

William & Mary Bill of Rights Journal

Volume 20 (2011-2012)
Issue 4

Article 5

May 2012

The Internet at 20: Evolution of a Constitution for Cyberspace

Henry H. Perritt Jr.

Follow this and additional works at: <https://scholarship.law.wm.edu/wmborj>



Part of the [Internet Law Commons](#)

Repository Citation

Henry H. Perritt Jr., *The Internet at 20: Evolution of a Constitution for Cyberspace*, 20 Wm. & Mary Bill Rts. J. 1115 (2012), <https://scholarship.law.wm.edu/wmborj/vol20/iss4/5>

Copyright c 2012 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.

<https://scholarship.law.wm.edu/wmborj>

THE INTERNET AT 20: EVOLUTION OF A CONSTITUTION FOR CYBERSPACE

Henry H. Perritt, Jr. *

INTRODUCTION

In 1995, this *Journal* published my¹ article arguing for broader public access to government-generated information, explaining that the Internet provided the potential for a new window into government operations and decisions.² That article, summarized more thoroughly in Part I.C below, focused on only one aspect of the then-neophyte Internet's capacity to revolutionize how people interact with each other, participate in democratic political systems, conduct commerce, and create and communicate art.³

The Internet is now about twenty years old—measured from the time that the federal government decided to release it from its governmental sponsorship and control in the research and national security communities and launch it into the private sector as a global information infrastructure. Some of the earliest battles over the Internet were fought over access to government information. Gradually, the battlefield broadened, encompassing a wide range of federal and state constitutional issues, federal common law, and private international law.

The same core issues and principles explored in my 1995 article, however—deferring to competitive markets and encouraging them to produce a diversity of products and services, ensuring access to the marketplace by all consumers and producers, and providing a mechanism to compensate for injury⁴—now frame the full range of legal and policy questions arising from the Internet's ubiquity.

The combination of technological characteristics defining the Internet, regulatory philosophies first articulated by the Clinton administration, statutes addressing particular problems, judicial decisions, and market-driven commercial practices form

* Professor of Law and former Dean, Chicago-Kent College of Law. Member of the bar: Virginia (inactive), Pennsylvania (inactive), District of Columbia, Maryland, Illinois, Supreme Court of the United States. SB in Aeronautics and Astronautics, MIT, 1966, SM in Management, MIT Sloan School of Management, 1970, J.D., Georgetown University Law Center, 1975.

¹ To date, the author has never written an article in the first person. My involvement in the development of the Internet, however, warrants use of the first person in this Article.

² Henry H. Perritt, Jr., *Sources of Rights to Access Public Information*, 4 WM. & MARY BILL RTS. J. 179 (1995).

³ *See id.*

⁴ *Id.* at 183–90, 211.

the Internet's "constitution." As with the British Constitution, no overarching constitutional document exists; rather,

[S]afeguards of human rights and freedoms are not the rigid legalism and paper guarantees of written constitutions and Bills of Rights but the benevolent exercise of discretion by public officials, who are accountable through their political masters to the legislature and the people, accompanied by the efficiency and careful scrutiny of the legislative process.⁵

Further,

[T]here is no single, identifiable document that is widely accepted as a systematic statement of the basic tenets of British constitutional law.

But this is not the only possible definition of a "constitution." . . . [A] constitution [is] "the whole system of government of a country, the collection of rules which establish and regulate or govern the government."⁶

The same can be said about the Internet's constitution. It is not expressed in a single document. Instead, it comprises the open architecture inherent in the Internet's technological protocols together with a collection of government policies, legislative enactments, and judicial decisions that seek to protect the basic architectural philosophy, ensure space for entrepreneurial freedom, and guard against the abuse of economic or political power.

This Article looks back over the Internet's first twenty years, highlighting the crucial legal decisions by the executive, legislative, and judicial branches that have led to the Internet's success, and that now frame its constitution. I participated in many of these decisions and wrote more than a dozen law review articles and reports suggesting directions for public policy and law. This Article uses this foundation to consider the future, focusing on major legal controversies, the resolution of which will define the Internet's third decade—either strengthening or undermining its constitution.

⁵ Anthony Lester, *Fundamental Rights in the United Kingdom: The Law and the British Constitution*, 125 U. PA. L. REV. 337, 340–41 (1976) (describing the engines of the British Constitution).

⁶ Douglas W. Vick, *The Human Rights Act and the British Constitution*, 37 TEX. INT'L L.J. 329, 332 (2002) (footnotes omitted).

I. DEVELOPING A LEGAL FRAMEWORK

During the 1990s and early 2000s, policymakers and entrepreneurs developed a “constitution” for the Internet that succeeded in balancing a number of overlapping and conflicting objectives:

- ensuring open access to the physical infrastructure;⁷
- ensuring that intermediaries flourished and that content originators had free access to them;
- developing the tools for expansive e-commerce;
- developing rules for transborder jurisdiction so that the burden of enforcement did not cause intermediaries to shut out controversial content; and
- managing security, intelligence, and law enforcement goals so that people were not afraid to use the Internet.⁸

Intertwined with these objectives was the need for a system to manage Internet domain names and addresses that would be broadly acceptable around the world.

A. Foundations

Work on developing legal regimes to govern the Internet began in earnest in the mid-1990s, around the time my article was published in this *Journal*. By then, the basic technological and policy foundation for the Internet was reasonably secure.⁹ Conferences had been held at Harvard University’s Kennedy School of Government in 1990, and elsewhere, on unleashing the Internet from its academic and federally subsidized origins.¹⁰ In 1994, the National Research Council published a report on the potential of what would become the Internet to support communications and information exchange activities throughout society.¹¹ By 1995, the federal government had defunded the Internet, and handed its further development to private entities using the growing array of private networks with growing bandwidth.¹²

⁷ The infrastructure access issue initially focused on opening up the Public Switched Telephone Network (PSTN), and later on assuring net neutrality by a handful of Internet backbone service providers and content intermediaries.

⁸ See, e.g., LAWRENCE LESSIG, *CODE: AND OTHER LAWS OF CYBERSPACE* (1999).

⁹ See generally NAT’L RESEARCH COUNCIL ET AL., *REALIZING THE INFORMATION FUTURE: THE INTERNET AND BEYOND* (1994).

¹⁰ See generally Barry M. Leiner, et al., *Brief History of the Internet*, INTERNET SOC’Y (2003), available at <http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet>.

¹¹ See NAT’L RESEARCH COUNCIL ET AL., *supra* note 9.

¹² See Leiner, *supra* note 10.

The 1990 Harvard Conference addressed technological, economic, and broad public policy issues presented by the evolution of the Internet into the private sector.¹³ I was one of the few participants who focused on legal issues. My article, *Tort Liability, the First Amendment, and Equal Access to Electronic Networks*,¹⁴ refined some of the legal ideas I had first addressed in a paper presented at the conference. Observing that the unbundling of value at the heart of the Internet's architecture would result in a greater diversity of products and services, narrowly focused on particular functions, and able to interconnect seamlessly with functions performed by products and services offered by others, the article articulated three goals for the legal framework for the Internet:

1. It should promote a "diversity of information products and services in a competitive marketplace; [t]his means that suppliers must have reasonable autonomy in designing their products."¹⁵
2. It should protect "users and organizers of information content" from being "foreclosed from access to markets or audiences;"¹⁶ and
3. It must provide compensation for injury suffered from information content when victims can prove traditional levels of fault, while shielding intermediaries from liability for content posted by others.¹⁷

A small group of lawyers met monthly in Washington for a couple of years after the Harvard Conference: David Johnson, Ron Plessner, Jerry Berman, Robert Gellman,¹⁸ Kent Stuckey, and me.¹⁹ We developed ongoing relationships and conversations with other critical policy developers: Becky Burr,²⁰ Mitch Kapor,²¹ Larry

¹³ See KAHIN: BUILDING INFORMATION INFRASTRUCTURE (Brian Kahin ed., 1992) (edited versions of papers presented at the conference).

¹⁴ Henry H. Perritt, Jr., *Tort Liability, the First Amendment, and Equal Access to Electronic Networks*, 5 HARV. J.L. & TECH. 65 (1992).

¹⁵ *Id.* at 71.

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183 (2003).

¹⁹ Hereinafter the "Washington Group."

²⁰ *J. Beckwith Burr*, WILMERHALE, http://www.wilmerhale.com/becky_burr/ (last visited May 1, 2012). J. Beckwith ("Becky") Burr, then an attorney-advisor at the Federal Trade Commission (FTC) and later a senior Internet policy adviser at the National Telecommunications and Information Administration (NTIA), worked with Magaziner to develop the Clinton administration's policy for the Internet and e-commerce. *Id.* She was the Washington Group's main liaison with the Magaziner effort. *Id.*

²¹ *Biography: Mitchell Kapor*, KAPOR.COM, <http://www.kapor.com/bio/index.html> (last visited May 1, 2012). Mitch Kapor was the developer of Lotus 1-2-3, the first commercially useful spreadsheet application. *Id.* He participated in the Harvard Conference and several subsequent panel discussions on Internet policy organized by the Washington Group.

Lessig,²² and Ron Staudt.²³ Together, we helped crystallize principles that guided the broadening public discourse over the Internet.

Meanwhile, Congress was beginning to glimpse the potential. The High-Performance Computing Act of 1991²⁴ recognized the potential for society to benefit from “rapid adoption of open network standards,”²⁵ and “of an information infrastructure of data bases, services, access mechanisms, and research facilities available for use through the [Internet].”²⁶ It authorized the establishment of the National Research and Education Network,²⁷ with the capability of handling data at one gigabit per second, developed “by purchasing standard commercial transmission and network services from [private] vendors,”²⁸ and lead to the “establishment of privately operated high-speed commercial networks.”²⁹

When the Clinton administration took office in January of 1993, it became clear to those interested in wide-area computer networking that dial-up electronic bulletin boards, e-mail, and perhaps the Internet were on the threshold of revolutionizing public access to governmental information.³⁰ Vice President Gore had emerged while he was still in the Senate as an evangelist for the “Information Superhighway.”³¹ Technological visionaries were beginning to talk about the possibility of a broader “electronic commerce” revolution. Ron Plessner, a member of the Washington Group, recruited me to join the telecommunications section of the Clinton Transition

²² Larry Lessig, *Short Biography*, LESSIG BLOG, <http://www.lessig.org/info/bio> (last visited May 1, 2012). Larry Lessig, then a junior faculty member at the University of Chicago Law School, initially joined our efforts as a participant in conferences addressing Internet jurisdiction and governance. *Id.* He went on to become one of the most prominent and thoughtful public intellectuals addressing Internet issues, especially copyright law’s potential to do harm.

²³ *Faculty Biographies: Ronald W. Staudt*, IIT CHICAGO-KENT COLL. OF LAW, <http://www.kentlaw.edu/faculty/rstaudt/> (last visited May 1, 2012). Ron Staudt was a professor of law at Chicago-Kent College of Law and a pioneer in harnessing information technology to make legal institutions more effective. *Id.* As a board member of the National Center for Automated Information Research (NCAIR), he encouraged NCAIR to fund several conferences organized by the Washington Group.

²⁴ Pub. L. No. 102-194, 105 Stat. 1594 (1991) (codified at 15 U.S.C. §§ 5501–5543 (1998)).

²⁵ 15 U.S.C. § 5502(4) (1998).

²⁶ *Id.* § 5502(1)(c).

²⁷ *Id.* § 5512(a).

²⁸ *Id.* § 5512(c)(8).

²⁹ *Id.* § 5512(c)(4).

³⁰ See John Podesta, *Podesta Details Clinton Administration’s Open-Government Achievements*, FREEDOM FORUM, <http://www.freedomforum.org/packages/first/foi/podesta.htm>.

³¹ See, e.g., 137 CONG. REC. S12,734 (daily ed. Sept. 11, 1991) (statement of Sen. Gore) (referring to “information superhighway,” on passage of S. 272, High-Performance Computing and National Research Act).

Team.³² Although the nominal focus of the section was on the Federal Communications Commission (FCC), Ron and I pushed for language in our transition report addressing broader issues of networking.

It was not yet clear, however, what the administration's philosophy should be regarding the regulatory environment for the emerging technologies. The same issues of access, intermediary liability, security for e-commerce, and standardization existed whether proprietary networks like Compuserve and America Online dominated the future or whether they were marginalized by the Internet's open architecture.

The Office of Management and Budget and the General Services Administration commissioned me to write a "white paper" on some of the issues, focused on the ground rules for accessing government information, such as judicial decisions, statutes, and agency rules and regulations in electronic form.³³ The issues were easier here because they did not confront private property ownership in the purely private sphere. Indeed, a federal statute—the Freedom of Information Act (FOIA)³⁴—already guaranteed access to information in paper formats. The question was how it should be extended to electronic formats. I had already done some of the early work on how to resolve this question.³⁵

My article previously published in this *Journal* framed the problem and possible solutions:³⁶ "The [a]rticle mobilize[d] the legal arguments entitling members of the public, including publishers, to access and emphasize[d] the clash of interests when a government," tempted by new revenue possibilities, "seeks to sponsor a monopoly for access to information in electronic formats."³⁷ It analyzed FOIA and its state counterparts, which are intended to increase public access,³⁸ and copyright law, which

³² See D. Ian Hopper, *Critics Blast Report Supporting Carnivore*, ABC NEWS (Nov. 22, 2011), <http://abcnews.go.com/Technology/Story?id=119286&page=1=.TXCcaRXOFBS#.TxtNDG8V2HN>.

³³ HENRY H. PERRITT, JR., PUBLIC INFORMATION IN THE NATIONAL INFORMATION INFRASTRUCTURE, REPORT TO THE REGULATORY INFORMATION SERVICE CENTER, GENERAL SERVICES ADMINISTRATION, AND TO THE ADMINISTRATOR OF THE OFFICE OF INFORMATION AND REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET (1994).

³⁴ 5 U.S.C. § 552 (2009).

³⁵ See, e.g., Henry H. Perritt, Jr., *Determining the Content and Identifying Suppliers of Public Information in Electronic Form*, 17 GOV'T PUB. REV. 325 (1990); Henry H. Perritt, Jr., *Electronic Acquisition and Release of Federal Agency Information: Analysis of Recommendations Adopted by the Administrative Conference of the United States*, 41 ADMIN. L. REV. 253 (1989); Henry H. Perritt, Jr., *Federal Electronic Information Policy*, 63 TEMP. L. REV. 201 (1990); Henry H. Perritt, Jr. & Christopher J. Lhulier, *Information Access Rights Based on International Human Rights Law*, 45 BUFF. L. REV. 899 (1997); Henry H. Perritt, Jr., *Should Local Governments Sell Local Spatial Databases Through State Monopolies?*, 35 JURIMETRICS J. 449 (1995); Perritt, *supra* note 2; Henry H. Perritt, Jr., *The Information Highway: On Ramps, Checkpoints, and Tollbooths*, 13 GOV'T INFO. Q. 143 (1996).

³⁶ Perritt, *supra* note 2, at 179.

³⁷ *Id.*

³⁸ *Id.* at 186–95.

gives the “owner” of information the power to prevent access or use.³⁹ It considered how the First Amendment may come into play by limiting information monopolies, whether supported by copyright law or just imposed as a matter of public policy and economic interest of those already possessing the information.⁴⁰ It evaluated antitrust⁴¹ and burdens on interstate commerce⁴² limitations on information monopolies.

During the same period, I authored ACUS Recommendation 88-10,⁴³ which encouraged agencies to apply the FOIA to electronic formats, recommended greater use of information technology to disseminate agency information, and discouraged exclusive arrangements for disseminating public information. It supported agency experimentation with electronic means of providing public participation and rule-making, adjudication, and other administrative proceedings.⁴⁴ Subsequently, I drafted a set of principles for access to federal information in electronic formats eventually adopted by the American Bar Association’s House of Delegates in August 1991,⁴⁵ which shaped amendments to FOIA,⁴⁶ and worked with Ron Plesser as he mediated an agreement among stakeholders on what became the Paperwork Reduction Act of 1995.⁴⁷ Among other things, the Paperwork Reduction Act prohibited agencies from “establish[ing] an exclusive, restricted, or other distribution arrangement[s],”⁴⁸ and assured private entrepreneurs of access to public information so that they could develop their own value-added products.

While I was working on the white paper,⁴⁹ Ira Magaziner, in the White House Office, aided by Becky Burr at the National Telecommunications and Information Administration, undertook the task of developing a broader policy statement.⁵⁰ Magaziner’s effort took longer than mine because it involved a much broader spectrum of interests. It produced two documents: a “Green Paper” on Internet domain

³⁹ *Id.* at 197–204.

⁴⁰ *Id.* at 205–10.

⁴¹ *Id.* at 211–14.

⁴² *Id.* at 214–17.

