the Internet.[102] Even if individual members of peer-to-peer file-sharing communities were considered to have posted simply by allowing the file-sharing software to broadcast what is temporarily available on the user's hard drive for downloading by others, the transaction costs of negotiating licences with each individual would be prohibitive. The Supreme Court of Canada will soon decide on the legal status of the common ISP practice of "catching", whereby local copies of Internet content are stored on an ISP's server to speed delivery to customers who later request that particular content. The Federal Court of Appeal previously ruled that catching is not strictly necessary to ISPs' intermediary role, in which they benefit from an exception in the *Copyright Act* for entities that merely provide "the means of telecommunication necessary for another person to communicate the work."[103]

1. Example: Overlay Software

The volume of valuable content available for free on the Web continues to astound. What constitutes valuable content, of course, varies by user, but there is no denying the benefits of free access to newspapers, for example. While some news sites have always required paid subscriptions, and others require the user to endure a privacy-sacrificing "free" registration process, most continue to be available at no cost, as they have been since the "dot-com" boom days. These sites, however, tend to be advertising-supported and as pressure increases to make Web media properties profitable, advertising techniques have become ever more aggressive and annoying. In response, entrepreneurs offer programs with names like "Ad Blocker"[104] and "Junkbusters"[105] that allow savvy users to block banner and pop-up advertisements from appearing on their screen during browsing sessions.

In the grey area in the middle of this advertising arms race is a type of client-side application software known as overlay software. Overlay software, such as

---

[100] A view suggested by Tuomi, *supra* note 96 at 90-91.

[101] *Re SOCAN Statement of Royalties, Public Performance of Musical Works 1996, 1997, 1998 (Tariff 22, Internet)* (1999), 1 C.P.R. (4th) 417 (Copyright Board), reversed in part, [2002] 4 F.C. 3, 215 D.L.R. (4th) 118 (C.A.), leave to appeal and cross-appeal to S.C.C. granted, [2002] S.C.C.A. No. 289 (QL) [*Tariff 22*].

[102] Michael Koch, "Only in Canada, You Say? Perhaps Not: Federal Court of Appeal Rules on Internet Copyright" (2002/2003) 3 Internet and E-Commerce Law in Canada 25 at 27.

[103] R.S.C. 1985, c. C-42, s. 2.4(1)(b).

[104] Online: Ad Blocker <http://www.ad-blocker.com/>.

[105] Online: Junkbusters <http://www.junkbusters.com/>.

"Gator",[106] is marketed as "online companion software" and claims to enhance the browsing process by automating functions such as filling out forms and entering passwords. "Marketed" is perhaps not the right word: the software appears more often to be acquired unintentionally by downloading other free software programs, such as the peer-to-peer file-sharing program KaZaA. Bundled with the Gator "eWallet", however, comes another Gator program, called "OfferCompanion", touted as "your direct link to some of the Web's most valuable offers." OfferCompanion is, as the Gator Web site acknowledges, "ad-supported software". While the user browses the World Wide Web, the software communicates with Gator's servers and through the magic of "contextual advertising", pop-up advertisements appear on the user's screen that have been paid for by Gator's advertiser customers. The problem, in the view of the publishers of several of the Web's premiere commercial media Web sites, is that these advertisements often appear directly over top of advertisements that would otherwise appear on the visited Web site.

The Washington Post Company, the New York Times Company, Dow Jones, and other media companies brought an action against Gator[107] alleging trademark and copyright infringement, among other things.[108] The plaintiffs were granted an injunction restraining Gator from placing advertisements over their Web pages,[109] and an undisclosed settlement followed.[110] The Web publishers argued that Gator interfered with their Web pages, in which they have made significant investments, without their permission. Gator countered that the software does no such thing, that the plaintiffs' Web sites were not altered in any way. Rather, the sites just appeared differently on the screens of those users running the Gator software. Ottawa intellectual property lawyer Eric Smith has taken the publishers' position, arguing that they may have had good claims in copyright infringement, trademark infringement, and unfair competition under Canadian law.[111]

Regardless of whether the publishers would have succeeded in making out such claims, there is a larger issue at stake. This kind of dispute has implications for the extent to which Internet users can control the way Web content appears on their computer screens. The Gator software does not actually alter the content of Web pages. It does not achieve the same result as a "hacking", whereby the content of the

---

[106] Online: Gator <http://www.gator.com/>.

[107] *Washingtonpost.newsweek Interactive, LLC. v. Gator Corporation*, [2002] U.S. Dist. LEXIS 20881 (E.D. Va.).

[108] Stefanie Olsen, "Publishers Sue Gator over Pop-Ups" *CNet News.com* (27 June 2002), online: CNet News.com <http://news.com.com/2100-1023-940072.html>.

[109] Stefanie Olsen, "Judge: See Ya Later, Gator" *CNet News.com* (12 July 2002), online: CNet News.com <http://news.com.com/2100-1023-943515.html>.

[110] Stefanie Olsen, "Court says Gator-style Ads Are Legal" *CNet News.com* (1 July 2003), online: CNet News.com <http://news.com.com/2102-1024_3-1022791.html>.

[111] Eric J. Smith, "Contextual Advertising: The Case Against 'Theftware'" (2002/2003) 3 Internet and E-Commerce Law in Canada 33.

site *as it sits on the provider's server* is changed.[112] Only the way a particular page is displayed on a particular user's screen is altered. Other overlay software products offer functionality such as highlighting key words, links to reference sources (often paid advertisements), and annotations written by other surfers. In fact, Internet users can dramatically alter the appearance of every Web page they visit by simply changing their browser settings so as not to display graphics (thus excluding most advertisements). "Accessibility" features in Microsoft operating systems allow similarly extensive alterations, for instance, by displaying text in very large size for the benefit of the visually impaired. Users can further control their Web experience by blocking cookies and Java scripts (mini-programs which can be delivered and executed along with Web content) if they know how. The difference in the Gator case, of course, is that the software permits such modification on a mass scale, and the distributor profits from the modifications.

The legal right of consumers to avoid advertisements on free media is not a new issue; in fact, it is also playing out in the case of digital television recorders (such as ReplayTV and TiVo).[113] These devices allow viewers effectively to skip over the advertisements on television programs. Other devices can mute the sound or change the channel when advertisements are played.[114] The president of Turner Broadcasting caused a furor in mid-2002 when he suggested (in the words of one news article) that "people who watch television without commercials were stealing from entertainment producers—with possible exceptions made for folks who need to use the bathroom."[115] The same dividing line between consumer self-help measures to avoid advertising and for-profit attempts to divert "eyeballs" (or consumer attention) is being explored in both cases.

As the overlay software example suggests, the scope of rights relating to the application layer remains unclear, yet these rights are critical to the ability of users at the edge to control what the Internet does for them. While copyright issues relating to the protection of valuable material on-line dominate at the content sublayer, copyright's role at the application layer is to protect the applications used to access that content. In both realms, fair dealing rights claimed or historically enjoyed by

---

[112] Canada proved to be the home of the most notorious Web hacker to date, "mafiaboy", a Montreal teen who intermittently crippled the Web sites of Amazon, CNN, Dell, eBay, and Yahoo! from 7-15 February 2000 by means of a distributed denial of service attack in which Web servers were flooded with so many requests for data that they were effectively clogged. He was charged under subsections 342.1(1) (unauthorized use of computer) and 430(1.1) (mischief in relation to data) of the *Criminal Code* (R.S.C. 1985, c. C-46) and sentenced on 12 September 2001 to eight months detention plus one year probation (*R. c. M.C.*, [2001] J.Q. no. 4318 (C.Q. jeun.) (QL)).

[113] Online: Replay TV <http://www.replaytv.com/>; online: TiVo <http://www.tivo.com/>.

[114] See *e.g.* the "Ad Zapper", online: <http://www.adzapper.com/>.

[115] Michael Freedman, "Zapper War: TV Producers in Quest to Outlaw Device that Allows Consumers to Skip Ads" *ABCNews.com* (27 June 2002), online: ABCNews.com <http://abcnews.go.com/sections/business/DailyNews/forbes_zapper_020627.html>.

consumers are being challenged by the strong exclusionary claims of corporate copyright holders, which are in turn backed up by self-enforcing technical constraints.