⁴³ Recommendation of the Administrative Conference Regarding Federal Agency Use of Computers in Acquiring and Releasing Information, 1 C.F.R. § 305.88-10 (1989) [hereinafter ACUS Recommendation 88-10].

⁴⁴ *Id.*

⁴⁵ See Henry H. Perritt, Jr., *Electronic Freedom of Information*, 50 ADMIN. L. REV. 391, 398 n.61 (1998) (summarizing ABA recommendations).

⁴⁶ Electronic Freedom of Information Act Amendments of 1996, 110 Stat. 3048, 3050 § 5 (1996) (amending 5 U.S.C. § 552(a)(3)); see also Perritt, *supra* note 45, at 395–98 (analyzing EFOIA).

⁴⁷ Pub. L. No. 104-13, 109 Stat. 163 (1995) (codified at 44 U.S.C. §§ 3501–3520 (2002)); see Perritt, *supra* note 45, at 407–08 (analyzing Paperwork Reduction Act).

⁴⁸ 44 U.S.C. § 3506(d)(4)(A) (2002).

⁴⁹ See *supra* note 33 and accompanying text.

⁵⁰ See *infra* notes 51–52.

names,⁵¹ and a framework for global electronic commerce,⁵² both of which had seminal and continuing influence. The framework was analogous to the *Federalist Papers* in articulating constitutional principles for the Internet. It committed the United States government to “widespread competition and increased consumer choice” as the defining features of the new digital marketplace, “a non-regulatory, market-oriented approach to electronic commerce,” and discouraged “taxes and duties, restrictions on the type of information transmitted, control over standards development, licensing requirements and rate regulation of service providers,” likely to throttle the Internet in its adolescence.⁵³

From the earliest discussions about moving the Internet from the government-funded research and education communities to the private marketplace, it was apparent that new issues related to freedom of expression, access rights, and liability of intermediaries would arise.⁵⁴

B. Creative Commons Philosophy⁵⁵

These early principles developed for access to government information and for regulation of the Internet drew upon and reinforced the Internet’s unique technological architecture. The Internet is fundamentally different from the Public Switched Telephone Network (PSTN) and from broadcast radio and television networks.⁵⁶ It is indifferent to the type of traffic contained in the packets that move across it. The originating computer takes a full-motion video, an e-mail message, the text of an article, or a Facebook posting, and breaks it up into packets and sends them into the Internet.⁵⁷ Once they get into the Internet, they look like any other packets to all the

⁵¹ Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (June 10, 1998) (summarizing process for developing the Green Paper). The Green Paper is considered further in Part II.E.1.

⁵² See *Framework for Global Information Infrastructure*, THE WHITE HOUSE (July 1, 1997), <http://clinton4.nara.gov/WH/New/Commerce/read.html>.

⁵³ *Id.*

⁵⁴ See, e.g., Henry H. Perritt, Jr., *Dispute Resolution in Electronic Network Communities*, 38 VILL. L. REV. 349 (1993) (evaluating different legal models for assuring access to Internet resources); Henry H. Perritt, Jr., *The Congress, the Courts and Computer Based Communications Networks: Answering Questions about Access and Content Control*, 38 VILL. L. REV. 319 (1993) (surveying and synthesizing symposium articles on freedom of expression, intermediary liability, and access guarantees in Internet-like networks); Perritt, *supra* note 14 (identifying principal legal issues likely to shape the evolution of the Internet).

⁵⁵ The term “creative commons” came into use later, and is generally applied to applications software and content. The term, however, embraces the foundational philosophy of the Internet.

⁵⁶ See Henry H. Perritt, Jr., *Technologies of Storytelling: New Models for Movies*, 10 VA. SPORTS & ENT. L.J. 106, 215 (2010).

⁵⁷ Henry H. Perritt, Jr., *What Is the Internet?*, INTERNET JURISDICTION, <http://www.kentlaw.edu/cyberlaw/resources/whatis.html>.

routers. The receiving computer reassembles them into a full-motion video, a message, an article or a new Facebook item. This indifference to traffic content reflects the Internet's four architectural principles.

1. Different layers of the Internet perform different functions. This embodies the approach of "OSI stack," which enables each layer to pass messages to adjacent layers through a standardized, open architecture that prescribes the formats for such interlayer communication.⁵⁸ This layering principle means that the Internet itself is concerned only with passing standardized packets—Internet Packets (IP)—from one edge to another. The communications lines and switches—called "routers"—in the middle of the Internet "cloud"⁵⁹ are indifferent to the content of the IP packets that traverse the cloud. This layering or building block approach means that designers of any one layer can make engineering judgments for that layer without concerning themselves with the capacity of adjacent layers to handle their traffic.⁶⁰ The result is more specialized innovation and a more competitive market structure than if innovation at any one layer had to wait until all the other layers involved could be adapted.

2. Closely related to the layering principle is the Internet's "end-to-end design principle."⁶¹ Applications such as email processing, compression and decompression of audio or video files, reassembly of message components into the proper order, take place in applications outside, rather than inside, the cloud.⁶² This contrasts sharply with the design principle of the traditional circuit-switched PSTN, where most of the intelligence is inside the network and the devices beyond the edges of the network are relatively "stupid."⁶³ The end-to-end principle enhances competition because it leaves it to users and providers operating beyond the edge of the network to decide what applications they want to use and what innovations they want to make or commission.

3. "[T]he Internet Protocol separates the underlying network from the services that ride on top of them. IP [i]s . . . an open standard, so that anyone c[an] use it to create new applications and new networks."⁶⁴ Thus, the Internet can be implemented on almost any kind of underlying communications channel, including dedicated telephone trunk circuits, optical fiber modulation and multiplexing protocols, microwave or other radio. The underlying communications technologies affect the bandwidth of Internet connectivity obtainable over those protocols, but otherwise the users of the

⁵⁸ Perritt, *supra* note 56, at 214–15.

⁵⁹ "The Internet is frequently represented in network diagrams as a cloud, signifying that users communicating through the Internet do not need to be concerned what is inside the cloud." *Id.* at 214 n.467.

⁶⁰ *Id.*

⁶¹ See Perritt, *supra* note 56, at 215; Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1164–65 n.2 (1999).

⁶² Perritt, *supra* note 56.

⁶³ *Id.* at 215.

⁶⁴ *Reconsidering Our Communications Laws: Ensuring Competition and Innovation: Hearing Before the S. Comm. on the Judiciary*, 109th Cong., 2d Sess. 116 (2006) (statement of Vinton G. Cerf, Vice President and Chief Internet Evangelist, Google Inc.).

Internet do not need to be concerned about how the bits are actually transmitted and received through wires, optical fibers, or space.

4. The overarching rationale, a result of honoring the first three, is that no central gatekeeper controls the Internet. This governing principle allows for creativity to occur at the network edges. In such an environment, entrepreneurs with new ideas for applications do not need permission for their inventions to reach end users. Closed networks, like cable video systems, are different. There, network owners control what consumers can see and do.⁶⁵

C. Ensuring Access

The need to ensure the integration of all of the Internet's separate parts was apparent early in the Internet's emergence.⁶⁶ To do this, anyone who wanted to contribute to the communications and information infrastructure represented by the Internet must have access. Common carrier regulation was the traditional means for the law to guarantee access to communications and transportation infrastructures, but common carrier regulation was not consistent with decentralization and privatization.⁶⁷

1. Telecommunications Act of 1996

The Telecommunications Act of 1996 moved public policy fundamentally away from a centralized regulated monopoly approach toward a competitive one more reliant on market forces.⁶⁸ Central to its philosophy was ensuring access to the infrastructure. The Act was premised on the now-quaint vision that the future would be dominated by video entertainment transmitted by telephone companies and telecommunications service provided by cable companies.⁶⁹ The word "Internet" appears only four times in the statute,⁷⁰ outside special provisions dealing with protecting children from harmful information on the Internet. At the same time, however, it fundamentally altered the industry structure by opening up competition in the

⁶⁵ *Id.* at 2–3.

⁶⁶ See generally Henry H. Perritt, Jr., *Access to the National Information Infrastructure*, 30 WAKE FOREST L. REV. 51 (1995) (analyzing traditional legal mechanisms for assuring access to communications infrastructures and recommending a minimalist approach for law, focused on interfaces).

⁶⁷ See *id.* at 67.

⁶⁸ See Nicholas Economides, *The Telecommunications Act of 1996 and Its Impact*, 11 JAPAN & WORLD ECON. 455, 456–57 (1999).

⁶⁹ H.R. REP. NO. 104-204(i) at *53 (1995), reprinted in 1996 U.S.C.C.A.N. 10, 16–17 (“Telephone company entry into the delivery of video services will encourage telephone companies to modernize their communications infrastructure. Specifically, the deployment of broadband networks would be accelerated if telephone companies were permitted to offer video programming. These networks would be capable of transmitting voice, data, and video to consumers.”).

⁷⁰ Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

PSTN.⁷¹ It also instructed the FCC to take action to provide incentives to deploy advanced broadband technologies.⁷² Pitched battles ensued before the Commission and in the courts over how competition should be assured under the Act.⁷³

The 1996 legislation expresses a preference for facilities-based competition.⁷⁴ A facilities-based competitor has its own physical infrastructure.⁷⁵ But, to achieve a completely facilities-based market structure, new entrants would have to overcome enormous economic and legal barriers to entry. They would have to build their own local loops, dig up the streets to bury their wires or optical fiber, put up their own poles to carry above-ground wire and fiber, and deploy their own switching centers. The core legal strategy embedded in the 1996 Act was to use its interconnection, unbundling, and resale obligations as a way of giving new entrants a foothold until they could build out their own physical infrastructure.⁷⁶ Incentives for incumbents also were important. If incumbents could receive revenue for sharing their existing facilities with new entrants, they might have less incentive to deploy new technologies that would reduce costs and open up revenue opportunities from new product lines. The FCC dealt with this possible adverse incentive by basing allowable charges for new entrants on forward-looking, rather than historical, costs.⁷⁷ The incumbent could not recover costs based on the cost of its embedded technologies, but on the costs of the most efficient technology in the marketplace—costs that were falling rapidly.⁷⁸ That reduced total revenue achievable by maintaining existing assets and provided an incentive to the incumbent to upgrade.⁷⁹

⁷¹ See 47 U.S.C. § 251 (1999) (requiring interconnection and unbundling of network elements); *id.* § 259 (requiring established providers to share infrastructure with new entrants); *id.* § 271 (blocking Bell operating companies from entering the long distance market until they ensured competition in their local exchange markets).

⁷² See *id.* § 1302 (2008); see also *Ad Hoc Telecomm. Users Comm. v. FCC*, 572 F.3d 903, 908 (D.C. Cir. 2009) (characterizing Telecommunications Act of 1996, 47 U.S.C. § 1302).

⁷³ See generally HENRY H. PERRITT, JR., *DIGITAL COMMUNICATIONS LAW* § 7 (rev. ed. 2010) (analyzing details of FCC decisions and court decisions under the 1996 Act).

⁷⁴ See H.R. REP. NO. 104-204(i) (explaining the need for the resale obligation to permit emergence of facilities-based competition).

⁷⁵ *Id.*

⁷⁶ See generally Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

⁷⁷ *Id.*; 47 C.F.R. § 51.505 (2012).

⁷⁸ See *id.*

⁷⁹ See *Time Warner Cable*, 15 FCC Rcd. 1124, 1134 (Jan. 5, 2000) (explaining that incumbent cable television providers are not entitled to access open video systems in their market area “in order to preserve the incentive of such cable operators to upgrade and maintain their franchised systems and to promote facilities-based competition. If such an operator were permitted to become a programming provider on an open video system serving its franchise areas, it would have less incentive to invest in its own facilities and strengthen its position as a facilities-based competitor in these areas.” (footnote omitted)).

Three years after the enactment of the 1996 Act, some of the key controversies reached the Supreme Court in *AT&T Corp. v. Iowa Utilities Board*.⁸⁰ The Court approved most aspects of the FCC's approach, and directed that the Commission give more attention to the criteria for unbundling and sharing specific network elements.⁸¹

2. "Digital Tornado"

Shortly after enactment of the 1996 Act, on March 27, 1997, the FCC released a staff paper entitled *Digital Tornado: The Internet and Telecommunications Policy*, authored by Kevin Werbach, analyzing the FCC policy alternatives for the Internet.⁸² A central theme running through the paper was that the FCC, and other government agencies, should seek to limit regulation of Internet services.⁸³ In framing his approach, Werbach stated:

Because it is not tied to traditional models or regulatory environments, the Internet holds the potential to dramatically change the communications landscape. The Internet creates new forms of competition, valuable services for end users, and benefits to the economy. Government policy approaches toward the Internet should therefore start from two basic principles: avoid unnecessary regulation, and question the applicability of traditional rules.⁸⁴

3. Making the "Pipe" Bigger

Once the basic decision was made to privatize and commercialize the Internet, and once the PSTN was opened up, key technological developments increased the momentum through the 1990s and 2000s. The first barrier to fall allowed access speeds to increase.⁸⁵ When the Internet was unleashed in the early 1990s, access was possible through dedicated lines leased from the telephone company or through dial-up

⁸⁰ 525 U.S. 366 (1999).

⁸¹ *Id.* at 387–92.

⁸² Kevin Werbach, *Digital Tornado: The Internet and Telecommunications Policy* (FCC Office of Plans & Policy, Working Paper No. 29, 1997), available at http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf.

⁸³ *Id.*

⁸⁴ *Id.* at ii.

⁸⁵ Use of the word "speed" is potentially misleading. All electronic signals move more or less at the speed of light—186,000 miles per second. The rate at which data can be handled, however, depends on bandwidth. An ordinary telephone voice circuit provides about 4 KHz of bandwidth, limiting data rates to 56 Kbps with advanced modulation techniques. See MARGARET LEVINE YOUNG, *INTERNET: THE COMPLETE REFERENCE* 10 (2d ed. 2002). "Speed," as used in this text, refers to the speed of data transmission.

modems connected to ordinary voice telephone lines.⁸⁶ By the early 2000s, penetration of cable television infrastructure, the development of cable modems, and the modification of cable networks to handle traffic in both directions, revolutionized bandwidth available at the edges of the network.

Somewhat later, new technologies deployed by the telephone companies, principally Digital Subscriber Lines (DSLs), allowed data rates on retail telephone lines to increase commensurately.⁸⁷ By the end of the twentieth century, major telephone service providers, having mainly crushed the threat of competitive local exchange carriers (CLECs),⁸⁸ committed substantial capital to improve their networks⁸⁹ by deploying optical fiber beyond central offices,⁹⁰ often directly to residences and commercial premises, and marketing DSL service to all of their customers.

One of the impediments to widespread use of the Internet was the need to know the domain name (URL) of a desired destination. Search engines evolved as a kind of automated index to URLs. One of the most successful early search engines was AltaVista, developed by Digital Equipment Corporation and introduced in 1995.⁹¹ By the beginning of 1999, Google began to emerge as a search engine with a better search algorithm,⁹² and by the mid-2000s it dominated the search engine industry.⁹³

⁸⁶ Typical bandwidth was 1.4 to 1.5 Mbps on a leased T1 line or 56 Kbps through a dial-up modem. *Id.* at 13.

⁸⁷ DSL, developed at Bellcore in the mid-1980s, demonstrated the feasibility of inserting broadband digital signals on the wires designed for baseband analog voice signals. See Gareth Marples, *The History of DSL Internet Access—A Race for Technological Speed*, THEHISTORYOF.NET (Sept. 11, 2008), <http://thehistoryof.net/history-of-dsl.html>.

⁸⁸ The Telecommunications Act of 1996 allowed competitive local exchange carriers to compete with incumbent local exchange carriers by allowing CLECs to use their infrastructure. *CLEC*, WEBOPEDIA, <http://www.webopedia.com/TERM/C/CLEC.html> (last visited May 1, 2012).

⁸⁹ Widespread availability of DSL required telephone companies to remove loading coils from the part of the network that connected central offices to residential and commercial customers. Loading coils extend the reach of voice signals by reducing the capacitance of longer lines. See *Load Coils?*, DSLREPORTS.COM, <http://www.dslreports.com/faq/657> (last visited May 1, 2012). Capacitance is an undesirable feature of a communications channel because it smooths out the oscillations in an analog signal. See *id.* Loading coils, however, also block higher frequency signals, making DSL data transmission impossible.

⁹⁰ Widespread deployment of an optical fiber infrastructure has made it possible for the Internet to accommodate exploding demand for higher bandwidth. Signals transmitted over optical fiber experience much less attenuation and interference than the same signals transmitted over copper (or other metallic) wire. An optical fiber offers orders of magnitude, higher bandwidths, and longer link distances than copper wire.