Applications like overlay software and peer-to-peer file-sharing programs allow the user to override the control of content that the entertainment industry enjoys in traditional media by virtue of the existence of "gatekeepers" like advertising-supported broadcasters. In the absence of such central points of control, however, strategies such as the limitation of client-side applications (e.g., e-book viewers and browsers) are being pursued by those seeking to regain hegemony, often through compliant intermediaries like computer manufacturers. Unfortunately, few users are aware of these strategies.

The overlay software case also raises questions about the individual user's ability to control which applications run on his or her PC. Surreptitiously installed programs like Gator that produce commercial benefits for their sponsors (in this case, browsing data prized by advertisers) present privacy concerns. On the other hand, malicious applications like viruses and Trojan horses present all-too-common risks of property damage and data loss. What is the nature of the user's legal rights in this regard? Does the user implicitly cede some control over his or her machine by plugging it into the Internet? If so, are there general rules that mediate all Internet participants' vulnerabilities?

These questions are only now beginning to be posed, thanks to increasing awareness of the importance of the application layer to the overall Internet experience. The inherently international nature of the application layer (as opposed to, for example, the physical layer) will complicate the resolution of these issues. That said, if one jurisdiction can force the producers of a mass-market software application to give effect to a particular policy choice, such as limiting the strength of data encryption features, then that decision can have a global effect. This problem further illustrates the importance of user control over application software and of keeping applications conceptually separate in legal and policy analysis.

C. Operational Layer

There has been relatively less legislative and adjudicative activity to date directly relating to the operational layer, but the issues are no less important. Legal issues at the operational layer are often referred to as matters of "Internet governance", although the scope of this term is itself a matter of some debate. To those who see broad policy implications in the control of the essential centralized resources and functions, the term is almost akin to "Internet regulation". For others who seek to keep the operational realm free of politics (as if that were possible), these are matters of mere "technical coordination". The sources of legal and quasi-legal authority in this realm are unusual, and in most cases, institutions and rules are still very much in the formative stage.

In addition to the familiar domain name issue, several lesser-known operational layer topics are introduced below. These issues are examined in the context of three

sublayers: (1) centralized resources and functions; (2) standards and protocols; and (3) ISP functions. The example of e-mail service brings these three groups of elements together and illustrates the impact that they have on the way the Internet works as a whole.[116]

1. Centralized Resources and Functions Sublayer

The elements of the centralized resources and functions sublayer include network identifiers (i.e., names, numbers, and addresses), the DNS, and the RSS. During the early, non-public internetworking era when access was restricted to U.S. government agencies and contractors, and later scientists at universities, these resources and systems were effectively self-governed—which is to say that authority over them was informal and often wielded by trusted individuals known in the network community. As the Internet expanded, and particularly when commercial ISPs joined in, the potential scarcity of these resources slowly started to prompt questions about their governance.

The first and most prominent of such clashes was the still unresolved conflict between trademarks and domain names. The friction between trademark systems and the DNS has been extensively treated by legal scholarship around the world,[117] and in Canada.[118] Trademark systems can accommodate multiple simultaneous uses of similar brands and names worldwide, while the DNS does not, or at least has not been permitted to do so by the powerful global trademark lobby.[119] While domain names can be thought of as elements of the Internet's centralized resources and functions, domain names can implicate a much broader set of legal issues. As Teresa Scassa has noted, questions surrounding the right to use particular domain names (among other expressive on-line activities, like Web site design) "raise serious concerns about the

---

[116] See Part II.C.4, below.

[117] For some of the more insightful domain name/trademark articles, see Dan L. Burk, "Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks" (1995) 1 Richmond J.L. & Tech. 1; Robert Shaw, "Internet Domain Names: Whose Domain is This?" in Kahin & Keller, *supra* note 37, 107.

[118] Teresa Scassa, "Intellectual Property on the Cyber-Picket Line: A Comment on *British Columbia Automobile Assn. v. Office and Professional Employees' International Union, Local 378*", Case Comment (2002) 39 Alta. L. Rev. 934 [Scassa, "Cyber-Picket Line"]; Bradley J. Freedman & Robert J.C. Deane, "Trade-marks and the Internet: A Canadian Perspective" (2001) 34 U.B.C. L. Rev. 345; Chad Mitchell Bayne, "Domain Names: A Canadian Perspective" (2000) 17 C.I.P.R. 31; Lisa Katz Jones, "Trademark.com: Trademark Law in Cyberspace" (1999) 37 Alta. L. Rev. 991; Jonathan E. Moskin, "Canada and the Future of Internet Governance" (1999) 15 C.I.P.R. 247; Robert M. Frank, "Cybernames: Domain Name Issues and Conflicts in Cyberspace" (1996) 12 C.I.P.R. 245; Andrea F. Rush, "Internet Domain Name Protection: A Canadian Perspective" (1997) 11 I.P.J. 1.

[119] An argument made in Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge: Massachusetts Institute of Technology Press, 2002) at 231 [Mueller, *Ruling the Root*].

balance being struck between monopolistic intellectual property rights and the fundamental right of freedom of expression."[120]

The most significant new legal regimes created in the operational context to date are dispute resolution systems for the allocation of domain names. Most are modelled after the *Uniform Domain Name Dispute Resolution Policy* (UDRP) of ICANN.[121] These processes, depending on who you ask, either help the trademark industry prevent individuals and protest groups from using whatever characters they like in their domain names or help to rid the Internet of "cybersquatting": the opportunistic registration and auctioning of attractive names, particularly those implying an association with well-known corporations.

Domain name law is now a field unto itself,[122] but the process of formalizing Internet governance is deserving of further mention. In the mid-1990s, outsiders began examining the power over domain names that was held by individuals and certain institutions. The U.S. National Science Foundation initially had executive authority. Later, responsibility was assumed by the U.S. National Telecommunications and Information Administration, which administered operating contracts with some individuals with considerable influence in the area. The reform process that culminated in the creation of ICANN constituted an unprecedented process of codifying unwritten Internet law.[123]

Before ICANN, people and agencies often held decision-making power over key elements of the Internet's operational infrastructure only by historical accident. In other cases, government contracts that began as obscure procurements for a U.S. academic research network became the root of enormous power (and in some cases wealth) in the commercial era.[124] ICANN is intended to serve as the international, non-profit, non-governmental, industry self-regulating body for the Internet's key centralized resources and functions, including the DNS. While ICANN continually insists that it is only engaged in technical policy-making for a narrow set of coordinated Internet functions, others view it as the full-fledged regulator of the DNS

---

[120] Scassa, "Cyber-Picket Line", *supra* note 118 at 934.

[121] Online: ICANN <http://www.icann.org/udrp/udrp.htm>. See Bradley J. Freedman & Robert J.C. Deane, "The Uniform Domain Name Dispute Resolution Policy: A Practical Guide" (2002) 1:1 C.J.L.T., online: Dalhousie University Electronic Text Centre <http://cjit.dal.ca/>; W. Victor Tuomi, "Cybersquatters Not Welcome: A Review of Domain Name Dispute Resolution Procedures" (2001) 18 C.I.P.R. 103.

[122] A good source for current information is the online companion to Ellen Rony & Peter Rony, *The Domain Name Handbook: High Stakes and Strategies in Cyberspace* (Lawrence, Kan.: R&D Books, 1998), online: <http://www.domainhandbook.com/>.

[123] See A. Michael Froomkin, "Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution" (2000) 50 Duke L.J. 17.

[124] The best place to start an investigation into these fascinating arrangements is the U.S. government policy statement known as the "White Paper". See U.S. Department of Commerce, *Management of Internet Names and Addresses* (5 June 1998), online: U.S. Department of Commerce <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>.

and possibly other operational layer functions.[125] ICANN's major accomplishments to date include the promulgation of the UDRP and the admission of seven new, generic Top-Level Domains (gTLDs) to the existing ".com", ".net", and ".org": ".aero", ".biz", ".coop", ".info", ".museum", ".name", and ".pro". This was accomplished, however, only after an acrimonious two-and-a-half-year process.[126]

At the international level, the most sensitive Internet governance issue is the U.S. government's continuing role as the source of legal authority for the management of the top levels of the centralized resources and functions.[127] The European Union has been the most outspoken critic of the U.S. government's continuing involvement,[128] and even the latter's own 1998 policy paper recommended that it withdraw completely.[129] The proper role of governments in this sphere, and particularly that of the U.S. government, are major unresolved issues in international Internet policy.[130]

2. Standards and Protocols Sublayer

This layer consists mainly of the TCP/IP suite, the language spoken by all computers on the Internet. It has been suggested that while edge code is inherently diverse, core code, like the TCP/IP suite, is inherently uniform. This difference emphasizes the importance of understanding the different patterns of control over the two types of code. In many obscure, technical ways, the architecture of core code (and in particular the TCP/IP protocol suite) limits what is possible on the Internet. Counterbalancing the tremendous power of this kind of code is the historical fact that the TCP/IP suite is in the public domain; that is, the TCP/IP suite is typically not the property of any one vendor. Since adopting these standards and protocols is essentially compulsory in order to participate in the Internet, policy-makers must be aware of the institutions and politics of this obscure realm. Unfortunately, scholars are only in the early stages of exploring these matters, so the legal literature is quite thin.