⁹¹ *AltaVista: A Brief History of the AltaVista Search Engine*, WEBSEARCHWORKSHOP, http://www.websearchworkshop.co.uk/altavista_history.php (last visited May 1, 2012).

⁹² *Google History*, GOOGLE, <http://www.google.com/about/corporate/company/history.html> (last visited May 1, 2012).

⁹³ *Google: A Brief History of the Google Search Engine*, WEBSEARCHWORKSHOP, http://www.websearchworkshop.co.uk/google_history.php (last visited May 1, 2012).

Compression algorithms facilitated distribution of music and videos. Internet distribution of music exploded with the development of the MP3 compression algorithm and associated hardware and software known as codecs.⁹⁴ The introduction of mpeg-4 in 1998 similarly facilitated Internet distribution of full-motion video files.⁹⁵

Load sharing was widespread by 2000, enhancing the capacity of popular websites.⁹⁶ As e-commerce exploded, the traffic to popular websites was more than a single server could handle.⁹⁷ A protocol was needed that could share the burden among multiple servers controlled by the same entity and providing essentially the same information.⁹⁸ The result was “load sharing,” which “balance[s] the load across a bunch of physical servers . . . mak[ing] those servers look like one great big server to the outside world.”⁹⁹

Wireless data communications at speeds similar to those employed in wired computer networks have permitted the Internet to expand beyond the infrastructure defined by physical wires.¹⁰⁰ One can access the Internet now—at least in areas of fairly dense population—from anywhere.

Development and deployment of wireless data systems that could handle data at speeds useful to computer networks awaited assignment of higher-frequency radio spectrum and hardware that could operate at those higher frequencies.¹⁰¹ In 1985,

⁹⁴ Mary Bellis, *The History of MP3*, ABOUT.COM (2012), <http://inventors.about.com/od/mstartinventions/a/MPThree.htm>.

⁹⁵ Both standards involve patented technology that is licensed by MPEG LA, LLC. MPEGLA, <http://www.mpegla.com/main/default.aspx> (last visited May 1, 2012); *see id.*

⁹⁶ Load balancing was a feature of Microsoft Windows NT, introduced in 1993. *A History of Windows*, MICROSOFT.COM, <http://windows.microsoft.com/en-us/windows/history> (last visited May 1, 2012). Cisco introduced a more sophisticated load-balancing product in 1996, promoted as a replacement for the Domain Name Service (DNS) round robin strategy. CISCO SYS., *Load Balancing 1* (1998), available at http://www.cisco.com/warp/public/cc/pd/cxsr/400/tech/lobal_wp.pdf.

⁹⁷ KJ (Ken) Salchow, Jr., *Load Balancing 101: The Evolution to Application Delivery Controllers 1* (2007), available at <http://www.f5.com/ppc/downloads/load-balancing101-evolution-adc.pdf>.

⁹⁸ *Id.*

⁹⁹ *Id.* Early efforts involved having a DNS serving the URL of the service provide different IP addresses in rotation, as queries were received. *Id.* at 1–2. Later developments involved having a cluster of servers listen to one IP address through a border router, which then redirected queries to various servers behind the firewall with locally assigned IP addresses. *Id.* at 3. Later, “application delivery controllers” were developed, which resided outside application servers. They presented virtual server addresses to the outside world and then forwarded connections to the most appropriate real server. *Id.* at 4.

¹⁰⁰ *See*, YOUNG, *supra* note 85, at 15.

¹⁰¹ Theoretical principles of radio engineering dictate that the bandwidth of a signal increases as the data rate being transmitted increases. The higher bandwidth necessary for higher data rates could not be accommodated at lower frequencies which were already crowded with broadcast radio and television, military and public safety, and other commercial communications.

the FCC first authorized the use of unlicensed¹⁰² spread spectrum¹⁰³ transmitters in the 902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz bands.¹⁰⁴ The result was an explosion of wireless local area networks (LANs) under protocols popularly known as Wi-Fi.¹⁰⁵

Third (3G) and fourth generation (4G) wireless technologies, generally associated with smart phones, enable high-bandwidth wireless connections for a variety of portable devices, including smartphones, tablets such as the iPad, and netbook and laptop computers.¹⁰⁶ These technologies became commercially available in 2001¹⁰⁷ and 2010, respectively.¹⁰⁸ Expanding broadband wireless access was an important goal of the congressionally mandated National Broadband Plan,¹⁰⁹ published by the FCC in 2010.¹¹⁰

The ubiquity of high-bandwidth wireless data connections means that one can be connected to the Internet all the time. Constant connectivity has two major implications. First, it dramatically increases demand for Internet-accessible products and services. Audiences can listen to music almost constantly, watch movies or other video entertainment at odd moments of leisure while they wait for appointments or ride the bus or train, and order books or other consumer products impulsively, as soon as they

¹⁰² Before that, every transmitter required a station license.

¹⁰³ The FCC explained spread spectrum modulation: “Spread spectrum communication systems use special modulation techniques that spread the energy of the signal being transmitted over a very wide bandwidth. The information to be conveyed is modulated onto a carrier by some conventional techniques, usually a digital modulation technique, and the bandwidth of the signal is deliberately widened by means of a spreading function. The spreading technique used in the transmitter is duplicated in the receiver to enable detection and decoding of the signal. Spread spectrum systems offer two important technological advantages over conventional transmission schemes. First, the spreading reduces the power density of the signal at any given frequency within the transmitted bandwidth, thereby reducing the probability of causing interference to other signals occupying the same spectrum. Second, the signal processing in spread spectrum systems tends to suppress undesired signals, thereby enabling such systems to tolerate strong interfering signals.” FCC SPECTRUM POLICY TASK FORCE, REPORT OF THE UNLICENSED DEVICES AND EXPERIMENTAL LICENSES WORKING GROUP 8 n.13 (2002), available at <http://transition.fcc.gov/sptf/files/E&UWGFinalReport.pdf> [hereinafter FCC UNLICENSED DEVICES REPORT].

¹⁰⁴ *Id.* at 8.

¹⁰⁵ *Id.* at 6.

¹⁰⁶ *3G and 4G Wireless*, FCC, <http://www.fcc.gov/topic/3g-4g-wireless> (last visited May 1, 2012).

¹⁰⁷ See Danielle Dunne, *What is ‘3G’ Technology?*, CNN.COM (Oct. 22, 2001), <http://europe.cnn.com/2001/TECH/industry/10/22/3g.defined.idg/index.html>.

¹⁰⁸ Kristena Hansen, *4G Wireless Technology: A Look at What’s Ahead*, L.A. TIMES (June 13, 2010), <http://articles.latimes.com/2010/jun/13/business/la-fi-4g-20100614>.

¹⁰⁹ 47 U.S.C. § 1305 (2005) (authorizing the establishment of a national broadband service development and expansion program).

¹¹⁰ FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN (2010), available at <http://download.broadband.gov/plan/national-broadband-plan.pdf>.

hear favorable reports from a friend or on the radio or television. This phenomenon means that industry structures built around segmentation of delivery channels—such as movie theaters, television, and DVDs in the video entertainment industry—must now recalibrate their business models to accommodate a marketplace where the old product categories are irrelevant.

Second, ease of use becomes even more important when one is browsing the Internet, checking out friends on Facebook, playing a song, watching a movie, or ordering merchandise on a small handheld device instead of a desktop or laptop computer. This means that consumers will gravitate to one-stop, integrated services, such as Amazon and Facebook, instead of going to the trouble of checking out different websites. This is likely to intensify the preference for cyberspace “empires,” considered in Part II.A.

4. Convergence of Cable Modem and Telephone Regulation

The FCC gradually merged aspects of cable and telephone regulation as it applied to the Internet, initially deregulating DSL, and more recently recognizing that some regulation may be necessary to assure net neutrality, as considered in Part II.B.

In *National Cable & Telecommunications Ass’n v. Brand X Internet Services*,¹¹¹ the Supreme Court upheld the FCC’s determination that broadband Internet service provided by cable companies does not constitute a “telecommunications service” under Title II of the Communications Act.¹¹² Accordingly, such service is not subject to mandatory common carrier regulation. Shortly after deregulating cable modem service, the FCC announced a decision to treat broadband Internet access provided by Regional Bell Operating Companies (RBOCs) like cable modem Internet access,¹¹³ placing telephone company offerings of broadband service outside all the traditional telephone company regulatory requirements—common-carriage, unbundling, resale, tariffing, price regulation, and inter-carrier compensation.¹¹⁴

Robust competition for Internet access services is emerging and will accelerate, the Commission concluded, encompassing not only the present market leaders, cable modem service and DSL service, but increasingly satellite-based and fixed broadband wireless,¹¹⁵ and access through the electricity grid.

¹¹¹ 545 U.S. 967 (2005).

¹¹² *Id.* at 996–97.

¹¹³ Appropriate Framework for Broadband Access to the Internet over Wireline Facilities et al., 20 FCC Rcd. 14853 (2005).

¹¹⁴ Exemption of the broadband pipe provided by the telephone companies does not, however, mean that the services they provide that run through the pipe are exempt. Consider the FCC’s treatment of voice over IP Providers (VoIP). *See id.* ¶ 54, at 14964.

¹¹⁵ *Id.* ¶ 59, at 14885.

D. Domain Name Regulation

Domain name administration is central to regulation of the Internet.¹¹⁶ One can have an Internet presence such as a website only if one has a domain name.¹¹⁷ Refusal to register a domain name or revocation of an existing domain name excludes the applicant or holder from the Internet. Accordingly, whoever regulates domain names has fundamental regulatory control over the Internet.

Certain characteristics of the Internet make regulation of addresses and domain names necessary. The Internet's common name and address space means that each domain name and numerical Internet address must be unique. Otherwise, routers could not route packets unambiguously to the correct destination.

Soon after taking office, the Clinton administration undertook the task of deciding how domain name regulation should work in a decentralized, privatized Internet.¹¹⁸ The process continued until well into the President's second term, and resulted in the Green Paper,¹¹⁹ which announced that the United States government would recognize a new not-for-profit corporation that would take over administration of the domain name system.¹²⁰ The result was the Internet Corporation for Assigned Names and Numbers (ICANN).¹²¹

¹¹⁶ The system for assigning domain names and for managing the top levels of the hierarchical DNS are described in RFC 1591. J. Postel, *Domain Name System Structure and Delegation, Request for Comments: 1591* (Mar. 1994), available at <http://www.ietf.org/rfc/rfc1591.txt>.

¹¹⁷ That is not strictly true. Internet packets are routed based on numerical IP addresses. One could theoretically maintain an Internet presence with an IP address and without a domain name, but users seeking the holder of the IP address would have to know the numerical address. Moreover, assignment of IP addresses is integrated with assignment of domain names. Management of Internet Names and Addresses, 63 Fed. Reg. 31,741, 31,742 (June 10, 1998) (explaining the relationship between assigning IP addresses and assignment of domain names) [hereinafter White Paper].

¹¹⁸ See Improvement of Technical Management of Internet Names and Addresses, 63 Fed. Reg. 8826, 8827 (Feb. 20, 1998) [hereinafter Green Paper].

¹¹⁹ See White Paper, *supra* note 117, at 31,741 (summarizing process for developing the Green Paper). The Green Paper actually was a proposal with a request for comments. See Green Paper, *supra* note 118, at 8827. The policy statement emerged from the comment process. White Paper, *supra* note 117, at 31,741 (explaining the Green Paper). Nevertheless, the final policy statement is popularly known as the Green Paper, as well.

¹²⁰ White Paper, *supra* note 117, at 31,749.

¹²¹ Under solicitation number 52SBNT9C1020, the National Institute of Standards and Technology solicited a sole source contract from ICANN. The United States government and ICANN entered into a memorandum of understanding that provided ground rules for ICANN. HENRY H. PERRITT, JR., *LAW AND THE INFORMATION SUPERHIGHWAY* 521 (2d ed. 2001). The relationship among ICANN, registries, and registrars is summarized in *Dotster, Inc. v. ICANN*, 296 F. Supp. 2d 1159, 1160 (C.D. Cal. 2003).

ICANN adopted the Uniform Domain-Name Dispute Resolution Policy,¹²² imposing on all registrants of domain names an obligation to submit to private dispute resolution under ICANN rules.¹²³ ICANN also adopted rules for domain name dispute resolution.¹²⁴ The rules provide uniform standards for complaints, private resolution panels, and power of panels.¹²⁵ A number of organizations, including the World Intellectual Property Organization (WIPO), established dispute resolution mechanisms to comply with the ICANN rules.¹²⁶ The WIPO panels have resolved several thousand disputes, although WIPO's Uniform Dispute Resolution Policy has been subjected to sharp criticism.¹²⁷ I am a member of the panel for WIPO dispute resolution.¹²⁸

Though the ICANN dispute resolution system is limited to disputes alleging that domain names interfere with trademarks, a broader power exists as well.¹²⁹ Registries are obligated by standard ICANN terms to terminate domain names when the holder engages in "abuse."¹³⁰ In October 2008, the ICANN staff issued a report on registration abuse policies, critical of the lack of uniform policies in applying the abuse standard.¹³¹ Nevertheless, the abuse policies are potentially available to use domain names as leverage to enforce a broader set of legal duties. Enforcing an international or foreign adjudicatory decision against Internet domain names can be an effective supplement to traditional judgment execution against tangible property. The domain registry would be the "sheriff," acting on a "writ of execution."¹³² As the ICANN Staff Report indicated, more uniform policies are needed to make clear what "judgments" are entitled to enforcement and what process is due before a domain name is revoked.¹³³

¹²² See *Domain Name Dispute Resolution Policies*, ICANN, <http://www.icann.org/en/udrp/> (last visited May 1, 2012).

¹²³ *Uniform Domain-Name Dispute-Resolution Policy*, ICANN (Oct. 24, 1999), available at <http://www.icann.org/udrp/udrp.htm>.

¹²⁴ *Id.*

¹²⁵ See, e.g., *Domain Name Dispute Resolution Policies*, *supra* note 122.

¹²⁶ See *Domain Name Dispute Resolution Service for Generic Top-Level Domains*, WORLD INTELLECTUAL PROP. ORG., <http://www.wipo.int/amc/en/domains/gtld/> (last visited May 1, 2012).

¹²⁷ See, e.g., A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 96–101 (2000).

¹²⁸ *WIPO Domain Name Panelists*, WORLD INTELLECTUAL PROP. ORG., <http://www.wipo.int/amc/en/domains/panel/panelists.html> (last visited May 1, 2012).

¹²⁹ See *Uniform Domain Name Dispute Resolution Policy*, *supra* note 123.

¹³⁰ MARIKA KONINGS, GNSO ISSUES REPORT ON REGISTRATION ABUSE POLICIES 11 (2008), available at <http://gnso.icann.org/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29Oct08.pdf> [hereinafter ABUSE REPORT].

¹³¹ *Id.* at 5.

¹³² Henry H. Perritt, Jr., *Will the Judgment-Proof Own Cyberspace?*, 32 INT'L LAW. 1121, 1148 (1998).

¹³³ ABUSE REPORT, *supra* note 130, at 45; see also Perritt, *supra* note 132, at 1178.

E. Immunity for Intermediaries

Tort liability for intermediaries might impede broad access. On the other hand, intermediaries are attractive targets to satisfy the transborder jurisdiction problem, as considered in Part I.F. This tension concerned the Washington Group. We brainstormed about two directions for legal intervention: recognizing an immunity for intermediaries, and establishment of an alternative dispute resolution mechanism to address most claims of harm resulting from Internet-based content.¹³⁴ The immunity we considered was codified in section 230 of the Communications Decency Act,¹³⁵ for everything except intellectual property, and in the safe harbor provisions of the Digital Millennium Copyright Act (DMCA).¹³⁶

Alternative dispute resolution would reduce intermediary concerns about liability because it could lessen the uncertainty and costs of litigation in the regular courts, and could limit remedies to removal of the accused content. Even if such systems did not preempt traditional judicial processes and remedies—which would be difficult to do without an international treaty—it would divert many controversies into the alternative system. The alternative dispute resolution ideas were partially codified in the Domain Name Dispute Resolution system mandated as a requirement for Domain Name registrars,¹³⁷ and in the procedural provisions of the DMCA safe harbor.¹³⁸

F. Jurisdiction

Figuring out how the Internet should be regulated involved figuring out how prescriptive and adjudicatory jurisdiction¹³⁹ should work.¹⁴⁰ Legal jurisdiction is

¹³⁴ See *supra* notes 19–23 and accompanying text.

¹³⁵ Pub. L. No. 104-104, 110 Stat. 137 (1996) (codified as amended at 47 U.S.C. § 230 (2006)).

¹³⁶ Digital Millennium Copyright Act, Pub. L. No. 105-304, § 202(a), 112 Stat. 2877 (1998) (codified as amended at 17 U.S.C. § 512 (2006)). The Safe Harbor Provisions of the DCMA were brokered to a significant degree by Washington Group member Ron Plesser, who had chaired the telecommunications section of President Clinton's Transition Team.