---

[125] Milton Mueller, "ICANN and Internet Governance: Sorting Through the Debris of Self-Regulation" (1999) 1 Info 497; Jonathan Weinberg, "ICANN as Regulator" (Paper presented at the 29th Research Conference on Information, Communication, and Internet Policy, October 2001) [unpublished], online: Cornell University <http://www.arxiv.org/abs/cs.CY/0109099>.

[126] See Mueller, *Ruling the Root*, *supra* note 119 at 201ff.

[127] See Kim G. von Arx & Gregory R. Hagen, "Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control" (2002) 9 Rich. J.L. & Tech. 4.

[128] See "European Parliament Resolution on the Commission Communication to the Council and the European Parliament on 'The Organisation and Management of the Internet—International and European Policy Issues 1998-2000' (COM(2000) 202—C5-0263/2000—2000/2140(COS))" in EC, *Sitting of Thursday, 15 March 2001*, [2001] O.J. C. 44-343/198 at 286.

[129] U.S. Department of Commerce, *supra* note 124.

[130] This is the subject of Craig McTaggart, "The ENUM Protocol, Telecommunications Numbering, and Internet Governance" Cardozo J. Int'l. & Comp. L. [forthcoming in 2004].

The primary Internet standards development body is the Internet Engineering Task Force (IETF).[131] The IETF was founded in 1996 by a very small group of like-minded engineers who shared a common interest in developing interoperable TCP/IP networks. By the mid-1990s, meeting attendance began to exceed two thousand people, the vast majority of whom were representatives of Internet industry equipment vendors and software developers. The term "standards-setting" is not, however, an entirely accurate way to describe what the IETF does. The IETF is a forum in which operational and architectural ideas are proposed and experimented with. Ideas that meet with some measure of approval from interested members are put forward as standards that equipment vendors and networks are free to adopt or ignore: The IETF does not impose standards.[132] Philip Weiser describes the open standards bargain as follows:

> The Internet's openness created a virtuous cycle where members of the Internet community continued to improve upon its basic architecture by adding new functionalities that were placed in the public domain, thereby making the Internet a more valuable network. On the supply side, a culture emerged whereby developers would work with one another and rely on open standards rather than compete with one another to establish the basic architecture that supports the Internet. Because trusted standard-setting organizations adopted these key standards and made them open, developers did not have to worry about these standards being ignored and defeated, thereby undermining the value of any applications built off of those standards.[133]

It is essential that the Internet industry continue to see the value in open standards and interoperability. The alternative is to have multiple non-interoperable, non-interconnected systems, somewhat akin to the state of the computer industry before TCP/IP allowed communication between equipment of different types running different software. In the clever words of Sharon Eisner Gillett and Mitchell Kapor (co-founder of Lotus and the Electronic Frontier Foundation), "Interoperability is like Tinkerbell: it only works if everyone believes in it."[134] The same could be said for the Internet generally, where interoperability is based on open standards like those of the IETF.

---

[131] Online: IETF <http://www.ietf.org/>.

[132] See S. Bradner, "RFC 2026: The Internet Standards Process (Rev. 3)" (October 1996), online: IETF <http://www.ietf.org/rfc/rfc2026.txt>. Request For Comments ("RFCs") are the IETF's semi-official technical documentation series. There are several different types of RFCs, of which "Internet standard" is only one. For more on the IETF, see IETF Secretariat & G. Malkin, "RFC 1718: The Tao of the IETF: A Guide for New Attendees of the Internet Engineering Task Force" (November 1994), online: IETF <http://www.ietf.org/rfc/rfc1718.txt>.

[133] Philip J. Weiser, "Internet Governance, Standard Setting, and Self-Regulation" (2001) 28 N. Ky. L. Rev. 822 at 826-27.

[134] Sharon Eisner Gillett & Mitchell Kapor, "The Self-Governing Internet: Coordination By Design" in Kahin & Keller, *supra* note 37, 3 at 16.

While the members of the IETF can theoretically change the way the Internet works by "amending" its core code, change tends to happen rather slowly. New standards and protocols must be implemented by ISPs one by one. They cannot be imposed Internet-wide all at once. This point is illustrated by the time that it is taking to upgrade the TCP/IP suite from its current version, "IPv4", to a new version, "IPv6", that has been "stable" (an engineering term meaning "ready for implementation") since 1998.[135] This upgrade is considered crucial, both for avoiding a shortage of IP addresses and enabling new security and routing features.[136] Implementation has been very slow, however, since IPv4 appears to be serving the needs of the internetworking community well enough for now (at least in North America, where IP addresses are plentiful). The current slump in the Internet industry is making investment in new equipment that is IPv6-enabled even slower. The transition to IPv6 will not likely happen until enough large (i.e., American) ISPs hear their customers demanding it.

The Internet's remarkable decentralization, which empowers its "edges", can also be a weakness by preventing its constituent networks from taking Internet-wide collective action, even when the technical experts insist that such action is necessary. This decentralization may become more of a problem as expectations of the Internet continue to grow (e.g., that it be able to carry television-quality video). These problems will, in turn, likely have the effect of increasing the profile of the IETF and its processes.

3. ISP Functions Sublayer

Standards and protocols are only useful if they are adopted by ISPs, which perform the actual transmission of Internet traffic. ISPs come in all sizes, from local retail dial-up access providers, to large institutions like universities, to wholesale "backbone" carriers that aggregate traffic and that, at least notionally, connect everything to everything else. The sum of the myriad interconnections among ISPs can perhaps be said to be "the Internet".

ISPs and Internet applications have enjoyed something of a special status under Canadian law to date.[137] Of all the parties involved in making the Internet happen, ISPs would seem to be the easiest target for regulation by domestic authorities because they play a gatekeeper role and have operations, assets, and revenues within at least one court's jurisdiction. However, ISPs frequently argue that they have no

---

[135] See S. Deering & R. Hinden, "RFC 2460: Internet Protocol, Version 6 (IPv6)" (December 1998), online: IETF <http://www.ietf.org/rfc/rfc2460.txt>.

[136] To learn more, see the Web site of IPv6.org, a self-organized Internet technical community group which promotes the transition to IPv6, online: IPv6 <http://www.ipv6.org/>.

[137] See generally Andrew Bernstein & Rima Ramchandani, "Don't Shoot the Messenger!: A Discussion of ISP Liability" (2002) 1:2 C.J.L.T., online: Dalhousie University Electronic Text Centre <http://cjlt.dal.ca>.

knowledge of what customers use their Internet connections for, and thus should not be held liable for harm caused by those uses.

The ISP industry, led by the Canadian Association of Internet Providers (CAIP),[138] has been very successful in convincing decision-makers to treat ISPs as mere conduits for others' activities. Consider, for example, the exemption from copyright infringement liability recognized by the Copyright Board (and affirmed by the Federal Court of Appeal) in the *Tariff 22* proceedings.[139] The regulatory status of the ISP under the *Telecommunications Act*[140] and *Broadcasting Act*[141] was clarified somewhat by the CRTC in its feel-good *New Media* decision (taken at the height of "dot-com" mania), in which the commission acceded to public pressure to take a "hands-off" approach.[142]

The most potentially controversial aspect of the relationship between ISPs and their customers regards personal privacy. Ethan Katsh defines privacy as "being able to control information about oneself."[143] In the Internet environment, this includes one's on-line identity and habits. ISPs have the technical ability to monitor and record every move that their customers make on the Internet. Ian Kerr has suggested that ISPs may stand in a fiduciary relationship to their customers because ISPs are in a position to learn highly personal information about their clients and sometimes must decide in what circumstances and to whom this information should be revealed.[144] Referring to the specific case of an ISP aiding a securities-related investigation, Michael Geist has noted, "The ISP's ability to cooperate under circumstances mandated by legal necessity suggests that they may possess greater access to data than they might have the public believe."[145]

Indeed, this access is precisely why the federal department of justice is currently proposing measures to facilitate law enforcement interception and acquisition of e-mail messages stored on ISP servers.[146] An international movement in this direction

---

[138] Online: CAIP <http://www.caip.ca/>.

[139] S*upra* note 101.

[140] S.C. 1993, c. 38.

[141] R.S.C. 1985, c. B-9.

[142] *New Media* (17 May 1999), Telecom Public Notice CRTC 99-14 and Broadcasting Public Notice CRTC 1999-84, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Notices/1999/PB99-84.htm>. The results of the *New Media* proceeding are discussed in Part II.D.2, below.

[143] M. Ethan Katsh, *Law in a Digital World* (New York: Oxford University Press, 1995) at 228.

[144] Ian R. Kerr, "The Legal Relationship between Online Service Providers and Users" (2001) 35 Can. Bus. L.J. 419.

[145] Geist, *Internet Law in Canada*, *supra* note 51 at 89.

[146] See Department of Justice Canada, Industry Canada & Solicitor General Canada, "Lawful Access—Consultation Document" (25 August 2002) at "Interception of E-Mail", online: Department of Justice Canada <http://canada.justice.gc.ca/en/cons/la_al/>.

was underway prior to the events of 11 September 2001,[147] but this initiative is now a part of the broader federal strategy embodied in the *Anti-terrorism Act*.[148] One Canadian court has explicitly recognized that Internet e-mail ought to carry a reasonable expectation of privacy, raising the bar for justifying lawful interception.[149] Civil liberties and privacy advocates, however, remain concerned that these initiatives are increasing law enforcement power beyond what can be justified in a free and democratic society.[150]

While most Canadian ISPs are members of CAIP and endorse the CAIP Privacy Code,[151] this code is voluntary and each member is free to define how it subscribes to each principle. On the other hand, ISPs are subject to the *Personal Information Protection and Electronic Documents Act*[152] and the Privacy Commissioner of Canada has already investigated several complaints relating to ISP business practices.[153] Internet privacy,[154] of course, is just a small part of the much larger (and fast-growing) field of privacy law.[155] As noted at the beginning of this part, privacy is one of the issues pervading all of the layers in this typology. Space does not permit a complete examination of privacy issues in this paper. Nevertheless, a case from the Privacy Commissioner serves as the introduction to an in-depth examination of issues at the operational layer surrounding e-mail service.

---

[147] See especially Council of Europe, *Convention on Cybercrime*, 23 November 2001, Eur. T.S. 185, 41 I.L.M. 282, online: Council of Europe <http://conventions.coe.int/Treaty/eN/Treaties/Html/185.htm>.

[148] S.C. 2001, c. 41.

[149] *R. v. Weir* (1998), 213 A.R. 285, 59 Alta. L.R. (3d) 319 (Q.B.), aff'd (2001), 281 A.R. 333, 156 C.C.C. (3d) 188 (C.A.).

[150] See *e.g.* Lisa Austin, "Is Privacy a Casualty of the War on Terrorism?" in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001) 251.

[151] Canadian Association of Internet Providers, "CAIP Privacy Code", online: CAIP <http://www.caip.ca/issues/selfreg/privacy-code/privacy.htm> (as amended 7 November 2000).

[152] S.C. 2000, c. 5 [*PIPEDA*].

[153] See *e.g.* Privacy Commissioner of Canada, *Unsolicited E-Mail from an Internet Service Provider* (3 July 2001), online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/cf-dc_010703_e.asp> (the complaint was determined not to have been well-founded).

[154] See also James A. Fontana, *The Law of Search and Seizure in Canada*, 5th ed. (Markham, Ont.: Butterworths, 2002), c. 16, "Technical and Electronic Surveillance", c. 23, "Computer-Related Searches"; Robert W. Hubbard, Peter DeFreitas & Susan Magotiaux, "The Internet: Expectations of Privacy in a New Context" (2002) 45 Crim. L.Q. 170; John G. Boufford, "Privacy on the Information Highway" (1998) 47 U.N.B.L.J. 219.

[155] See *e.g.* Colin H.H. McNairn & Alexander K. Scott, *Privacy Law in Canada* (Markham, Ont.: Butterworths, 2001); Stephanie Perrin *et al*., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001); Teresa Scassa, "Text and Context: Making Sense of Canada's New Personal Information Protection Legislation" (2000/2001) 32 Ottawa L. Rev. 1; Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada*, looseleaf (Toronto: Carswell, 2000); Michael Power, "Bill C-6: Federal Legislation in the Age of the Internet" (1999) 26 Man. L.J. 235.

4. Example: E-Mail Service

One issue that seems bound to lead to litigation and perhaps even legislation in the future is that of e-mail service. Perhaps without even noticing, Canadians have come to depend on Internet e-mail as a major, or in some cases primary, means of communication. Even important documents like job applications are routinely sent by e-mail (and e-mail alone) today. Many universities allow graduating students to keep the addresses they had as students, recognizing the value of having a direct link to the hearts and minds of future donors. Use and misuse of "work e-mail" accounts has given rise to a host of problems of its own.[156] Now that many people view their e-mail address as an essential part of their identity, and their e-mail account as an essential means of communication, we are starting to see how high expectations for e-mail service can be.

E-mail is an application, and one of the Internet's most popular at that, but it is different in one key respect from other applications such as Web browsers. E-mail requires the services of an intermediary to send, receive, and store e-mails for users (i.e., to operate local mail servers). This intermediary is normally an ISP, and because of the necessity of their intervention, e-mail is best thought of as an operational layer issue.

A Privacy Commissioner case involving the withholding of e-mails illustrates both the degree to which some people are becoming dependent on e-mail, and how unclear its legal status remains. The commissioner's summary of the complaint sets the stage:

> An individual complained that her internet service provider (ISP), by continuing to take in and store her e-mails while her account was under suspension and by withholding them from her pending payment of arrears, had improperly used her personal information without her knowledge and consent for a purpose other than that for which it had been collected.[157]

After the second time the ISP suspended the subscriber's Internet service account, she contacted the ISP and made a reference to canceling her account, but does not appear to have unequivocally communicated that intention. The ISP continued to collect e-mail messages on her behalf, but would not give her access to messages until her arrears were paid. According to the commissioner's findings, she never paid those arrears, but subsequently became aware that messages to that account were not

---

[156] Kevin Coon & Jonathan Cocker, "Legal Issues of E-Mail and Internet Access in the Workplace" (2000/2001) 1 Internet and E-Commerce Law in Canada 81; Charles Morgan, "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44 McGill L.J. 849; Holly L. Rasky, "Can an Employer Search the Contents of Its Employees' E-Mail?" (1998) 20 Advocates' Q. 221.

[157] *Internet Service Provider Accused of Withholding E-Mails Sent to Suspended Account* (28 August 2002) Privacy Commissioner of Canada Finding 66 at para. 1, online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/cf-dc_020828_e.asp> (complaint well-founded) [*Withholding E-Mails*].

bouncing back to senders as undeliverable, and "with persistence" she was able to retrieve those messages.[158]

With respect to the subscriber's complaint that the ISP's actions contravened *PIPEDA*, the commissioner found that the governing service agreement did not give her any notice of how the service provider would handle her incoming e-mails during a suspension period and thus could not have formed a sufficient basis for her knowledge and consent regarding such practices. Finally, the commissioner concluded, "Nor could the ISP's continued absorption, storage, and withholding of e-mails pending payment of arrears be in any reasonable sense deemed uses consistent with the purpose for which the company ordinarily collected e-mails on behalf of its clients."[159] The ISP was found to have used the subscriber's personal information without her consent for purposes other than that for which it had been collected; thus, the ISP's actions contravened *PIPEDA*. However, the Privacy Commissioner recognized the validity of the contract between the subscriber and the ISP and noted that the ISP had since amended its standard agreement to give better notice of this practice, thereby complying with the legislation.