¹³⁷ See *supra* Part I.D.

¹³⁸ To qualify for the immunity, a service provider must remove material when it receives notice directed to its designated agent claiming that the material infringes a copyright. The notice must meet requirements defined in the statute. The originator of removed material is entitled to notice and to have the material put back up unless the person claiming copyright infringement files suit for infringement. 17 U.S.C. § 512(c)(2)–(3), (g)(2)(C).

¹³⁹ Known as “personal jurisdiction” in the United States. See Michael D. Ramsey, *International Law Limits on Investor Liability in Human Rights Litigation*, 50 HARV. INT'L L.J. 271, 296 (2009).

¹⁴⁰ Prescriptive jurisdiction refers to the power to make rules. Adjudicatory jurisdiction refers to the power to adjudicate alleged rule violations. See Graeme B. Dinwoodie, *Developing a Private International Intellectual Property Law: The Demise of Territoriality?*, 51 WM. &

fundamentally local, aligned with the boundaries of sovereign power; the Internet is inherently global, crossing sovereign boundaries.

A number of early cases, some involving pre-Internet technologies such as dial-up bulletin boards, crystallized concerns that traditional doctrines of adjudicative jurisdiction might be unsuitable for the Internet.¹⁴¹ The early case law was synthesized by the district court in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*,¹⁴² which articulated a “sliding scale,” relied on in many subsequent personal jurisdiction cases.¹⁴³ *Zippo* held that passive websites should not be subject to jurisdiction merely because they were visible in the forum state, but that contracts involving knowing and repeated transmission of files to and from the forum state would support jurisdiction.¹⁴⁴ In between these two extremes, jurisdiction should depend on the degree of interactivity built into the website.¹⁴⁵

I wrote two law review articles in the mid-1990s summarizing the state of the debate.¹⁴⁶ At first, it was difficult to get the American Bar Association and others interested in the question. The prevailing view among lawyers was that the Internet was a toy and would never become a significant channel for professional interaction or commerce. Nevertheless, some of us in the bar, the industry, and the academic and policy communities argued about how to adapt traditional jurisdiction concepts to the realities of the Internet.¹⁴⁷

The two poles in the debate were framed by David Johnson (a member of the Washington Group) and David Post, on the one hand, and Jack Goldsmith, on the other.¹⁴⁸ In 1997, as I was moving from the faculty of Villanova University School of Law to become the Dean at Chicago-Kent College, I organized a law review

MARY L. REV. 711, 785 (2009) (distinguishing between prescriptive and adjudicatory jurisdiction); Ramsey, *supra* note 139, at 295–96 (same).

¹⁴¹ *Compare* *CompuServe, Inc. v. Patterson*, 89 F.3d 1257, 1264–66 (6th Cir. 1996) (finding personal jurisdiction in Ohio over a Texas resident who purposefully directed business activities toward Ohio by knowingly entering into a contract with CompuServe, an Ohio resident, and then “deliberately” and “repeatedly” transmitting files to Ohio), *and* *Inset Sys., Inc. v. Instruction Set*, 937 F. Supp. 161, 165 (D. Conn. 1996) (finding personal jurisdiction because advertising on the Internet constituted purposeful doing of business in Connecticut because “unlike television and radio advertising, the advertisement is available continuously to any Internet user”), *with* *Bensusan Rest. Corp. v. King*, 937 F. Supp. 295, 301 (S.D.N.Y. 1996) (refusing to exercise jurisdiction based on passive website alone and distinguishing *CompuServe*).

¹⁴² 952 F. Supp. 1119 (W.D. Pa. 1997).

¹⁴³ *Id.* at 1124.

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

¹⁴⁶ Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1 (1996); Henry H. Perritt, Jr., *Will the Judgment-Proof Own Cyberspace?*, 32 INT’L LAW. 1121 (1998).

¹⁴⁷ Perritt, *Jurisdiction in Cyberspace*, *supra* note 146, at 4.

¹⁴⁸ *See infra* notes 149–51 and accompanying text.

symposium including Johnson and Goldsmith to explore the debate among several of us about Internet jurisdiction.¹⁴⁹

Post and Johnson argued that, “[C]yberspace—is creating a realm of human interaction in which . . . physical location and physical space are becoming both indeterminate and functionally irrelevant.”¹⁵⁰ “Cyberspace . . . needs and can create its own law and legal institutions.”¹⁵¹ Jack Goldsmith argued that cyberspace is not “hermetically separated from the ‘real’ world.”¹⁵² “The easiest way to control illegal cross-border information flows is to enforce the regulation against the local assets of the foreign supplier of the information.”¹⁵³

The Computer Science and Telecommunications Board of the National Academy of Sciences convened a committee on “Global Networks and Local Values” in the late 1990s to consider these questions.¹⁵⁴ The committee’s report¹⁵⁵ stopped short of making policy recommendations, but observed that “extraterritorial enforcement of national laws is possible in principle, [but] this generally presupposes that the nation-state can exercise jurisdiction over some element of the transnational activity—e.g., by seizing local property or by restricting access to its market.”¹⁵⁶

At the turn of the century, the Hague Conference on Private International Law undertook an effort to negotiate an international convention on adjudicatory jurisdiction and transnational enforcement of judgments in the international e-commerce context.¹⁵⁷ Expert groups convened by the Conference¹⁵⁸ considered the idea of

¹⁴⁹ See Symposium, *Symposium on the Internet and Legal Theory*, 73 CHI.-KENT L. REV. 941 (1998).

¹⁵⁰ David G. Post & David R. Johnson, “*Chaos Prevailing on Every Continent*”: *Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055, 1057–58 (1998).

¹⁵¹ David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

¹⁵² Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119, 1119 (1998).

¹⁵³ *Id.* at 1125.

¹⁵⁴ *Global Networks and Local Values*, COMPUTER SCI. & TELECOMM. BD., http://sites.nationalacademies.org/CSTB/CompletedProjects/CSTB_042333. I served as a member of the committee. *Faculty Biographies: Henry H. Perritt Jr.*, IIT CHICAGO-KENT COLLEGE OF LAW (Aug. 18, 2010), <http://www.kentlaw.edu/faculty/hperritt/>.

¹⁵⁵ NAT’L ACAD. OF SCIS. NAT’L RESEARCH COUNCIL, *GLOBAL NETWORKS AND LOCAL VALUES: A COMPARATIVE LOOK AT GERMANY AND THE UNITED STATES (2001)*, available at <http://www.nap.edu/catalog/10033.html>.

¹⁵⁶ *Id.* at 192.

¹⁵⁷ Press Release, Hague Conference on Private International Law, Geneva Round Table on Electronic Commerce and Private International Law (Sept. 2, 2001), available at <http://www.hcch.net/upload/wop/press01e.html>. I was an active participant in the resulting activities. See *id.*

¹⁵⁸ See Hague Conference on Private International Law, *Electronic Commerce and the Internet (Press Release Including Conclusions and Recommendations)* (Sept. 2, 1999), http://www.hcch.net/index_en.php?act=events.details&year=1999&varevent=63 (announcing round table of experts in Geneva); HAGUE CONFERENCE ON PRIVATE INT’L LAW, ELECTRONIC

“targeting” as a principle for localizing Internet activity: targeting consumers in a particular country would support jurisdiction; unsophisticated sites not engaging in targeting would not be subject to jurisdiction elsewhere based on the website alone.¹⁵⁹

Early in the activities of the Conference, I encouraged the State Department representative to reach out to stakeholders and get them involved—there would be little point in developing a draft convention only to have significant political interests in the United States torpedo it. Representatives of the entertainment industry (led by Disney) and representatives of the Internet industry were split.¹⁶⁰ The entertainment industry favored expansive jurisdictional rules because they wanted to be able to sue alleged copyright infringers in United States courts.¹⁶¹ The Internet industry, particularly internet service providers (ISPs), wanted restrictive jurisdictional rules because they wanted to insulate themselves from litigation in foreign forums.¹⁶² The French *Yahoo!* case was on everyone’s mind.¹⁶³ Because of the conflict between the two most important stakeholders, the United States government was unable to take a position on the more important issues at the center of the effort. This frustrated and annoyed the non-U.S. participants, and the result was essentially to abandon the effort to craft an international convention.¹⁶⁴

The *Zippo* formula, while incomplete, provided the key for the convergence on a set of principles generally followed now in hundreds of cases.¹⁶⁵ In them, the

COMMERCE AND INTERNATIONAL JURISDICTION (Catherine Kessedjian, ed., 2000), available at <http://www.hcch.net/upload/wop/jdgmpl12.pdf> [hereinafter OTTAWA REPORT].

¹⁵⁹ Ottawa Report, *supra* note 158, at 7.

¹⁶⁰ See generally Mary Shannon Martin, *Keep it Online: The Hague Convention and the Need for Online Alternative Dispute Resolution in International Business-to-Consumer E-Commerce*, 20 B.U. INT’L L.J. 125, 136–41 (2002) (discussing different views in relation to the convention).

¹⁶¹ See Ronald A. Brand, *Intellectual Property, Electronic Commerce and the Preliminary Draft Hague Jurisdiction and Judgments Convention*, 62 U. PITT. L. REV. 581, 594–97 (2001) (discussing intellectual property rights in the context of the Convention).

¹⁶² See *id.* at 597–98 (discussing concerns related to electronic commerce).

¹⁶³ In the *Yahoo!* case, a French court ordered Yahoo! to block access to materials on Nazism that violated French law. See *Yahoo! Inc. v. La Ligue Contre Le Racisme*, 433 F.3d 1199, 1202–03 (9th Cir. 2006) (en banc) (holding that the district court lacked personal jurisdiction; summarizing procedural history). Yahoo! unsuccessfully argued that “there was no technical solution which would enable it to *comply fully* with the terms of the court order.” *Id.* at 1203. The United States litigation was an attempt by Yahoo! to block enforcement of the French judgment in the United States.

¹⁶⁴ See Arthur T. von Mehren, *Drafting a Convention on International Jurisdiction and the Effects of Foreign Judgments Acceptable World-Wide: Can the Hague Conference Project Succeed?*, 49 AM. J. COMP. L. 191, 193 (2001) (discussing lack of consensus among participants).

¹⁶⁵ See, e.g., *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 714 (4th Cir. 2002) (adopting the *Zippo* model to find personal jurisdiction); *Mink v. AAAA Dev. LLC*, 190 F.3d 333, 336 (5th Cir. 1999) (using the reasoning of *Zippo* to find personal jurisdiction over the defendant); *Cybersell, Inc. v. Cybersell Inc.*, 130 F.3d 414, 419 (9th Cir. 1997) (adopting the *Zippo* formula).

Goldsmith view has largely prevailed: the customary requirement for “minimum contacts” and “fair play and substantial justice” have proved workable for the vast majority of Internet cases.¹⁶⁶ Pressure for new jurisdictional concepts or for an international treaty has largely evaporated.

Nevertheless, the focus on enforcing judgments against local assets puts pressure on immunity for intermediaries¹⁶⁷ because intermediaries usually have local assets and they represent deep pockets.

G. Electronic Commerce

1. In General

Realization of the Internet’s potential to transform private markets required the proliferation of e-commerce. E-commerce had existed since the 1960s through dedicated communication circuits and by means of Electronic Data Interchange (EDI) standards that permitted disparate proprietary computer systems to make sense of the data sent and received.¹⁶⁸ Electronic funds transfer, ATM machines, and point-of-sale credit card terminals were widely accepted by the end of the 1980s.¹⁶⁹ The spread of the Internet made an easy-to-use interface available in the form of web browsers, and simplified the processes of establishing computer-to-computer connections.

1995 was a pivotal year. Jeff Bezos launched Amazon.com,¹⁷⁰ and Dell and Cisco both began to use the Internet to interact directly with customers.¹⁷¹ By mid-2011, few types of consumer goods were *not* sold online. E-commerce flourished on

¹⁶⁶ See *CollegeSource, Inc. v. AcademyOne, Inc.*, 653 F.3d 1066 (9th Cir. 2011) (finding specific jurisdiction but not general jurisdiction in dispute between two Internet-based college course catalog providers). *Compare id.* at 1075 (finding Internet connections from California insufficient to meet demanding standard of “continuous and systematic” for general jurisdiction), *with id.* 1078–79 (concluding that specific jurisdiction was satisfied because defendant expressly aimed its downloading requests to California and the dispute related to those contacts).

¹⁶⁷ See *supra* notes 133–36 and accompanying text.

¹⁶⁸ See C.J. Anumba & K. Ruikar, *Electronic Commerce in Construction-Trends and Prospects*, 11 AUTOMATION CONSTRUCTION 265, 267 (2002) (noting the impact of EDI); Janine S. Hiller & Don Lloyd Cook, *From Clipper Ships to Clipper Chips: The Evolution of Payment Systems for Electronic Commerce*, 17 J.L. & COM. 53, 55 (1997) (noting that the evolution of the internet began in the 1960s).

¹⁶⁹ Anumba & Ruikar, *supra* note 168, at 268.

¹⁷⁰ Amazon enjoyed explosive growth. Sales revenue grew 838% from 1996 to 1997, and customer accounts grew 738% in the same period. Letter from Jeffrey P. Bezos, Founder and Chief Executive Officer, Amazon.com to Shareholders (1997), *available at* http://media.corporate-ir.net/media_files/irol/97/97664/reports/Shareholderletter97.pdf. The impact on perceptions of e-commerce was almost as dramatic. If so many people were willing to buy books through the web, they might be willing to buy other things.

¹⁷¹ See Press Release, Cisco, Cisco Systems Broadens Internet Access to the Desktop, Acquires Internet Junction, Inc. (Sept. 6, 1995), *available at* http://newsroom.cisco.com/dlls/1995/corp_090695.html.

the Internet despite early concerns about payment systems, lack of consumer trust, consumer reluctance to incur transaction costs of using the web, and reluctance of service or product suppliers to risk their intellectual property.¹⁷² Most of these concerns proved unwarranted. In the mid-1990s, many argued that e-commerce would require the development of entirely new payment systems.¹⁷³ I disagreed. In two law review articles written in the late 1990s,¹⁷⁴ I argued that the existing credit card systems would prove perfectly adequate and acceptable to consumers. By 2000, it was clear that this was the case,¹⁷⁵ largely because of the dispute resolution system built in to credit card transactions.¹⁷⁶

Concerns about inconvenience were mitigated by one-click shopping, popularized by Amazon, beginning in 1999.¹⁷⁷ The one-click method reduced the number of steps a consumer must take to order an item from an e-commerce site, and relieved a consumer from having to reenter all of his basic information, such as name, address, and credit card information.¹⁷⁸

On the other hand, the easy replication of information in digital form undermined traditional business models in some industries, particularly those for music and video entertainment. The result was a war over enforcement of copyright on the Internet, which still clouds the future of e-commerce.¹⁷⁹

¹⁷² See *infra* notes 173–75 and accompanying text.

¹⁷³ Compare Sarah Jane Hughes, *A Case for Regulating Cyberpayments*, 51 ADMIN. L. REV. 809, 813–14 (1999) (noting the demise of most cyberpayment systems as e-commerce developed), with Hiller & Cook, *supra* note 168, at 98 (“To the extent electronic commerce grows, it is certain that it will not flourish unless acceptable systems for payment are available.”), and Kerry Lynn Macintosh, *How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet*, 11 HARV. J.L. & TECH. 733, 738–39 (1998) (arguing that the Internet needs its own private electronic currencies), and Robert F. Stankey, *Internet Payment Systems: Legal Issues Facing Businesses, Consumers and Payment Service Providers*, 6 COMMLAW CONCEPTUS 11, 12 (1998) (arguing that the percentage of credit card transactions will decline as e-commerce grows).

¹⁷⁴ Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 RUTGERS COMPUTER & TECH. L.J. 1, 2 (1996); Henry H. Perritt, Jr., *Payment Infrastructures for Open Systems*, 3 DATA L. REP. 1, 20 (1995).

¹⁷⁵ Henry H. Perritt, Jr., *Dispute Resolution in Cyberspace: Demand for New Forms of ADR*, 15 OHIO ST. J. DISP. RESOL. 675, 676 (2000) (explaining why intermediary-provided dispute resolution, such as credit card charge-backs and escrow arrangements, prove more attractive in practice than independent third-party mechanisms such as arbitration or mediation).

¹⁷⁶ *Id.* at 690–94 (explaining credit card charge-back system).

¹⁷⁷ Ronald J. Mann & Travis Siebeneicher, *Just One Click: The Reality of Internet Retail Contracting*, 108 COLUM. L. REV. 984, 1002 (2008) (noting Amazon’s “renowned” one-click patent).