The commissioner, however, did not stop there and neither did the subscriber. The summary continues, under the heading "Further Considerations":

> The Commissioner remained concerned about the implications of storing and withholding potentially important messages without informing the intended recipient of their existence or the sender of their non-delivery. The practice falsely leads the sender to believe that the message has gone through unimpeded. The Commissioner recommended, in the interests of best practice, that the ISP immediately cease collecting, storing, and denying access to, e-mails addressed to holders of accounts under suspension and adopt instead the practice of deflecting such e-mails back to the senders with notification to the effect that the messages could not be delivered.[160]

This non-binding statement illustrates the commissioner's personal concern for the sanctity of e-mail, but it is difficult to see how this scenario would remain a privacy issue (and thus within his jurisdiction) if a service agreement that gives adequate notice of the practice does not contravene *PIPEDA*.

Perhaps emboldened by the commissioner's attempt to urge the development of a normative "duty to bounce", the subscriber soon after filed a well-publicized civil action in the Federal Court seeking compensatory damages in the amount of $80,000 and punitive damages of $30,000.[161] One of the "hostage" emails was allegedly a job

---

[158] *Ibid*. at para. 4.

[159] *Ibid*. at para. 11.

[160] *Ibid*. at para. 15.

[161] *Carter v. Inter.net Canada Limited* (11 October 2002), Toronto T-1745-02 (F.C.T.D.). See also Evan Hansen, "Who owns your E-mail?" *CNet News* (29 October 2002), online: CNet News <http://news.com.com/2102-1023-963631.html> (the first line of which reads, "Nancy Carter has a message for Internet service providers: Keep your hands off my e-mail").

offer, which the subscriber lost because the sender assumed she was not interested in the position since she did not reply, as was her custom, to that particular message. While section 16(c), the remedies section of *PIPEDA*, stipulates that the court may "award damages to the complainant, including damages for any humiliation that the complainant has suffered," whether this kind of economic loss will be found to have been a foreseeable consequence of the ISP's impugned actions (the use of the subscriber's personal information without her consent for purposes other than that for which it had been collected) remains to be seen.[162] If the subscriber can neither prove that she instructed the ISP in unequivocal terms to terminate her account nor point to conduct consistent with a belief that she had done so (e.g., sending out the customary change-of-address message), her chances of success seem slim.

The commissioner's decision demonstrates that so long as ISPs give adequate notice of, and so long as subscribers consent to, ISP business practices that may be considered privacy-invasive, *PIPEDA* does not prohibit such practices. Whether subscribers actually read their service agreements is another matter. If they did, they might be surprised at what they would find. What is the ISP's liability when an e-mail sent by a correspondent is never received at all instead of being withheld by the ISP (as almost everyone has experienced at least once)? The terms of service binding the largest single group of residential Internet access customers in Canada, those of the Sympatico network, are typical:

> You expressly understand and agree that: (a) the Sympatico network and the Services are provided on an "as is" and "as available" basis and … (b) Sympatico specifically makes no warranties that the Sympatico Network or any of the Services, including any content, information, products or services obtained from or through the use of the Sympatico Network or the Services, will be provided on an uninterrupted, timely, secure or error-free basis or that such services or the results derived therefrom will meet your requirements or expectations.[163]

Imagine a disclaimer applying to any other service as important (in many people's eyes) as Internet access which states that the service will only be provided "as available" and is not warranted to "meet your requirements or expectations." Surely customers are entitled at least to expect the delivery of e-mail messages. However, both courts[164] and the CRTC[165] have found the Internet access market to be

---

[162] The commissioner nevertheless found the impugned actions to be "standard industry practice" (*Withholding E-mails*, *supra* note 157 at para. 14).

[163] Sympatico Inc., "Sympatico Network Terms and Conditions" (last updated 1 April 2003), s. 19, online: Sympatico <http://www1.sympatico.ca/About_Us/terms.html>. In the interest of readability, I have converted this passage from upper-case to sentence-case letters.

[164] In *1267623 Ontario Inc. v. Nexx Online Inc.* (1999), 45 O.R. (3d) 40 at 50, 46 B.L.R. (2d) 317 (S.C.J.), which is currently the leading Canadian case dealing with "spam" and "netiquette", Wilson J. noted that a subscriber whose account has been terminated by an ISP could simply find a new one. Space does not permit me to consider the problem of spam (or "unsolicited commercial e-mail"), other than to note that as of July 2002, spam was thought to constitute over one-third of all e-mail traveling

competitive, and one presumes that the market will sort out which ISPs provide good service.

In the telephone industry, by contrast, companies providing basic service have to meet stringent quality standards.[166] It may only be a matter of time before consumers call for ISPs to be similarly regulated. Even before Rogers Communications bungled the transition of its high-speed Internet customer base from "@home.com" e-mail addresses to "@rogers.com" e-mail addresses in late 2001,[167] a group of disgruntled Toronto area customers attempted to bring a class action against Rogers for alleged cable Internet service interruptions.[168] For its part, the Residential Broadband Users Association (RBUA), a consumers group, stayed out of the dispute, preferring to maintain dialogue with Rogers in the hopes of improving service for all customers.[169]

While some service quality problems are doubtless the fault of one's ISP, the reality is that Internet performance depends on many different factors, including the service provided by the dozens of different ISPs that might be involved in routing any given e-mail from one side of the world to the other and the availability of key centralized resources and functions, such as the RSS. Even if Parliament or the CRTC wanted to regulate,[170] ISPs would protest that they simply cannot control the Internet at large and therefore cannot make any promises in respect of its performance. Viewed from this perspective, one might think it is a minor miracle that the Internet works at all, and perhaps it is. The availability of the content layer, and the operation of the application layer underneath it, both depend on the performance of the operational layer.

This is why the least-known realm of the Internet, the largely invisible operational layer, may present the most important legal and policy challenges for the future. Operational layer elements have either avoided regulatory attention, as in the case of the standards and protocols sublayer, or been the subject of experimental and "hands off" policies to date, as in the cases of the centralized resources and functions

---

over the Internet (Robert Lemos, "You've Got Spam, and More Spam" *CNet News* (29 August 2002), online: CNet News <http://news.com.com/2100-1001-955842.html>).

[165] *Regulation Under the Telecommunications Act of Certain Telecommunications Services Offered by "Broadcast Carriers"* (9 July 1998), Telecom Decision CRTC 98-9, s. 19, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/1998/DT98-9.htm> [*Broadcast Carriers*].

[166] *CRTC Creates New Quality of Service Indicators for Telephone Companies* (9 April 2001), Telecom Decision CRTC 2001-217, online: CRTC <http://www.crtc.gc.ca/archive/eng/Decisions/2001/DT2001-217.htm>.

[167] The transition was necessitated by the bankruptcy of U.S.-based Excite@Home, of which Rogers Communications was a shareholder. See Patrick Brethour, "Rogers E-Mail Clients Drag Feet on Switch Away from At Home" *The Globe and Mail* (30 November 2001) B1.

[168] This was the subject of the *Kanitz* case, *supra* note 85, in which Rogers was successful on a motion to have a proposed class action stayed on the grounds that the user agreement stipulated that any disputes arising under it were to be referred to, and determined by, arbitration alone.

[169] RBUA, News Release, "Statement on class action lawsuit brought against Rogers Cable" (23 July 2001), online: RBUA <http://www.rbua.org/policy/01-07-23-lawsuit.php>.

[170] On the question of the CRTC's jurisdiction over Internet services, see Part II.D.2, below.

and ISP functions. Since these elements serve as the glue that holds the rest of the Internet together, the current obscurity of their governance seems out of step with their significance to the Internet at large. The operational layer's components are essential to all uses of the Internet, yet we know the least about who controls these elements and what legal obligations apply or should apply to them.

Operational layer issues also highlight the jurisdictional puzzles that can beset Internet-related analysis. In the case of e-mail, for example, the jurisdiction in which the defendant is located would depend on whether the e-mail service provider is a local ISP or a Webmail provider. Webmail providers can theoretically be located anywhere in the world (the popular service hotmail.com, for example, is operated by Microsoft Corporation and its central servers are located in Washington State). The physical location of the server is also relevant to the question of whether SOCAN's proposed Internet music tariff would apply to a given communication of a work over the Internet. Physical location also plays a role in determining whether telephone calls over the Internet are subject to universal service subsidy charges, as explained in the next section.