¹⁷⁸ *Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1348 (Fed. Cir. 2001). See generally *id.* at 1360–66 (suggesting Amazon’s patent for one-click ordering might be invalid).

¹⁷⁹ See *infra* notes 180–213 and accompanying text.

2. Copyright

Proliferation of personal computers set off alarm bells in the community of intellectual property rightsholders, particularly those whose business models depended on protecting copyright.¹⁸⁰ As the Internet became more popular, major organizations of rightsholders aggressively promoted copy protection schemes and launched aggressive litigation campaigns against perceived infringers.¹⁸¹

The ongoing controversy was shaped by the enactment of the DMCA, extension of the copyright term, imposition of liability on major unlicensed file sharing services, extension of secondary liability to intermediaries, and constriction of the fair use privilege.¹⁸²

a. DMCA

The DCMA¹⁸³ prohibits circumvention of technological measures that effectively control access to protected works¹⁸⁴ and the use of technologies that facilitate circumvention.¹⁸⁵ This encourages copy protection, which reduces user flexibility in working with copyrighted materials.¹⁸⁶

b. Extension of Copyright Term

In *Eldred v. Ashcroft*,¹⁸⁷ the Supreme Court rejected 7–2, a constitutional challenge to the Copyright Term Extension Act (CTEA),¹⁸⁸ which extended copyright

¹⁸⁰ In 1974, the National Commission on New Technological Uses of Copyrighted Works (CONTU) reported to Congress on the relationship of new technologies and the effectiveness of copyright law. See NAT'L COMM'N ON NEW TECH. USES OF COPYRIGHTED WORKS, FINAL REPORT OF THE NATIONAL COMMISSION ON NEW TECHNOLOGY USES OF COPYRIGHTED WORKS (1978), available at <http://digital-law-online.info/CONTU/contu18.html> [hereinafter CONTU Report]. Oddly, it limited its work to copyright protection for computer programs and the potential of photocopiers to undermine copyright. See Note, *Toward a Unified Theory of Copyright Infringement for an Advanced Technological Era*, 96 HARV. L. REV. 450, 451 & n.10 (1982) (noting technology's potential to undermine the ability of copyright owners to control distribution of their work and noting the limitation of CONTU).

¹⁸¹ See Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 VAND. J. ENT. & TECH. L. 695, 721–25 (2011) (describing Recording Industry Association of America litigation initiative resulting in more than 30,000 civil action claims).

¹⁸² See *infra* notes 183–213 and accompanying text.

¹⁸³ Pub. L. No. 105-304, 112 Stat. 2860 (1998).

¹⁸⁴ 17 U.S.C. § 1201(a) (2006).

¹⁸⁵ *Id.* § 1201(b).

¹⁸⁶ See Henry H. Perritt, Jr., *Flanking the DRM Maginot Line Against New Music Markets*, 16 MICH. ST. J. INT'L L. 113 (2007) (explaining and criticizing copy protection efforts).

¹⁸⁷ 537 U.S. 186 (2003).

¹⁸⁸ Pub. L. No. 105-298, 112 Stat. 2827–28 (1998) (amending 17 U.S.C. §§ 302, 304 (1994)).

protection from creation until seventy years after the author's death and extended the term for copyrights already existing at the time of enactment.¹⁸⁹ The extension reduces the portion of works in the public domain.¹⁹⁰

c. Secondary Liability

The Supreme Court extended liability for secondary infringement of copyright in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*,¹⁹¹ holding that the distributor of music file-sharing software could be secondarily liable for direct infringement by users of the software upon proof that the distributors clearly expressed intent that the software be used for infringing activities.¹⁹²

So far, lower courts have resisted attempts to expand secondary liability in other contexts. In *Viacom International Inc. v. YouTube, Inc.*, the plaintiffs asked the district court to hold YouTube liable for secondary infringement for failing to make it easier for rightsholders to cause infringing material posted by others to be removed from the YouTube site.¹⁹³ The court granted summary judgment to the defendants, holding that they satisfied the requirements of the DMCA safe harbor by insisting on identification of specific infringing items before taking steps to remove them and that they did not lose the safe harbor protection by failing to deploy more aggressive infringement monitoring software.¹⁹⁴

In *Perfect 10, Inc. v. Visa International Service Ass'n*, the court of appeals affirmed dismissal of an action brought against credit card processors for copyright infringement arising from their cardholders' downloading copyrighted images from third-party websites.¹⁹⁵ The court of appeals, agreeing with the district court, found that the credit card companies had no direct connection to that infringement.¹⁹⁶ Although credit cards made it easier for websites to profit from infringing activity, infringement could occur even without payment.¹⁹⁷ Perfect 10 did not allege "specific acts" by the credit card companies intended to encourage infringement.¹⁹⁸ Finally, even though the credit card processors could have stopped processing credit card payments to the infringing websites, that did not mean that failure to do so equated to vicarious infringement.¹⁹⁹ The court easily rejected a claim of contributory trademark

¹⁸⁹ *Id.*

¹⁹⁰ Dennis S. Karjala, *Judicial Review of Copyright Term Extension Legislation*, 36 LOY. L.A. L. REV. 199, 201 (2003).

¹⁹¹ 545 U.S. 913 (2005).

¹⁹² *Id.* at 928–41.

¹⁹³ 718 F. Supp. 2d 514, 516–19, 525–26 (S.D.N.Y. 2010).

¹⁹⁴ *Id.* at 528–29.

¹⁹⁵ 494 F.3d 788 (9th Cir. 2007).

¹⁹⁶ *Id.* at 796.

¹⁹⁷ *Id.* at 796–97.

¹⁹⁸ *Id.* at 802.

¹⁹⁹ *Id.* at 803.

infringement, finding that the credit card companies had no power to control the activities of the infringing sites.²⁰⁰

Potential secondary liability by intermediaries undercuts the immunity considered in Part II.E of this Article, and thus can lead to shutting out riskier forms of content from the Internet. The DMCA's safe harbor for intermediaries, analyzed in Part II.G.2, combined with the result in the *Viacom* case,²⁰¹ mitigates this risk.

d. Fair Use

By far the most important privilege within the Internet context is the fair use privilege, codified in Title 17, § 107.²⁰²

The Supreme Court noted in *Sony Corp. of America v. Universal City Studios, Inc.*²⁰³ and *Campbell v. Acuff-Rose Music, Inc.*²⁰⁴ that the last factor—the market effect of the purported fair use—is the most important.²⁰⁵ In recent years, the first factor—the purpose and character of the use—has gained in importance as “transformative” activities by accused infringers have been recognized as socially beneficial.²⁰⁶

Early cases involving the Internet took a restrictive view of fair use. In *UMG Recordings, Inc. v. MP3.com, Inc.*,²⁰⁷ the district court denied the fair use defense of an Internet web service that purchased tens of thousands of popular CDs and copied recordings onto its web servers so that subscribers could play the recordings from wherever they had Internet connections.²⁰⁸ In *Bowers v. Baystate Technologies*,

²⁰⁰ *Id.* at 807.

²⁰¹ *See supra* notes 193–94.

²⁰² 17 U.S.C. § 107 (2006). This section was intended to codify decisional law, rather than to expand or alter it. *See* *Quinto v. Legal Times of Wash., Inc.*, 506 F. Supp. 554, 560 (D.C. Cir. 1981); *Elsmere Music, Inc. v. NBC, Inc.* 482 F. Supp. 741, 745 n.8 (S.D.N.Y. 1980). Section 107 explains that whether a particular use of a copyrighted work is fair use, and thus non-infringing, is to be determined by consideration of a number of factors including:

- (1) the purpose and character of the use, including whether such use is of a commercial nature or as for non-profit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

§ 107 (1)–(4).

²⁰³ 464 U.S. 417 (1984).

²⁰⁴ 510 U.S. 569 (1994).

²⁰⁵ *Id.* at 574; *Sony*, 464 U.S. at 476 (Blackmun, J., dissenting).

²⁰⁶ *See* *Kelly v. Arriba Soft Corp.*, 280 F.3d 934, 940 (9th Cir. 2002) (finding the search engine presentation of thumbnail sketches of copyrighted photographs to be transformative).

²⁰⁷ 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000).

²⁰⁸ *Id.* at 350, 352.

Inc.,²⁰⁹ the Federal Circuit held that the Copyright Act did not preempt enforcement of a broad contractual prohibition on reverse engineering contained in a shrink-wrap agreement, even though the contract had the effect of prohibiting what would be fair use under the Copyright Act.²¹⁰

More recently, courts have breathed life back into fair use. In *Kelly v. Arriba Soft Corp.*,²¹¹ the Court of Appeals for the Ninth Circuit affirmed in part and reversed in part summary judgment in favor of search engine operators accused of copyright infringement for presenting “thumbnail” versions of copyrighted images on its search engine. The court stated that the uses were transformative due to the public benefit of the search engine and because use of the plaintiff’s images in the thumbnails did not harm the market for the plaintiff’s images or the value of his images.²¹² The plaintiff was denied fair use with respect to full-size reproductions of the photographs.²¹³

H. Security and Surveillance

The shift of information and communications to the Internet spawned concern from the law enforcement and intelligence communities that many of their traditional investigatory and intelligence-collection tools would become ineffective. The result has been the development of a variety of legal constraints and privileges related to electronic surveillance.

1. Wiretap Act and Stored Communications Act

Law enforcement authorities may compel access to communications and electronic messages and files by obtaining warrants and other orders under the provisions of the Wiretap Act and the Stored Communications Act (SCA),²¹⁴ or by obtaining a traditional search warrant under Rule 41 of the Federal Rules of Criminal Procedure.²¹⁵

²⁰⁹ 320 F.3d 1317 (Fed. Cir. 2003).

²¹⁰ *Id.* at 1317, 1324.

²¹¹ 280 F.3d 934.

²¹² *Id.* at 944.

²¹³ *Id.* at 948.

²¹⁴ 18 U.S.C. § 2516 (2006) (authorizing for interception of wire, oral, and electronic communications); *id.* § 2703 (noting stored communications); *see* *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432 (W.D. Tex. 1993) (assessing statutory damages against Secret Service for violating Stored Wire and Electronic Communications and Transactional Records Access Act).

²¹⁵ FED. R. CRIM. P. 41. Important differences exist between Rule 41 and Title III wiretap orders: a search warrant may be issued by a magistrate judge, but a wiretap warrant must be issued by an Article III judge; any federal law enforcement officer or attorney for the government may apply for a search warrant, but a wiretap warrant requires approval by designated high officials in the Justice Department; a search warrant may be issued upon a finding

The requirements for accessing stored electronic communications under the SCA are less demanding than the requirements for accessing live wire, oral, or electronic communications under the Wiretap Act or under Rule 41.²¹⁶ The procedures for intercepting stored communications and for accessing remote computing facilities are more flexible because the Fourth Amendment does not limit access to records kept by third parties.²¹⁷ The SCA addresses searches and seizures of three different types of stored communications: (a) contents of stored electronic communications that have been in electronic storage for 180 days or less; (b) contents of stored electronic communications that have been in electronic storage for more than 180 days; and (c) records, not involving content, concerning electronic communications.²¹⁸ Stored communications in storage for 180 days or less may be accessed pursuant to either federal or state warrants.²¹⁹ Information stored for more than 180 days may be accessed with a warrant, with notice to the subscriber or customer under an administrative, grand jury, or trial subpoena; or pursuant to a court order based on a governmental showing that the information sought is “relevant and material to an ongoing criminal investigation.”²²⁰

Transactional records concerning stored electronic communications may be accessed pursuant to a warrant, a court order such as that necessary for information stored in excess of 180 days, a formal written request relevant to a law enforcement investigation concerning telemarketing fraud, or an administrative subpoena authorized by federal or state statute.²²¹ The SCA immunizes e-mails stored on the servers of an e-mail service provider from civil subpoenas.²²²

Pen/Trap orders²²³ are used for obtaining stored data, such as Twitter screen names and subscriber information, the dates and times such screen names were used, IP addresses used, and information on payment methods.²²⁴

of probable cause but a wiretap warrant requires additional findings, including a finding that other investigative procedures are impracticable. *Compare id.*, with 18 U.S.C. §§ 2516, 2518.

²¹⁶ *See supra* note 214.

²¹⁷ U.S. CONST. amend. IV; *United States v. Miller*, 425 U.S. 435, 441–43 (1976).

²¹⁸ § 2703.

²¹⁹ *Id.* § 2703(a).

²²⁰ *Id.* § 2703(b)–(d); *see also* *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432, 432–33 (W.D. Tex. 1993) (awarding damages for violation of ECPA stored communications provisions but finding no Title I interception).

²²¹ § 2703(c).

²²² *See* *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 975–76 (C.D. Cal. 2010) (reviewing case law and holding that immunity extended to certain private Facebook postings).

²²³ §§ 3121–3127.

²²⁴ *See In re: § 2703(d) Order*, 787 F. Supp. 2d 430 (E.D. Va. 2011) (rejecting challenge to sealed SCA order compelling disclosure by Twitter). The court held that, because the government did not seek access to communications content, it need not meet the higher standards of content disclosure under the SCA. *Id.* at 434–35.

In *United States v. Warshak*,²²⁵ the court of appeals held that:

[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails “that are stored with, or sent or received through, a commercial ISP.” . . . The government may not compel a commercial ISP to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak’s emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.²²⁶

2. Carnivore

Carnivore (renamed DCS-1000 in 2001) was a controversial system used by the FBI to facilitate court-ordered intercepts of Internet communications and transactional data, including e-mail and web communications.²²⁷ The Carnivore controversy illustrates adaptation of traditional surveillance technologies and law to networked environments. Before Carnivore existed, an ISP was often unable to comply with an

²²⁵ 631 F.3d at 266 (6th Cir. 2010).

²²⁶ *Id.* at 288 (citations omitted). Although the government obtained access to about 27,000 e-mails without informing the subscriber, the court held that the evidence obtained from the e-mails could not be excluded from a criminal trial because the government relied in good faith on the SCA. *Id.*

²²⁷ For an extensive commentary on Carnivore, see Maricela Segura, Note, *Is Carnivore Devouring your Privacy?*, 75 S. CAL. L. REV. 231, 235–36 (2001), and Ted Bridis, *FBI Stops Using Carnivore Wiretap Software*, USATODAY.COM (Jan. 1, 2009, 2:29 AM), http://www.usatoday.com/tech/news/surveillance/2005-01-19-carnivore-obsolete_x.htm. Carnivore was originally modified sniffer software developed by the FBI and deployed on a Pentium III microcomputer. Jeff Tyson, *How Carnivore Worked*, HOWSTUFFWORKS.COM, <http://www.howstuffworks.com/carnivore3.htm>. When the Carnivore system was attached to a local area network segment by one-way tap, the FBI could execute a court order to eavesdrop on electronic communications. *Id.* Depending on the content of the order, Carnivore was set to intercept and record only those packets containing certain IP addresses, e-mail addresses, or text strings. *See id.*

The network interface card installed with the Carnivore software “saw” all of the packets traversing the particular network segment into which Carnivore was connected, but only those packets meeting the specified criteria were recorded for further processing. *Id.* The recorded packets were written as a file on a zip drive, along with a file containing the settings for the session that resulted in the creation of that data file. *Id.* *See generally* ILL. INST. OF TECH. RESEARCH INST., INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM: FINAL REPORT (2000), available at http://epic.org/privacy/carnivore/carniv_final.pdf [hereinafter CARNIVORE REPORT].

order because most widely available sniffer software intercepted *too* much. If an ISP turned over to the FBI more information than was authorized under a court order, the FBI might not be able to use any of the information as evidence in a subsequent prosecution. Getting too much information constitutes a failure to “minimize” the eavesdropping and often justifies suppression of all the information, not just that portion that exceeds the court order.

Accordingly, technical personnel at the FBI’s Quantico laboratory undertook to program limitations onto traditional sniffer functionality so that whenever an ISP was unable to supply only the information authorized by a court order, the FBI could itself deploy a system that would obtain only the authorized information.²²⁸

When word of the system’s existence leaked, much controversy erupted, leading to congressional hearings.²²⁹ Attorney General Janet Reno, after evaluating competing proposals, selected the Illinois Institute of Technology Research Institute (IITRI) to perform a review.²³⁰ I was the senior legal member of the review team, which issued its final report in December of 2000.²³¹ We concluded that,

[w]hen Carnivore is used in accordance with a Title III order, it provides investigators with no more information than is permitted by a given court order . . . [that] Carnivore reduces, but does not eliminate, risk of both intentional and unintentional unauthorized acquisition of electronic communication information by FBI personnel, but introduces little additional risk of acquisition by persons other than FBI personnel.²³²

The report made a number of specific technical recommendations to prevent errors in setting up Carnivore in a particular deployment and to improve audit trails.²³³

3. CALEA

The Communications Assistance for Law Enforcement Act (CALEA)²³⁴ obligates telecommunication service providers to design their networks to facilitate eavesdropping by law enforcement authorities. All of CALEA’s required capabilities are expressly premised on the condition that any information will be obtained “pursuant to a court order or other lawful authorization.”²³⁵ The FCC may not, under

²²⁸ CARNIVORE REPORT, *supra* note 227, at 1.