The novelty of the problems found at the operational layer, combined with the layer's international scope, can be expected to continue stretching traditional legal regimes to the limit. The operational layer has already spawned *sui generis* regimes such as ICANN. Among areas to watch in the future, the international legal status of the IETF and other non-governmental stewards of standards and protocols will be particularly interesting. Furthermore, the ultimate control over the centralized resources and functions of the Internet wielded by the United States will likely be challenged more frequently by those in the international community seeking truly international governance of the Internet's shared infrastructure.

The Internet community faces significant collective challenges in maintaining and upgrading that shared infrastructure to meet ever-increasing user expectations. An optimal level of coordinated planning of the Internet's common infrastructure lies somewhere between the complete lack of centralized control of content and the strong centralized control of the DNS. The problems caused by the requirement that each domain name be globally unique may eventually be overshadowed by the exhaustion of the pool of IP addresses that IPv4 provides, unless IPv6 can be implemented in a timely manner. However, as explained in the standards and protocols sublayer discussion above, that implementation does not appear to be happening, at least in North America. If the advantages of IPv6 are lost, then so are the operational and associated regulatory advantages over traditional physical layer networks.

D. Physical Layer

The content, application, and operational layers all "ride" over the physical layer. Physical layer elements, like content layer elements, tend to be subject to legal regimes that predate the Internet. In other words, physical layer elements are governed in the same way now as they were before the Internet joined them into one interoperable, interconnected whole. In this section, some of these legal regimes and

their applicability to each of the equipment and networks sublayers will be identified. The specific example of IP telephony is used to illustrate the types of considerations relevant to legal analysis at the physical layer.

1. Equipment Sublayer

The Internet equipment industry can be thought of as a branch of the computer industry, which predates the Internet. The great achievement of TCP/IP, of course, is in linking different types of computers running different operating systems. Therefore, equipment can be designed independent of upper-layer considerations. Similarly, the computer law field continues to exist independent of Internet law, thanks in part to the modularity of Internet architecture. For this reason, the field of computer law, which is dominated by patent, copyright, and trade secret law, is not considered further in this paper.

2. Networks Sublayer

The regulation of public telecommunications networks also predates the Internet and continues independently of it. This independence, however, is being progressively undermined.[171] As the Internet and IP networks continue their apparent convergence into a single, unified platform for public and private communications, the physical layer will be influenced more and more by what is going on above it. That is, higher-layer issues will likely force changes in physical layer technology and policy, as is already the case in the broadband access realm.[172]

The incredible and largely unplanned success of the Internet has surprised everybody, including the communications industry and its commentators. Dreams of ubiquitous computing and communications abounded in the 1990s, but the visions tended to be of centrally controlled systems run by traditional telephone and cable companies. The buzzword was convergence, and the challenge was to determine how telephone and cable companies could be carefully allowed to enter each other's markets.[173] The theory was that both industries would convert to digital data networks that could carry voice as easily as video, rendering distinctions between the two arbitrary.[174] Then along came the Internet, at first operated by universities and

---

[171] The best general resource in this area is Sunny Handa *et al.*, *Communications Law in Canada*, looseleaf (Markham, Ont.: Butterworths, 2000).

[172] See *e.g.* the discussion of IP telephony regulation in Part II.D.3, below.

[173] The primary policy documents of the era were: CRTC, *Competition and Culture on Canada's Information Highway: Managing the Realities of Transition* (19 May 1995); Industry Canada, *Building the Information Society: Moving Canada into the 21st Century* (1996); Information Highway Advisory Council (IHAC), *Preparing Canada for a Digital World, Final Report of the Information Highway Advisory Council* (1997).

[174] See *e.g.* Sheridan E. Scott & David B. Elder, "Changing Communications Regulation in the Information Age" (2000) 14 Can. J. Admin. L. & Prac. 153; Sheridan Scott, "Regulation on the Information Highway: Capturing the Elusive Butterfly" (1995) 9 Can. J. Admin. L. & Prac. 305; Alan Ross & Jennifer Pawson, "Crossing Guards on the Electronic Highway: The Basis for Federal

institutions, but later joined by commercial ISPs. The Internet offered easy access to an unfathomably vast store of unadulterated and free information. While more expensive and sophisticated systems offering "video-on-demand" and satellite telephone service have come and gone, demand for the Internet continues to grow (though not at boom era levels).[175]

The CRTC has been dealing with the Internet in explicit terms (that is, using the term "Internet") since at least 1996, being among the first regulators in the world to do so. The CRTC now oversees an industry that has achieved the second highest broadband Internet penetration in the world, behind South Korea and ahead of Sweden.[176] The CRTC considers at least the Internet's content and physical layers to be very much within its jurisdiction, but has generally opted not to regulate. In its landmark *New Media* public notice of May 1999, the CRTC ruled that the *Broadcasting Act* applies to some content available over the Internet, but not to all content.[177] The CRTC interpreted its broadcasting jurisdiction widely but agreed to issue an exemption order,[178] leaving content consisting "only of audio, video, a combination of audio and video, or other visual images including still images that do not consist predominantly of alphanumeric text"[179] unconditionally (but not permanently) unlicenced. Content that consists predominantly of alphanumeric text (e.g., e-mail, most Web pages) remains outside the reach of the *Broadcasting Act*.

With respect to its *Telecommunications Act* jurisdiction, however, the CRTC has not shied away from taking action to encourage the development of the Canadian Internet service market. Initially, ISPs were thought of by the "bellheads" at the telephone companies as parasites on the PSTN, benefiting from its ubiquity but not contributing to it (in the form of universal service funding support). While this view was not strictly accurate (as explained below), ISPs enjoy a privileged place in Canada's telecommunications regulatory regime.[180] The restrictions traditionally placed on common carriers, such as non-discrimination among customers and traffic, made the PSTN a relatively "open" platform—one that could be used by unregulated

---

Jurisdiction Over Convergence Technology" (1994) 3 Dal. J. Leg. Studies 209; Hudson N. Janisch, "Optical Fibre to the Home: Keeping Our Policy Options Open" (1991) 3 Windsor Rev. Legal Soc. Issues 1.

[175] Statistics Canada, *supra* note 1.

[176] OECD, Directorate for Science, Technology and Industry, *The Development of Broadband Access in OECD Countries* DSTI/ICCP/TISP(2001)2/FINAL (Paris: OECD, 2001), Table 4 ("Broadband status (June 2001)"), online: OECD <http://www.oecd.org/dataoecd/48/33/2475737.pdf>.

[177] *Supra* note 142. See also Michael Koch, "CRTC Regulation of the Internet: Carriage Yes, Content No" in Osgoode Hall Law School, *Information Technology and Cyberspace Law* (Toronto: Emond Montgomery, 1999) c. 23.

[178] *Exemption Order for New Media Broadcasting Undertakings* (17 December 1999), Public Notice CRTC 1999-197, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Notices/1999/PB99-197.htm>.

[179] *Broadcasting Act*, *supra* note 141, s. 35.

[180] Due in part, no doubt, to political aversion to "killing the goose that laid the golden egg."

service providers largely as they pleased. Early commercial ISPs simply could order large numbers of business telephone lines, hook modems up to them, advertise a dial-in number, and they were in business. ISPs have directly benefited from these and other favourable regulatory policies. More recently they have been granted certain positive rights of access to the broadband Internet access facilities of both telephone companies and cable television companies.

The CRTC has attempted to take a very aggressive approach to "opening up" broadband network facilities to independent ISPs so that they can resell "high-speed" Internet services and compete with ISPs that are vertically integrated with the owners of the two dominant local access infrastructures in Canada (twisted copper pair and coaxial cable lines). With respect to cable TV companies, the CRTC ruled in July 1998 that it would not regulate the rates at which broadcast carriers (cable companies) offer retail level Internet services. It *would*, however, require companies to file tariffs setting out standard terms on which they would provide competitive providers of retail services with access to the cable companies' *telecommunications* facilities.[181]

With respect to Digital Subscriber Line (DSL) service, independent ISPs can also purchase, at discounted rates, those elements of telephone company high-speed Internet facilities that they need to provide competing DSL services. The state of competitiveness in the market for DSL services (and hence the need for CRTC intervention), however, has always been a topic of contention. For example, the independent members of CAIP[182] filed an application with the CRTC in August, 2001 alleging that they were unable to enter the residential market for high-speed DSL services in Ontario and Quebec due to anti-competitive conduct by Bell Canada and its affiliates. While the commission refused to restrict the Bell companies' pricing flexibility, it did impose "winback rules" to prevent them from trying to lure back former customers who have gone with a competitor for ninety days after the date of disconnection.[183] This type of restriction is typical in the local and long distance telephone service markets and illustrates the degree to which the CRTC is willing to apply traditional telecommunications regulatory tools and concepts to the Internet market.