²²⁹ *Id.* at 3.

²³⁰ *Id.* at 2.

²³¹ *Id.*

²³² *Id.* at xii.

²³³ *Id.* at xiv–xv.

²³⁴ 47 U.S.C. §§ 1001–1010 (2006).

²³⁵ U.S. Telecom Ass’n v. FCC, 227 F.3d 450, 465 (D.C. Cir. 2000) (citing 47 U.S.C. § 1002(a)(1)–(2)).

CALEA, “require carriers to provide the government with information that ‘is not authorized to be intercepted.’”²³⁶ CALEA applies to “telecommunications carriers,” but not to “information services.”²³⁷ Drawing the line between the two has engendered much controversy.

In *U.S. Telecom Ass’n v. FCC*, the Court of Appeals for the D.C. Circuit set aside certain parts of the FCC’s CALEA rules.²³⁸ The court approved the FCC’s interpretation of call-identifying information, available under CALEA, to include antenna tower location for cell phone calls.²³⁹ The court embraced the FCC’s reasoning that antenna tower information simply puts law enforcement agencies in the same position they had in monitoring plain old telephone service, where the telephone number provides location information.²⁴⁰ The court also approved the requirement to make packet-mode data available.²⁴¹

The litigation was a precursor to several controversies involved in *Carnivore*: the argument about *Smith v. Maryland*’s²⁴² distinction between content and dialed digits, the argument over interception of new data, such as antenna location, to make up for the absence of location information implicit with wire line wiretaps, and the challenge of separating header and payload data from packet-based communications—an issue strongly influencing some criticisms of *Carnivore* for over-collecting in pen mode.

In 2005, the FCC extended CALEA to Voice over Internet Protocol (VoIP) and to broadband access providers,²⁴³ a decision approved in *American Council on Education v. FCC*.²⁴⁴ The FCC rejected the government’s proposal that new technologies receive advance approval, finding that implementing the “proposal would have a chilling effect on innovation.”²⁴⁵

4. Mobile Device Location Information

District courts and courts of appeals disagree about whether “prospective cell site” data—information showing the location of a cell phone user—is available under

²³⁶ *Id.* at 465–66.

²³⁷ *Am. Council on Educ. v. FCC*, 451 F.3d 226, 228 (D.C. Cir. 2006) (citing 17 U.S.C. § 1002(a)).

²³⁸ *U.S. Telecom*, 227 F.3d at 450, 453.

²³⁹ *Id.* at 463.

²⁴⁰ *Id.* 463–64.

²⁴¹ *Id.* at 464–65.

²⁴² 442 U.S. 735 (1979).

²⁴³ Communications Assistance for Law Enforcement Act and Broadband Access and Services, 20 FCC Rcd. 14989 (2005).

²⁴⁴ 451 F.3d 226 (explaining requirements of CALEA, 47 U.S.C. §§ 1001–1010, to make certain telecommunications networks available for electronic eavesdropping by law enforcement agencies).

²⁴⁵ Communications Assistance for Law Enforcement Act and Broadband Access and Services, 21 FCC Rcd. 5360, 5395–96 (2006).

the Wiretap Act, the SCA, the Pen/Trap Act, or a combination of them, or whether probable cause must be shown.

In *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*,²⁴⁶ the court of appeals held that the magistrate judge “erred in allowing her impressions of the general expectation of privacy of citizens to transform that standard into anything else. . . . [t]h[e] standard is a lesser one than probable cause”²⁴⁷ Whether the probable cause or subsection (d) requirement applies may depend on the length of time for which historical cell site information (CSI) is sought.²⁴⁸ A magistrate judge in another circuit relied in part on the Third Circuit’s analysis to exercise his discretion to require probable cause for access to historical CSI for a period of 113 days.²⁴⁹

In *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*,²⁵⁰ the district court rejected access to prospective cell site location data under the wiretap statute (or under the Pen/Trap or SCA) because “[c]ell site data does not reflect the ‘contents’ of a communication.”²⁵¹ It also denied access to the data under the SCA subscriber records category.²⁵² In *In re Application of United States for an Order Authorizing the Installation and Use of a Pen Register Device, A Trap and Trace Device, and for Geographic Location Information*,²⁵³ reviewing the other district court decisions to date,²⁵⁴ the district court concluded that the only authority for prospective cell site information was Rule 41, necessitating a finding of probable cause.²⁵⁵ Other cases reach conflicting results.²⁵⁶

²⁴⁶ 620 F.3d 304 (3d Cir. 2010).

²⁴⁷ *Id.* at 313.

²⁴⁸ See *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, No. 11-MC-0113 (JO), 2011 WL 679925, at *1–2 (E.D.N.Y. Feb. 16, 2011) (granting order under subsection (d) and distinguishing historical data for longer period, for which probable cause is necessary); see also 18 U.S.C. § 2703(d) (2006).

²⁴⁹ *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, No. 10-MC-0897, 2010 WL 5437209, at *1–2 (E.D.N.Y. Dec. 23, 2010).

²⁵⁰ 396 F. Supp. 2d 747 (S.D. Tex. 2005).

²⁵¹ *Id.* at 758.

²⁵² *Id.* (referring to SCA subscriber records category under 18 U.S.C. § 2703(c)).

²⁵³ 497 F. Supp. 2d 301 (D.P.R. 2007).

²⁵⁴ *Id.* at 303–04.

²⁵⁵ *Id.* at 311.

²⁵⁶ Compare *In re Application of the U. S. for an Order*, 441 F. Supp. 2d 816, 826–36 (S.D. Tex. 2006) (rejecting the government’s hybrid theory), and *In re Application of the U.S. for an Order*, 415 F. Supp. 2d 211, 212 (W.D.N.Y. 2006) (finding that a judicial officer should not be able to extrapolate from separate and independent statutory provisions authority to obtain “real time” cell location data on anything less than a showing of probable cause), and *In re Application of the U.S. for an Order*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005) (finding that combination of CALEA and the Wiretap Act without probable cause did not authorize government to obtain location information by means of pen/trap order), and *In re Application of the U.S. for an Order*, 412 F. Supp. 2d 947 (E.D. Wis. 2006) (rejecting access to cell site location data, reasoning that the three statutes—the SCA, the CALEA, and the

Continued confusion over this issue is likely to result in more intrusive government surveillance based on mobile Internet technologies. If Congress intervenes, it is not certain whether it will act to protect personal privacy or to facilitate what law enforcement and intelligence communities say is necessary.

II. CONFRONTING THREATS TO THE FUTURE

The Internet has established itself as one of the dominant means for political communication, one of the principal channels for commerce, and is becoming the most important distribution mechanism for art and entertainment.²⁵⁷ As these trends continue, certain legal and policy issues will intensify.

During its first two decades, the Internet encountered a variety of actual or perceived threats to its continued growth and to its fundamental architectural characteristics. As the following sections of this Article show, some of the apparent threats turned out not to be real, and a combination of entrepreneurial and legal creativity accommodated others. The future also contains potential threats. Some will not materialize, while others may undermine the Internet's constitution, diverting politics, social interaction, commerce, and art into other infrastructures, leaving the Internet as a historical shooting star. Still others might fundamentally crush the grassroots energy on both consumer and supplier sides that have made the Internet a success.

The most important of the threats are the replacement of the Internet's decentralized character with an oligopolistic cluster of proprietary empires, the loss of net neutrality and discrimination against content in other forms, the eclipse of the public domain by holders of copyright monopolies, chilling of behaviorally targeted advertising, and overreaction to perceived security threats.²⁵⁸

A. Proprietary Empires

Proprietary empires have already emerged amid the Internet's success: Google for searches, Amazon for e-commerce, iTunes for music, and Netflix and Hulu for video entertainment. So far, their imperial policies have been benign, even in the

Pen/Trap Statute—did not authorize the requested eavesdropping), *and In re* Application of the U.S. for an Order, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (finding certification of relevance under Pen/Trap statute insufficient and that probable cause was required), *and In re* Application for an Order, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (classifying prospective cell site data as tracking device information under 18 U.S.C. § 3117 and not as minimal Pen/Trap information, rejecting government's hybrid statutory argument, and stating access without showing a probable cause would raise serious Fourth Amendment concerns), *with In re* Application of the U.S. for an Order, 411 F. Supp. 2d 678, 682–83 (W.D. La. 2006) (granting request for cell site location data under the same argument based on the three statutes).

²⁵⁷ See Shikar Ghosh, *Making Sense of the Internet*, HARV. BUS. REV., Mar.–Apr. 1998, at 126, 126–27.

²⁵⁸ See, e.g., *Values and Principles*, INTERNETSOCIETY.ORG, <http://www.internetsociety.org/node/21> (last visited May 1, 2012).

case of Amazon, in facilitating market access by small entrepreneurs.²⁵⁹ Imperial policies could change, however. If they do, the possibility of regulating through technology is far more threatening to the Internet's constitution than traditional governmental regulation backed up by legal institutions.²⁶⁰

The Internet is defined by its open architecture, as explained in Part I.B, but economic incentives exist to close the architecture. Most suppliers of services through the Internet have an incentive to allow it to function as intended—freely granting access to their own services to other suppliers performing complementary services.²⁶¹ Circumstances also exist, however, in which supplier self-interest is served by blocking access. These typically involve a monopoly position by the one denying access.

Monopolies may arise for several reasons. For example, a supplier may have proprietary interconnection technologies protected by intellectual property law offering features that distinguish it from competitors. In such circumstances, suppliers of complementary products may be willing to pay higher-than-market rates for access, so they can incorporate the proprietary features in the integrated offering to consumers. They expect to earn more than enough revenue from the integrated product to cover the supernormal fees paid to the owner of the proprietary features. The owner of the proprietary features makes a rational economic decision as to whether its profits will be larger if it charges a competitive access fee and has a larger customer base, or if it charges a higher fee²⁶² resulting in a smaller customer base. Apple provides an example of this phenomenon, resulting at different times in the adoption of competing philosophies. At some points, and for some products, Apple maintains a “closed system”: no independent supplier of complementary products and services is allowed to interconnect them with Apple's proprietary features unless it enters into a contract and pays what are presumably supernormal fees to Apple.²⁶³ Other times, as with iPhone applications, Apple has adopted an open approach in which it provides the necessary interface specifications and privileges to the world, allowing entrepreneurs to develop their applications as they wish.²⁶⁴ Thousands of Apps were

²⁵⁹ Jill Priluck, *Ahead in the Cloud*, SLATE (Nov. 24, 2010, 12:43 PM), http://www.slate.com/articles/business/small_business/2010/11/ahead_in_the_cloud.html.

²⁶⁰ See LAWRENCE LESSIG, *CODE: VERSION 2.0*, at 81–82 (2006) (explaining how regulation by technological restrictions is more subversive of liberty than traditional legal regulation by the state).

²⁶¹ See Complaint at 15–17, *United States v. WorldCom, Inc.*, No. 00-2789 (D.D.C. June 27, 2001) (describing incentives for networks confronted with network externalities to interconnect).

²⁶² Economists would call this “monopoly rents.” See generally Anne O. Krueger, *The Political Economy of the Rent-Seeking Society*, 64 AM. ECON. REV. 291 (1974).

²⁶³ See Rui Li, Note, *Antitrust, Intellectual Property Rights, and the Online Music Industry: An Antitrust Analysis of Apple's Combination of Services and Products*, NAT'L L. REV. 1–2, 5 (2011), available at <http://www.natlawreview.com/article/antitrust-intellectual-property-rights-and-online-music-industry-antitrust-analysis-apple-s->.

²⁶⁴ See Charles M. Davidson & Michael J. Santorelli, *Seizing the Moment: Spectrum Allocation Policy for the Wireless Broadband Century*, 19 COMM'LAW CONSP'CTUS 1, 13–14 (2010). But see *id.* at 42.

available for the iPhone in early 2010.²⁶⁵ Millions of iPhone users enthusiastically downloaded these Apps, resulting in higher profits for Apple because of the sale of more iPhones, as well as higher profits for AT&T and other iPhone service providers because consumers using Apps use more bandwidth for which they pay the service providers.²⁶⁶

The iPhone's open architecture²⁶⁷ for applications did not result from any intervention by the legal system. No court, legislature, or administrative agency told Apple that it was forbidden from closing the iPhone interfaces. Rather, it occurred because Apple made an independent, self-interested economic judgment that an open architecture would produce higher profits. The experience of the Internet and e-commerce strongly reinforces the attractiveness of such an open approach. Occasionally—especially in the early days of e-commerce²⁶⁸—offerors of websites, such as directories and indexes, embrace the business model in which specific vendors would be included only if they paid a fee. In almost all cases these business models have been unsuccessful and are abandoned.²⁶⁹ Directories and indexes proliferate. Almost none charge a fee for inclusion.²⁷⁰ The motivation for the business model is premised on using free inclusion to fuel demand for other services for which a fee is charged or by noneconomic motives.

Situations exist and are likely to recur, however, when suppliers are antagonistic to this open architecture philosophy. Some of them have established businesses, the outputs of which are being drawn into the Internet's information infrastructure, and the owners and operators of these businesses are unable to develop a business model in which these outputs can be offered for free while still sustaining the enterprise.²⁷¹ Major record labels, film studios, and other owners of rights in entertainment content are clear examples. In other cases, economic misfortune has confronted established enterprises for reasons not directly associated with exploitation of their outputs

²⁶⁵ *Id.* at 13–14; Matt Silverman, *iPhone Apps List 2010: 700+ Apps Reviewed by Category*, MASHABLE TECH (Jan. 3, 2010), <http://mashable.com/2010/01/03/iphone-apps-2010/>.

²⁶⁶ See Mike Bremin, *Can't We Enjoy Anything Without Paying for It??*, TECHMENTO (Mar. 19, 2011), http://techmento.com/2011/03/19/att_tethering_devices_payup/.

²⁶⁷ *Definition of: Open Architecture*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=open+architecture&i=48446,00.asp (last visited May 1, 2012).

²⁶⁸ In this context, “e-commerce” simply means developing and deploying Internet services with a profit motive.

²⁶⁹ See, e.g., Barry Schwartz, *Yahoo To Drop Paid Inclusion Program*, SEARCH ENGINE LAND (Oct. 15, 2009, 4:20 PM), <http://searchengineland.com/yahoo-to-drop-paid-inclusion-program-27852>.

²⁷⁰ Barry Schwartz, *Confirmed: Bing Tests Ads Within Organic Search Results*, SEARCH ENGINE LAND (July 22, 2011, 4:49 PM), <http://searchengineland.com/bing-tests-ads-within-organic-search-results-86957>.

²⁷¹ See Danny Sullivan, *2000 In Review: AdWords Launches; Yahoo Partners with Google; GoTo Syndicates*, SEARCH ENGINE LAND (Feb. 1, 2010, 9:00 AM), <http://searchengineland.com/2000-in-review-adwords-launches-yahoo-partners-with-google-34831>.

to the Internet.²⁷² The owners and operators of these businesses are scrambling to find substantive revenue streams, which causes them to look greedily at the possibility of generating revenue by charging for access to their outputs through the Internet. The newspaper and magazine industries at the end of 2009 provide clear examples.²⁷³

In most cases, the law does not need to get involved. The marketplace will decide whether closed approaches are viable, force suppliers to embrace the open architecture, or risk being driven from the market. In many instances, fee-based services survive and flourish; for example, thousands of lawyers pay substantial fees for accessing court decisions and statutes offered through the Internet by Westlaw and Lexis, millions of music fans pay iTunes ninety-nine cents per song or more to download music, and travelers expect to pay fees for airline tickets and hotel rooms through the Internet. No serious analyst proposes that the law must intervene to force these services to be made available for free.

Other circumstances exist, though, posing a danger to the well-being of economic life or to the viability of the Internet's core philosophy, which present stronger cases for legal intervention.²⁷⁴ The dynamics of a monopoly typically lead to three

²⁷² See *Reinventing the Newspaper*, ECONOMIST, July 9, 2011, at 7–9 (discussing problems facing news organizations).

²⁷³ See David Milstead, *Newspapers' Perilous Paywall Moment*, EDITOR & PUBLISHER, Aug. 2010, at 30–35.

²⁷⁴ Microeconomic theory teaches that monopolists can and will charge a higher price for the same good or service that would be priced lower in a competitive market. In a competitive market, assuming that all firms have the same cost curve, any firm has an incentive to sell at a price high enough for it to earn revenue even slightly in excess of cost. No firm can charge a price higher than another firm because that would shift demand from the firm charging the higher price to firms with a lower price. That means that the price for every firm in the market is the price at which the marginal revenue curve crosses the marginal cost curve. At a lower price, firms would lose money because their revenue would not cover their costs; at a higher price, profits would be higher but other firms could gain market share by charging a price that just covers cost.

The position of a monopolist is different because, by definition, it does not face the competitive threat of any other firm offering a lower price. Having the flexibility to set its price wherever it wants, the monopolist sets its price to maximize profits. Under the usual assumptions of elastic demand (elastic demand means that consumers buy less at a higher price and more at a lower price), the monopolist sets a higher price resulting in lower demand, where the revenue gains are sufficient to offset the reduced demand. Because consumers have to pay a higher price and consume less they are worse off. The difference between the benefit to the monopolist and the loss to consumers is called the “net welfare loss.”

Monopolies are unstable in markets that have a competitive structure. A monopolist may exist, for example, if the monopolist was an innovator and entered the market with a product as to which it was the only offeror, but the competitive market conditions mean that others will enter charging prices less than the monopoly price and take market share away from the original monopolist. So a monopoly can be maintained only under one or both of two conditions: (1) the monopolist imposes artificial barriers to entry and is able to enforce them, or (2) the size of the market is such that at a monopoly price, the monopolist (but not new

elements of public policy. The first, deeply embedded in the rationale for public utility regulation, is that price controls should be imposed on monopolists who enjoy natural monopolies.²⁷⁵ By limiting monopoly pricing, the state can protect against reallocating resources from consumers to monopolists.

Second, the law can remove artificial barriers to entry. One such barrier to entry is “predatory pricing” by the monopolist. Predatory pricing signifies that a monopolist, threatened by the prospect of a new entrant, will reduce prices in the short run to a level below that at which the new entrant can earn a profit.²⁷⁶ A monopolist can afford to do this, either because it can forego some of its monopoly profits in the short run in order to retain its monopoly in the long run, or because it has banked enough excess monopoly profits in the past to allow it to finance a short-term loss as a good investment to increase prices later and reinstate its monopoly profits. Antitrust law developed a complex set of rules to determine when predatory pricing exists and when it should be illegal.²⁷⁷

Third, the law can protect against denials of access to essential facilities and services by the monopolist.²⁷⁸ That, essentially, is what the debate over net neutrality is all about.²⁷⁹

The greatest threat to enhanced social welfare resulting from the Internet’s open architecture arises when a supplier of services at one layer seeks to extend its services into other layers—in other words, to engage in vertical integration. Pursuit of this strategy benefits from discouraging competing suppliers in the layers where the vertically integrating enterprise has weaker competitive offerings. This situation often arises when the market structure of one layer is a natural monopoly, because of

entrants) faces a declining cost-curve. The declining cost-curve case is called a “natural monopoly.” In such conditions, if demand increases at the monopoly price, the monopolist simply can produce more and, because its costs decline, still earn higher profits.

However, one of the central assumptions of microeconomic theory is that, at some point, costs increase with increasing production. Increased shifts must be added at higher labor costs, the price for raw materials increases, or congestion or other inefficiencies begin to increase costs per unit. When a natural monopoly exists because at the initial level of demand a monopolist faces a declining cost curve, the monopolist still confronts the threat that demand will increase to the point that its costs will increase if it produces more. At that point, there is room for new entrants because they probably can serve the increased demand at lower costs than the monopolist. *See generally* WILLIAM J. BAUMOL & ALAN S. BLINDER, *ECONOMICS: PRINCIPLES AND POLICY* (7th ed. 1997).

²⁷⁵ *See* Charles W. Lamden, *The Place of Accounting in Price Control*, 18 ACCT. REV., Jan. 1943, at 26, 26–27.

²⁷⁶ *See* Brocke Grp. Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 221–28 (1993).

²⁷⁷ *See, e.g.*, The Sherman Act, 15 U.S.C. § 2 (2006).

²⁷⁸ *See* PERRITT, *supra* note 73, § 2.04[B] (2011 supp.) (discussing “essential facilities doctrine” in antitrust law).

²⁷⁹ *See infra* Part II.B.

network effects or otherwise, while the market structure of adjacent layers is inherently competitive.²⁸⁰

The vice when natural monopolies at one level are leveraged to create an artificial monopoly at other levels is not the natural monopoly. By definition, a natural monopoly is more efficient when it is allowed to run its course—at least until the monopolist starts extracting monopoly rents.²⁸¹ Instead, the vice is the artificial exclusion of competition in adjacent layers where competition is the natural state.

Many parts of the Internet's technologies present economies of scale. When economies of scale exist, bigger is better—or at least more efficient—even though the economies may not be strong enough to present network effects leading to natural monopoly. It may simply be that the capital cost of a cell phone site is so great that no one can make money unless he has hundreds of thousands of customers to support that site. Or, it may not be profitable to deploy DSL or fiber to the curb in a market for telephone services unless a sufficient subscriber base exists to provide a return on the substantial investment. Network effects also operate with respect to any one-stop shopping facility, such as iTunes, Amazon, or Netflix.

In these circumstances, the owner of the capital-intensive resource—or a potential investor in a new such resource—has an incentive to exclude people who do not pay. It has a concomitant incentive not to allow its competitors to get a free ride on its investment to offer competing services at prices lower than the owner must charge to recoup its investment. It is this set of circumstances that gives rise to the most ferocious legal battles over how the Internet should be regulated—the battle over competitive access to telephone infrastructure and, more recently, the battle over net neutrality.²⁸²

Three basic kinds of access denials occur. The first two are vertical, the third is horizontal. In one type of vertical denial of access, a firm with substantial market share refuses to deal with an upstream supplier because it already has arrangements with a preferred upstream supplier. An example might be a refusal by AT&T to sell cell phones made by someone other than Apple. In another type of vertical denial of access, a firm with substantial market share refuses to sell to customers competing with preferred customers. One example is a manufacturer that refuses to sell its product to discount retailers. Another is Apple's refusal to sell iPhones that work on any network other than AT&T's. In the horizontal context, a firm with substantial market

²⁸⁰ Wilko Bolt & David B. Humphrey, *Public Good Issues in Target: Natural Monopoly, Scale Economies, Network Effects and Cost Allocation* 6–7 (European Cent. Bank, Working Paper No. 505, 2005), available at http://ssrn.com/abstract_id=750785.

²⁸¹ See generally *United States v. Microsoft Corp.*, 253 F.3d 34, 50 (D.C. Cir. 2001) (expressing doubt whether traditional antitrust monopolization doctrines are appropriate “in technologically dynamic markets characterized by network effects”).

²⁸² Zack Christenson, *Some Think It Is OK for the Government to Do What Net Neutrality Would Prevent Others from Doing*, AM. CONSUMER INST. (Mar. 1, 2011), <http://www.theamericanconsumer.org/2011/03/01/cfa>.

share refuses to cooperate; for example, by interconnecting with a competitor—usually a new entrant that threatens to take away market share.

Concern is growing that concentration in the telecommunications market may eviscerate the Internet's potential to provide an infrastructure in which competition can flourish. The FCC has generally allowed concentration to increase through major telephone firm mergers, arguing that new technologies and intermodal competition will preserve competitor opportunities and consumer choices. The FCC approved two major mergers of local exchange carrier networks with long-distance networks: the merger of Verizon and MCI,²⁸³ and the merger of SBC and AT&T.²⁸⁴ In March 2007, a district court approved the consent decrees recommended by the Justice Department in the SBC/AT&T and Verizon/MCI mergers.²⁸⁵

Concentration in the cable industry, like concentration in the telephone industry, is intensifying. In July 2006, the FCC approved transfer of Adelphia Communications Corporation's assets to Time Warner and Comcast.²⁸⁶ The FCC accepted the argument that the consolidation might result in reduced competition in the market for programming, and adopted a condition that would allow programmers seeking to use commercial leased access to submit disputes about the terms of access to commercial arbitration.²⁸⁷ It also found that the possibility of uniform price increases could reduce competition.²⁸⁸ The FCC further adopted commercial arbitration as a condition to mitigate that risk²⁸⁹ and imposed detailed provisions for any arbitration proceedings in an appendix to its decision.²⁹⁰

Empires are emerging that control backbone connectivity, but that is not all. Empires are also developing with respect to content distribution. Whether these empires pose threats to the Internet's constitution depends on imperial business policies. One can speculate on adverse directions for evolution. For example, Google dominates the market for Internet search and for search-related advertising. Its e-mail service, Gmail, represents a rapidly growing share of the market.²⁹¹ Its Android software for smart phones has displaced Apple's dominance of this market.²⁹² Google has also entered the hardware market. It has launched Google+, a social networking

²⁸³ *In re Verizon Commc'ns Inc. and MCI, Inc.*, 20 FCC Rcd. 18433 (2005).

²⁸⁴ *In re SBC Commc'ns Inc. and AT&T Corp.*, 20 FCC Rcd. 18290 (2005).

²⁸⁵ *United States v. SBC Commc'ns, Inc.*, 489 F. Supp. 2d 1, 3 (D.D.C. 2007).

²⁸⁶ *In re Adelphia Commc'n Corp.*, 21 FCC Rcd. 8203, 8332 (2006).

²⁸⁷ *Id.* at 8253–54.

²⁸⁸ *Id.* at 8273.

²⁸⁹ *Id.* at 8274.

²⁹⁰ *Id.* app. B.

²⁹¹ Erick Schonfeld, *Gmail Grew 43 Percent Last Year. AOL Mail and Hotmail Need to Start Worrying*, TECHCRUNCH (Jan. 14, 2009), <http://techcrunch.com/2009/01/14/gmail-grew-43-percent-last-year-aol-mail-and-hotmail-need-to-start-worrying/>.

²⁹² Jay Yarow, *Android Blows Past Apple to Take the Lead in Market Share for App Downloads*, BUSINESS INSIDER (Oct. 24, 2011), http://articles.businessinsider.com/2011-10-24/tech/30315528_1_android-apps-ios-smartphone.

service aimed at Facebook's market.²⁹³ Suppose Google makes a business decision to discourage competition in these markets. It could make it difficult for users of Android software to connect to e-mail services other than Gmail. It could provide display and search-order preferences to advertisers who book advertising directly with Google rather than with competing ad agencies. It could make it easy for Google+ members to find new friends through their Gmail accounts, while making it more difficult for Facebook members to do the same. The result would be a market structure in which Internet users obtain a larger and larger portion of their cyberspace resources through Google rather than its competitors.

As another example, take Amazon. It is the largest e-commerce vendor.²⁹⁴ To date, Amazon has been aggressive in opening up access to competing suppliers of books and entertainment products and merchandise.²⁹⁵ When one searches for a particular type of merchandise, Amazon routinely provides links to several suppliers, including itself.²⁹⁶ It makes it easy to download Kindle books to other display devices. It facilitates access to small, independent authors and publishers of conventional books and their e-book counterparts. But suppose Amazon changed its business model. It could make it more difficult for consumers to find competitive sellers of books, video, audio entertainment or the immense variety of other goods that Amazon sells. It could eliminate the possibility of downloading Kindle books to devices other than the Kindle itself. Similar possibilities exist for the handful of large ISPs such as AT&T, Verizon, and Comcast to violate net neutrality, as considered in Part II.B.

Proprietary empires also enlarge risks of political discrimination beyond the reach of the rule of law.²⁹⁷ If the development of cloud computing induces a significant fraction of individual and institutional users to use the cloud to store their documents and other electronic assets, this will have three major effects: (1) it will increase the vulnerability of Internet users to attacks on major repositories of data, (2) it will make it easier for empires to gain new territory and make it more costly for users to

²⁹³ See Susan Mayes Ostrander, *Google Plus vs. Facebook: Who's Winning?*, HUFFINGTON POST (Nov. 20, 2011), http://www.huffingtonpost.com/2011/09/20/google-vs-facebook_n_972080.html.

²⁹⁴ See Erick Schonfeld, *How Amazon Controls Ecommerce (Slides)*, TECHCRUNCH (May 11, 2011), <http://techcrunch.com/2011/05/11/how-amazon-controls-ecommerce-slides/> (estimating Amazon controls one-third of e-commerce).

²⁹⁵ See Pascal-Emmanuel Gobry, *Suddenly, Amazon Starts Competing with Its Biggest Suppliers*, BUSINESS INSIDER (May 30, 2011), http://articles.businessinsider.com/2011-05-11/tech/30022890_1_amazon-s-kindle-amazon-publishers.

²⁹⁶ See AMAZON, <http://www.amazon.com> (last visited May 1, 2012).

²⁹⁷ See generally Henry H. Perritt, Jr., *Cyberspace Self-Government: Town-Hall Democracy or Rediscovered Royalism?*, 12 BERKELEY TECH. L.J. 413 (1997) (discussing the relationship between the Internet and regulation); Henry H. Perritt, Jr., *Towards a Hybrid Regulatory Scheme for the Internet*, 2001 U. CHI. LEGAL F. 215 (2001) (discussing private and public, or "hybrid regulation").

move from one empire to another,²⁹⁸ and (3) it will make it easier for governments and private institutions to eavesdrop on individual Internet activity. No longer will an eavesdropper have to gain access to data stored on a particular, individually owned device; all that will be necessary is to gain access to a particular empire in the cloud.²⁹⁹ It may make it easier to censor unpopular content.³⁰⁰

B. Discrimination and Net Neutrality

The rise of proprietary empires in the Internet—more concretely, consolidation in the telephone and cable industries—is fueling debate in Congress and before the FCC on “net neutrality”: the fear that providers of basic infrastructure will design or program their facilities to give preferential treatment to certain suppliers or customers.³⁰¹

The growth of major bottlenecks in the Internet, represented by large ISPs and connection services such as AT&T and CompuServe present the threat of censorship.³⁰² ISPs are under pressure to block services likely to facilitate access to content infringing copyright³⁰³ and to expel infringing users,³⁰⁴ YouTube is threatened with liability for not being more active in detecting and removing allegedly infringing video posts,³⁰⁵ and Craigslist is being pressured to remove its “adult services” section.³⁰⁶

These developments not only threaten the fundamental architecture of the Internet, making the establishment of empires more likely, as considered in Part II.A,

²⁹⁸ See generally Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761 (2011) (arguing that the FCC should alter its philosophy based on the separation between telecommunications and computing and assure access to cloud computing utilities); *id.* at 1819 (arguing that “utility regulation should be the starting point for public policy discussions” of cloud computing).

²⁹⁹ *Id.* at 1819–20 (discussing the need for restrictions on government access to content stored in the cloud).

³⁰⁰ *Id.* at 1820–21 (discussing danger of censorship imposed through the cloud).

³⁰¹ See Josh Peterson, *FCC Net Neutrality Rules Take Effect, Experts Doubt Longevity*, DAILY CALLER (Nov. 21, 2011), <http://dailycaller.com/2011/11/21/fcc-net-neutrality-rules-take-effect-experts-doubt-longevity/>.

³⁰² See generally Dawn C. Nunziato, *The First Amendment Issue of Our Time*, 29 YALE L. & POL’Y REV. INTER ALIA 1 (2010) (assessing the net neutrality debate in the context of political speech that might be suppressed by ISPs).

³⁰³ See Fred von Lohmann, *FCC Rules Against Comcast for BitTorrent Blocking*, ELECTRONIC FRONTIER FOUND. (Aug. 3, 2008), <http://www.eff.org/deeplinks/2008/08/fcc-rules-against-comcast-bit-torrent-blocking> (describing Comcast’s blocking of BitTorrent traffic and FCC reaction).

³⁰⁴ See David Kravets, *Top Internet Providers Cool to RIAA 3-Strikes Plan*, WIRED (Jan. 5, 2009), <http://www.wired.com/threatlevel/2009/01/draft-verizon-o/>.

³⁰⁵ See *supra* Part I.E.2.c (discussing the *Viacom* case).

³⁰⁶ See Thad D., *The Ultimate Showdown: Blumenthal v. Craigslist*, YALE L. & TECH. (Sept. 16, 2010), <http://www.yalelawtech.org/net-neutrality/the-ultimate-showdown-blumenthal-v-craigslist/> (discussing dangers to free speech of efforts by state attorneys general to get Craigslist to remove the “Adult Services” section).

but they also increase the possibility of pressure to discriminate against particular groups or points of view, such as gay rights advocates or Muslims.