---

[181] *Broadcast Carriers*, *supra* note 165; *Regulation Under the Telecommunications Act of Cable Carriers' Access Services*, (6 July 1999), Telecom Decision CRTC 99-8, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/1999/DT99-8.htm>; *Terms and Rates Approved for Large Cable Carriers' Higher Speed Access Service* (21 August 2000), Telecom Order CRTC 2000-789, online: CRTC <http://www.crtc.gc.ca/archive/eng/Orders/2000/O2000-789.htm>; *Terms and Rates Approved for Large Cable Carriers' Higher Speed Access Service* (31 January 2001), Telecom Order CRTC 2000-789-1, online: CRTC <http://www.crtc.gc.ca/archive/eng/Orders/2000/O2000-789-1.htm>.

[182] That is to say, those that are not affiliated with the telephone or cable companies.

[183] *Independent Members of the Canadian Association of Internet Providers—Digital Subscriber Line Internet Services by Bell Canada and Bell Nexxia* (27 June 2002), Telecom Decision CRTC 2002-37 at para. 63, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/2002/DT2002-37.htm>.

The most significant privilege that the Internet industry has enjoyed is its exemption from the contribution regime that supports universal access to basic telecommunications services. ISPs have always contributed implicitly by paying fees for underlying telecommunications services, including elements of subsidy funding. Retail Internet service itself is exempt. This is in stark contrast to the broad range of other telecommunications services for which these charges must be paid.[184] The place of one particular Internet application within this contribution regime is the subject of the fourth and final layer example.

3. Example: IP Telephony[185]

One of the most anticipated innovations touted by the "netheads" of the Internet industry in the 1990s was IP telephony. While it has not yet taken off to the extent expected (and certainly not in the way its narrowband cousin, e-mail, has), many in the telecommunications industry believe that it is only a matter of time before all telephone calls travel in IP form.[186] IP telephony is a software application that can be run on any packet-switched data network (including the Internet). It allows users to simulate real-time telephone calls using various combinations of computers and/or telephones.

There are generally two types of IP telephony: "Internet telephony", where the underlying, long-haul transmission network is the Internet; and "Voice-over-IP", where the underlying, long-haul transmission network is any kind of packet-switched network other than the public Internet (often a private corporate network). Like e-mail, IP telephony is also an application. Instead of being dependent on the intervention of a service provider, however, IP telephony in most cases utilizes the interface between the Internet and the telephone system. Thus, IP telephony is most usefully analyzed in the context of the physical layer.

IP telephony combines audio digitization and compression technologies with Internet technology. While traditional telephone systems relied on electrical impulses to reproduce speech, modern telecommunication is based on the digital encoding of sound into streams of bits. The bits travel over defined paths (or "circuits") from origin to destination. These paths are controlled by the interconnecting telephone companies that jointly carry a given telephone call. For this reason, traditional

---

[184] *Changes to the Contribution Regime* (30 November 2000), Decision CRTC 2000-745 at para. 91, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/2000/DT2000-745.htm>. Because revenues from *wholesale* Internet services are subject to the contribution charge, the amount of lost subsidy funds is not as significant as it might sound.

[185] This section is derived in part from Craig McTaggart, "IP Telephony and Canada's Telecommunications Regulatory Regime" (2001/2002) 2 Internet and E-Commerce Law in Canada 49 [McTaggart, "IP Telephony"].

[186] Tiffany Kary, "Net Telephony Poised to Take Off?" *CNet News* (31 May 2002), online: CNet News <http://news.com.com/2100-1033-930014.html>.

telephony is referred to as "circuit-switched", and interconnecting networks are collectively referred to as the PSTN.

"Packet-switched" data networks, such as those running IP, carry streams of digitized sound that have been chopped up into packets. The originating device (such as a computer) sends the pieces of a telephone call over one or more packet-switched data networks, and a computer on the other "end" reassembles them and plays back the sound. When the process is repeated in the opposite direction, a "live" two-way voice conversation (or fax communication) can be carried on. Successive generations of IP telephony technology allowed this process to take place, first between two computers (known as "PC-to-PC"), then between a computer and a telephone ("PC-to-Phone"), and finally between two telephones. To facilitate such "Phone-to-Phone" calls, computer servers, referred to as "gateways", are employed and convert calls from circuit-switched mode to packet-switched mode (and *vice versa*).

IP telephony provides a new way of transmitting phone and fax calls, a service which has traditionally been highly regulated in most countries.[187] In Canada, the primary regulatory issue presented by IP telephony has been its impact on the explicit subsidy regime that supports universal service. The system of internal cross-subsidies and implicit subsidies that prevailed during the monopoly era was gradually made explicit with the onset of competition in Canadian telecommunications markets. That system, known as the "contribution regime", has undergone several major changes in the past decade, the details of which are not essential for present purposes.[188] As a result of several key decisions,[189] Canada does not regulate IP telephony specifically—in fact, most forms can be described as unregulated. Gross revenues above a certain threshold, however,[190] from some forms of IP telephony, depending on how the calls interact with the PSTN, are subject to an annual contribution charge, currently set at 1.1 percent.[191]

Whether the contribution charge is levied depends on where a given call is converted from packet-switched to circuit-switched form. If that conversion takes place within Canada, such that an ordinary telephone located within Canada is used at

---

[187] For information on the international regulatory status of IP telephony, see "Regulatory Aspects of IP Telephony" in International Telecommunication Union, *ITU Internet Reports: IP Telephony* (Geneva: International Telecommunication Union, 2000) c. 4.

[188] See McTaggart, "IP Telephony", *supra* note 186.

[189] Telecom Order CRTC 97-590 (1 May 1997), online: CRTC <http://www.crtc.gc.ca/archive/eng/Orders/1997/O97-590.htm>; *In the Matter of Proposed New Contribution Exemption Regime for Internet Service Providers* (17 September 1998), Telecom Order CRTC 98-929, online: CRTC <http://www.crtc.gc.ca/archive/eng/Orders/1998/O98-929.htm>; *Changes to the Contribution Regime*, *supra* note 185.

[190] That is, where the service provider in question has ten million dollars or more of such revenues in the year. See *Changes to the Contribution Regime*, *ibid.* at paras. 97-100. This effectively leaves small IP telephony operators outside the contribution regime.

[191] *Final 2003 Revenue-Percent Charge and Related Matters* (19 December 2003), Decision CRTC 2003-84, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/2003/DT2003-84.htm>.

one or both ends of an IP telephony call, any associated revenues earned in Canada are subject to the contribution charge. Any person offering international long distance services to the public, whether by means of IP telephony or otherwise, is required to hold a licence and report their eligible contribution revenues.[192]

IP telephony has never been illegal in Canada, as it still is in many countries such as Botswana, Nepal, and Turkey.[193] It cannot be blocked by telephone companies, even if they would prefer that their customers not use IP telephony, lest it reduce circuit-switched long distance revenues. SaskTel's high-speed Internet terms of service contain the odd stipulation: "The Service is not intended to be used for long distance services."[194] The nature of "plain vanilla" Internet access, however, is that users can do whatever they like with that access simply by employing the applications of their choice: the Internet empowers its users. In its decisions regarding the regulatory status of IP telephony, the CRTC has walked a fine line between preserving this freedom and ensuring that long-standing policy goals such as universal service continue to be met. We can expect more of these kinds of policy challenges as the Internet becomes more and more ingrained in Canadian society. The degree to which those in control of elements at one layer can or should be allowed to influence elements at other layers will likely be a frequent point of contention.

While higher layers can operate largely independently of the physical layer, they are increasingly affected by physical layer regulation. The Internet began its popular life as an alternative to, or even enemy of, the traditional telephone networks. Yet gradually, and particularly when the speed of telephone lines became a barrier to Internet growth, this independence was eroded. Now that the largest ISPs in Canada (and most of the world) are also the largest telephone and cable TV companies, Internet service is just another service regulated by the CRTC. The market is still the primary guarantor of consumer interests in this area. As the importance of Internet service to Canadians continues to grow, however, calls for greater CRTC involvement may be expected, particularly as the distinctions between old and new forms of communication continue to disappear.

IP telephony regulation is an interesting example of this transition as it is a case of the physical layer regulator imposing terms on the operation of an application-layer business. The CRTC explicitly recognized that it is either impossible or very difficult to identify the contents of each packet to see whether it carries bits of a contribution-eligible service. Instead, the regulation of IP telephony is focussed on the operation of servers that convert traffic for passage back and forth between traditional circuit-

---

[192] *Regulatory Regime for the Provision of International Telecommunications Services* (1 October 1998), Telecom Decision CRTC 98-17, online: CRTC <http://www.crtc.gc.ca/archive/ENG/Decisions/1998/DT98-17.htm>; CRTC, Letter, "Industry Task Force on International Contribution Issues—Final Consensus Report" (17 December 1999).

[193] International Telecommunication Union, *supra* note 188 at 36.

[194] SaskTel, "SaskTel High Speed Internet Terms of Service", online: SaskTel <http://www.sasktel.net/policies/high_speed_internet_serv.pdf>, s. 15 (effective date: 24 August 2001).

switched networks and Internet-style packet-switched networks. One can speculate that future Internet-related issues that resemble telecommunications issues, such as the operation of instant messaging networks, might also lead the CRTC to project its physical layer jurisdiction onto application layer matters. On a related note, the layer at which an element notionally resides can also significantly alter the question of legislative jurisdiction. The United States' ultimate control over the Internet's centralized resources and functions (which Canada has recently shifted from recognizing to protesting mildly) can be contrasted with the control over physical networks that national regulators like the CRTC continue to hold.

The case of independent ISP access to telephone and cable company broadband facilities, on the other hand, suggests that a "hands off" policy, while popular with respect to higher layers, may do more harm than good at lower layers. It is widely believed that a cable and DSL duopoly would result from the removal of the independent access rules, since incumbent network owners would have no incentive to help independent ISPs compete. Worse, with a stranglehold on most users' access to the Internet (at least through "fat pipes"), the physical network operators would be in a position to manipulate those elements of the operational layer that they also control. The need for competition among cable and broadband service providers illustrates how arguments and policy values relevant to one layer may be harmful if applied indiscriminately to other layers.

Lawful access to ISP facilities is an example of another phenomenon: that of addressing legal issues indirectly at other layers. Law enforcement agencies are seeking to interpose a measure of control at the ISP functions sublayer and at the physical layer to counteract the freedom from regulation provided by the application layer. Given the right degree of access to the underlying data streams, the contents of one's Internet sessions can be captured and studied. Users, however, may respond (if they are aware of such scrutiny) by employing encryption tools at the application layer. The only sure way to guarantee the security of one's computer, both against spying from the outside in the case of lawful access and from the inside in the case of surreptitious applications, is to unplug it from the Internet. This is an option whose appeal and even feasibility seems to be continually diminishing.

Conclusion

The reality of constant connection to the Internet will continue to bring to the fore both familiar and novel legal and policy issues in the Internet context. The layered conceptual model put forward in this article is intended to provide a useful way of thinking about the Internet in that context. The article is premised on the idea that when confronting such issues, decision-makers, policy-makers, and legal analysts should identify the precise issue before them and consider its possible links to, and implications for, other elements of the Internet. A view of the Internet that includes the content, application, operational, and physical layers (and their respective sublayers) supports a much more comprehensive understanding of Internet legal and policy issues.

There are at least three ways in which this four-layer approach to Internet legal and policy analysis may prove useful in future work. First, identifying the specific elements of Internet architecture implicated in any given issue may provide insights into preliminary analytical considerations such as identifying parties, applicable legal regimes, and relevant jurisdictions. Second, since the architectural and legal circumstances of the layers can differ markedly, one must be careful not to let the characteristics or prevailing wisdom regarding one layer unduly influence one's analysis of elements at other layers. Third, since control of elements at one layer can have consequences for elements at other layers, it is important to understand these elements on their own terms, and in particular, to identify who controls them.

A layered approach to the Internet can help in the preliminary identification of parties, applicable legal regimes, and relevant jurisdictions by drawing attention to the many different elements of Internet architecture that may be implicated by any given issue. For example, the most common Internet application, e-mail, requires software applications on users' computers to work in conjunction with software on their ISPs' servers, in the case of hosted e-mail accounts, or with those of a Web-based service provider, in the case of Webmail. These servers can theoretically be located anywhere "on" the Internet. In turn, both forms of e-mail service depend on the availability of key centralized resources and functions such as the DNS and the RSS. Assigning blame for service problems is complicated by the fact that so many different actors are involved, the legal rights and obligations of whom generally remain vague in this relatively new domain.

This article has sought to broaden the reader's appreciation for the number of different elements of Internet architecture (and therefore independent actors) that must function together to make the Internet work. In many regards, we are still in the early stages of sorting out the legal status of, and relationships among, these elements and those who operate them. Fundamental questions of what legal regimes apply or should apply remain to be explored. Ironically, though perhaps not surprisingly, national jurisdiction over physical layer matters is being seized upon as a means of indirectly addressing higher-layer issues, such as IP telephony. This interplay between layers and legal regimes highlights the degree to which the architectural and legal circumstances of the layers can differ, making it important to keep the characteristics and considerations relating to the various layers and sublayers separate during analysis.

In particular, it is important to bear in mind the contrast between the bountiful diversity of content and transactions at the top layer, on one hand, and the technical and economic constraints typical of the operational and physical layers, where uniformity or scarcity are more often the dominant features. While the Internet can theoretically support an unlimited number of Web sites about books, for example, it is generally thought to be capable of supporting only one of each domain name. Similarly, the number of different applications that users can employ on the Internet is limited only by their creative ability. Yet the number of options that the average user

has for connecting to the Internet is usually limited, particularly outside of urban areas. Diversity and choice characterize the Internet's upper layers, but not its lower layers.

A particularly interesting avenue for future research would be a consideration of the implications of control of elements at one layer for elements at other layers. For example, the roles of the providers of operational layer infrastructure, such as the centralized resources and functions and ISP networks, need exploration. The effects of the extension of power over the physical layer into the application and content realms are potentially troubling. On the theory that "who pays the piper calls the tune," end-user control over the application layer, for example, should be jealously guarded against the encroachment of television-style systems where all programming choices are in the hands of one-way broadcasters. Of course, some consumers can be expected to demand simpler versions of the Internet, such as America Online, being content to give up some degree of edge-based control in favour of centralized programming. As suggested by the discussion of overlay software, the demands of advertisers sometimes clash with the interests of individual users. This conflict has a long history in other media, and is often characterized by surreptitious invasions of unwitting users' privacy. Control of Internet elements is an important issue, given the number of different elements involved and the highly dispersed nature of that control.

The extremely wide range of legal and policy issues canvassed in this article—themselves only a fraction of existing Internet-related problems—illustrates the tremendous breadth of the field. This breadth is all the more remarkable given that the Internet entered the public consciousness less than ten years ago. Whether Internet law exists as a separate field of law or merely brings together related issues from many existing fields, continues to be a subject of debate.[195] Without taking a position on that question, which perhaps only time can answer, this article argues that a catholic approach to Internet legal and policy analysis should be preferred over a blinkered one, given the impact of the Internet's layered architecture on the analysis of any given issue.

[195] See Frank H. Easterbrook, "Cyberspace and the Law of the Horse" [1996] U. Chi. Legal F. 207; Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harv. L. Rev. 501.

ARPANET	Advanced Research Projects Agency Network
BGP	Border Gateway Protocol
CAIP	Canadian Association of Internet Providers
CRTC	Canadian Radio-television and Telecommunications Commission
DNS	Domain Name System
DSL	Digital Subscriber Line
EDI	Electronic Data Interchange
gTLD	generic Top-Level Domain
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IHAC	Information Highway Advisory Council
IP	Internet Protocol
ISP	Internet Service Provider
NIC	Network Interface Card
NSFNET	National Science Foundation Network
PC	Personal Computer
PSTN	Public Switched Telephone Network
RBUA	Residential Broadband Users Association
RSS	Root Server System
SMTP	Simple Mail Transfer Protocol
SOCAN	Society of Composers, Authors, and Music Pulishers of Canada
SWIFT	Society for Interbank Financial Telecommunication
TCP/IP	Transmission Control Protocol / Internet Protocol
UDRP	Uniform Domain Name Dispute Resolution Policy