The debate on net neutrality implicates technological, economic, and regulatory issues. The technological concern arises from the way Internet routers work. A router is a specialized computer that knows how to read the headers of Internet packets and to handle the packets according to the Internet address of the destination and the Internet address of the origin. A router accepts a flow of Internet packets at its input port—a wire pair, coaxial cable, or optical fiber, any of which might be connected to a wireless channel—strips off the information comprising the “envelope” prescribed by the network communications protocol such as Ethernet, frame relay, or asynchronous transfer mode, and examines the destination address of the Internet packet inside. It then consults a routing table maintained in an active memory inside the router and, based on the entry in the routing table corresponding to the destination address, sends that Internet packet to one of two or more output ports. Each output port on a router is connected to another router, perhaps hundreds or thousands of miles away. The routing tables are periodically updated through specialized messages that move through the Internet that normally are invisible to users of the Internet.

Internet packets move from origin to destination through a series of routers. These moves typically are called “hops.” Functionally, the Internet thus can be represented as a logical tree in which each router represents a node at which two or more choices are available as to the path a packet follows to the next node. In theory, an arbitrarily large and complex network can be constructed from a binary tree, signifying that each router has only two output ports. In practice, routers handling substantial amounts of traffic have more than two output ports.

The links in such a tree represent the communications channels connecting the routers. As explained in Part I.A, the Internet is indifferent as to the physical, propagation, or modulation techniques used to carry Internet traffic. Accordingly, one link may be a dial-up telephone line, another link may be a hard-wired wire pair, another link may be an optical fiber capable of moving gigabits per second.

The decision that each router makes with respect to each Internet packet is roughly analogous to the decision that an airline passenger makes in advance with respect to changing planes at a hub airport. Usually, more than one route is available from a particular origin to a particular destination, just as more than one airline route typically is available from one airport to a destination airport. The passenger arrives on one flight at a particular gate—representing an input port—and may leave on any one of several flights departing from other gates, representing output ports. Hub airports, of course, unlike Internet routers, have dozens or hundreds of input ports (gates) and dozens or hundreds of output ports (gates). Moreover, the route followed by an airline traveler, unlike the route followed by an Internet packet, is determined in advance through the reservation and ticketing processes. Nevertheless, there are decisions made at airports that resemble decisions made in routers. An airline passenger ticket for a flight involving changes of planes specifies the input flight, and

the airline dispatch operation determines the input port (gate) at which that flight arrives. The passenger ticket only defines the departure flight; it does not define the gate. The passenger, much like the router, must consult a display board or an airline representative to determine which output port (gate) corresponds to the departure flight number. That corresponds to a router looking up the appropriate output port corresponding to a destination address in its routing table.

Multiple strategies exist for routing packets over the Internet. For example, computer scientists and designers of Internet traffic patterns sometimes deploy routing strategies that involve the fewest hops. Other times, they employ strategies that select the path through the Internet with the highest bandwidth. Routing strategies also can be chosen based on economic decisions.³⁰⁷ These choices are reflected in the routing tables of the routers at particular points in the Internet that have routing tables appropriate to implement the strategy.

The economic incentives are strong for providers of high-bandwidth IP services in a duopolistic market to discriminate in favor of their own offerings or to strike deals with independent suppliers that give them traffic handling preferences.³⁰⁸

The result may not be transparent to consumers. Consumers will pay more money for higher bandwidth connections in their homes and offices, but they will not be forced to pay surcharges for access to disfavored services. Instead the providers of the disfavored services will have to pay more for their connectivity. Because some will not pay, consumers will see worse performance from the disfavored services.³⁰⁹ If things evolve this way, it will be difficult to organize a political coalition to force net neutrality obligations into law.

Many advocates of the Internet's potential to form the basic national infrastructure for communications, information dissemination, and entertainment are concerned about the adverse effects of growing concentration in the provision of Internet connectivity. This concern has been focused through a public debate on "net neutrality." To understand the net neutrality debate, which constitutes the major current public policy debate pitting communications service providers against Internet users, one can benefit from a review of two basic realities, the first dealing with technology and the second dealing with economics.

No one owns the entire Internet. Instead, the Internet is a collection of concepts, technical protocols and format standards that permit thousands—indeed millions—of owners of communications channels and routers to exchange traffic with each other. Because Internet user preferences, functions, and wealth differ, some users are willing to pay more to use the Internet than others. The owners of the hardware and computer programs comprising the routers and communications links thus have an incentive to engage in price discrimination—to charge what the traffic will bear. The owner of Internet assets can determine the identity of senders and recipients of

³⁰⁷ Perritt, *supra* note 56, at 217.

³⁰⁸ *Id.* at 214.

³⁰⁹ *Id.*

Internet traffic based on the origin and destination addresses of the Internet packets moving through their assets. They could therefore, if they wish, set up their routing tables according to the revenue likely to be obtainable from particular users.

The entrepreneur can program his routers to reject low-priced traffic. For example, he can program his router exchanging traffic with end users so that traffic destined for a high-priced provider is routed to the high-capacity communication link connected to a particular output port, while all other traffic is routed to another output port connected to a lower-capacity line. He can program his other router, located further inside the cloud, similarly to route only those packets to or from high-priced subscribers to high-capacity links and to route all others to lower-capacity links. The result is that users, whether they are consumers or providers, get better Internet connectivity if they pay more money, while those paying less money get worse Internet connectivity. The same techniques can be used to discriminate against competitors as well as to discriminate based on the price. For example, the owner of a router may set up the routing tables so that packets addressed to a competing service provider—say a provider of VoIP services—simply are thrown away while packets addressed to the owner’s own VoIP service are passed along to a high-capacity connection carrying that provider’s VoIP traffic. Because the router throws away packets addressed to the competitor, the end user experiences an inability to connect to any VoIP provider except that provided by the owner of the router.³¹⁰

This is exactly what Madison River Communications, LLC did. Madison River is an independent provider of telecommunications services to home subscribers, among others, in North Carolina. It programmed its equipment, presumably routers connected to DSL subscriber lines, to block traffic destined for certain VoIP traffic.³¹¹ It is not entirely clear from the official record made public whether Madison River blocked all VoIP packets or only those intended for VoIP providers competing with Madison’s own VoIP service.³¹² In any event, the FCC notified Madison that it was investigating complaints about its blocking practices and in March 2005, entered into a consent decree, fining Madison River \$15,000 and barring it for thirty months from “block[ing] ports used for VoIP applications or otherwise prevent[ing] customers from using VoIP applications.”³¹³ It does not matter whether Madison River was programming its routers to throw away all VoIP traffic or only VoIP traffic not addressed to its own VoIP servers; the point is that it was using the Internet’s capacity to discriminate against disfavored traffic.³¹⁴

Alarmed by risk of such discrimination developments, commercial entities, including independent VoIP providers and large-volume information enterprises

³¹⁰ *Id.* at 217–18.

³¹¹ *In re Madison River Commc’ns, LLC*, 20 FCC Rcd. 4295, 4297 (2005).

³¹² *Id.*

³¹³ *Id.* at 4297, 4299.

³¹⁴ See *Reconsidering Our Communications Laws: Ensuring Competition and Innovation: Hearing Before the S. Comm. on the Judiciary*, *supra* note 64.

such as Google and Yahoo!, urged Congress to enact new legislation that would ensure net neutrality. Net neutrality would disallow discrimination among consumers and providers of Internet traffic, although it would allow pricing based on the bandwidth of connections—at least price variations for bandwidth provided consumers.³¹⁵ The House of Representatives responded to their concerns. H.R. 5417³¹⁶ would have amended the Clayton Act³¹⁷ by adding a section prohibiting any broadband network provider from offering its network services on discriminatory terms and conditions, refusing to interconnect its facilities with the facilities of other providers of broadband network services, blocking traffic associated with any lawful content applications or services over the Internet, charging fees to avoid discrimination or blocking, and excluding hardware that does not physically damage or materially degrade other utilization of the network.³¹⁸ Hearings were held by both House and Senate committees considering this and similar legislation.³¹⁹

Consumer groups testified in favor of the legislation, in part because it would ensure the availability of competing providers of broadband video services.³²⁰ Opponents of the legislation argued that it was premature and inconsistent with the successful hands-off approach to Internet regulation that had led to massive innovation and investment in the Internet.³²¹ While some of these opponents were willing to accept legislation requiring studies of net neutrality, or relatively mild provisions, they opposed stronger provisions advocated by those most concerned about net neutrality.³²² They argued, however, that going beyond those basic investigations or principles represented “an effort to safeguard against a problem that, at this point and in the foreseeable future, is nonexistent.”³²³ Others argued that the FCC’s existing Internet principles, which the Commission had incorporated into merger approvals,³²⁴ combined with

³¹⁵ Perritt, *supra* note 56, at 218–19.

³¹⁶ H.R. 5417, 109th Cong. (2d Sess. 2006).

³¹⁷ 15 U.S.C. §§ 12–28 (2006).

³¹⁸ Perritt, *supra* note 56, at 219 (citing H.R. 5417, 109th Cong. § 3 (2d Sess. 2006) (adding 15 U.S.C. § 28 and redesignating existing § 28 as § 29)).

³¹⁹ *Id.*; see, e.g., H.R. REP. NO. 109-541 (2006) (report of the House Committee on the Judiciary to accompany H.R. 5417).

³²⁰ See *Communications, Consumer’s Choice, and Broadband Deployment Act of 2006 (Part III): Hearing on S. 2686 before the S. Comm. on Commerce, Sci., & Transp.*, 109th Cong. 13 (2006) (prepared statement of Ben Scott, Director, Free Press) [hereinafter *Hearing*].

³²¹ See *id.* at 26 (prepared statement of Dave McCurdy, President, CEO, Elec. Indus. Alliance).

³²² *Id.* at 25–26 (testifying favorably about “net neutrality” study presently included in S. 2868, and also acquiescing in net neutrality provision in H.R. 5252).

³²³ *Id.* at 30.

³²⁴ The “conditions” appendix of the FCC’s approval of the Verizon/MCI merger includes a section entitled “Net Neutrality,” which obligated Verizon/MCI for two years after the merger date to “conduct business in a manner that comports with the principles set forth in the FCC’s Policy Statement, issued September 23, 2005 (FCC 05-151).” *In re Verizon Comm’n Inc. and MCI, Inc.*, 20 FCC Rcd. 18433, 18509 (2005). Identical language appears in the

market forces, adequately addressed the problem.³²⁵ They argued that more prescriptive legislation would discourage investment in widening the lanes on the Internet highway to avoid traffic jams, which required investment, which in turn, required expectations of an adequate rate of return.³²⁶

The bill reported by the Senate Commerce Committee did not include proposed amendments to strengthen net neutrality provisions. Chairman Ted Stevens said, “We still have a massive disagreement over net neutrality. I still remain convinced that net neutrality is not something that we can define. We haven’t seen it anywhere here or in the world so far and that the World Wide Web is still open [sic].”³²⁷ The House, on the other hand reported H.R. 5417, with stronger net neutrality provisions.³²⁸

*In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications*³²⁹ involved a challenge to Comcast’s practice of throttling peer-to-peer traffic, specifically BitTorrent, used by its subscribers to share files. On the merits, the FCC found:

The record leaves no doubt that Comcast’s network management practices discriminate among applications and protocols rather than treating all equally. . . . Comcast has deployed equipment across its networks that monitors its customers’ TCP connections using deep packet inspection to determine how many connections are peer-to-peer uploads. When Comcast judges that there are too many peer-to-peer uploads in a given area, Comcast’s equipment terminates some of those connections by sending RST packets. In other words, Comcast determines how it will route some connections based not on their destinations but on their contents; in laymen’s terms, Comcast opens its customers’ mail because it wants to deliver mail not based on the address or type of stamp on the envelope but on the type of letter contained therein. Furthermore,

conditions appendix to the approval of the SBC/AT&T merger. *In re SBC Commc’ns Inc. and AT&T Corp.*, 20 FCC Rcd. 18290, 18368 (2005).

³²⁵ *Hearing, supra* note 320, at 11–12 (prepared statement of John Rutledge, on behalf of the U.S. Chamber of Commerce arguing that market forces are adequate and there is no need for a net neutrality law).

³²⁶ *Id.* at 12.

³²⁷ *S. 2686, Communications Reform Bill (Full Committee Markup): Hearing before the S. Comm. on Commerce, Sci., & Transp.*, 109th Cong. (June 28, 2006) (closing statement of Sen. Ted Stevens, Chairman, S. Comm. on Commerce, Sci., and Transp.).

³²⁸ H.R. REP. NO. 109-541 (2006); Perritt, *supra* note 56, at 219.

³²⁹ 23 FCC Rcd. 13028 (2008).

Comcast's interruption of customers' uploads by definition interferes with Internet users' downloads since "any end-point that is uploading has a corresponding end-point that is downloading." Also, because Comcast's method, sending RST packets to both sides of a TCP connection, is the same method computers connected via TCP use to communicate with each other, a customer has no way of knowing when Comcast (rather than its peer) terminates a connection.³³⁰

The FCC found that these practices were not narrowly tailored to easing network congestion and that Comcast had other, nondiscriminatory, methods for managing network congestion.³³¹

Because Comcast did not establish that the challenged procedures were reasonable network management practices,

Comcast's interference with peer-to-peer protocols . . . contravene[s] the federal policy of "promot[ing] the continued development of the Internet" because that interference impedes consumers from "run[ning] applications . . . of their choice," rather than those favored by Comcast, and that interference limits consumers' ability to "access the lawful Internet content of their choice," including the video programming made available by vendors like Vuze. Comcast's selective interference also appears to discourage the "development of technologies"—such as peer-to-peer technologies—that "maximize user control over what information is received by individuals . . . who use the Internet" because that interference (again) impedes consumers from "run[ning] applications . . . of their choice," rather than those favored by Comcast.³³²

The Commission responded to Comcast's challenge "that the Commission cannot exercise jurisdiction over its interference with peer-to-peer TCP connections . . . because such authority must be 'ancillary to something, but here it is not clear what that something might be'"³³³ by pointing to sections 1 (goal of making communications service available), 201 (common carrier practices must be just and reasonable), 706 (deployment of advanced telecommunications services), 256 (promotion of non-discriminatory access to public telecommunications networks), 257 (elimination of market-entry barriers for entrepreneurs and small businesses), and 601

³³⁰ *Id.* at 13050–51 (footnotes omitted).

³³¹ *Id.* at 13056–58 (footnotes omitted).

³³² *Id.* at 13052 (footnotes omitted).

³³³ *Id.* at 13035.

(assuring that cable providers offer widest possible diversity of services) of the Telecommunications Act.³³⁴

In *Comcast Corp. v. FCC*,³³⁵ the Court of Appeals for the D.C. Circuit invalidated the FCC's Comcast order. Noting that the FCC had found "that cable Internet service is neither a 'telecommunications service' covered by Title II of the Communications Act nor a 'cable service' covered by Title VI,"³³⁶ the court found that the Commission lacked ancillary authority under section 4(i) of the Act.³³⁷ Applying its established two-part test—that ancillary jurisdiction exists only when: "(1) the Commission's general jurisdictional grant under Title I [of the Communications Act] covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities,"³³⁸—it found that "[b]ecause the Commission has failed to tie its assertion of ancillary authority over Comcast's Internet service to any 'statutorily mandated responsibility,'" the order was invalid.³³⁹

The court rejected the FCC's argument that the Supreme Court recognized its authority to "require cable companies to allow independent ISPs access to their facilities' pursuant to its ancillary authority, rather than using Title II."³⁴⁰ It found that "policy statements alone" cannot satisfy the requirement for a statutory mandate to serve as the foundation for "ancillary jurisdiction."³⁴¹ The court rejected the FCC's argument that it had authority over broadband under section 706³⁴² and under section 257.³⁴³

In late 2010, the Commission responded to the D.C. Circuit by revising its net neutrality rules prohibiting broadband Internet access providers from discriminating against or blocking traffic.³⁴⁴ It addressed the court of appeals' ruling that it lacked jurisdiction by reiterating its authority under section 706 of the Act;³⁴⁵ its authority to promote competition and investment in, and to protect end users of, voice, video, and audio services;³⁴⁶ its responsibilities under Title II to regulate VoIP

³³⁴ *Id.* at 13036–37.

³³⁵ 600 F.3d 642 (D.C. Cir. 2010).

³³⁶ *Id.* at 645 (citing *In re High-Speed Access to the Internet Over Cable and Other Facilities*, 17 FCC Rcd. 4798, 4802 ¶ 7 (2002), *aff'd*, *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967 (2005)).

³³⁷ 47 U.S.C. § 154(i) (2006).

³³⁸ *Comcast Corp.*, 600 F.3d at 646 (quoting *Am. Library Ass'n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005)).

³³⁹ *Id.* at 661 (quoting *Am. Library*, 406 F.3d at 692).

³⁴⁰ *Id.* at 649 (quoting *Brand X*, 545 U.S. at 1002).

³⁴¹ *Id.* at 654.

³⁴² *Id.* at 658–59.

³⁴³ *Id.* at 659.

³⁴⁴ *In re Preserving the Open Internet Broadband Industry Practices*, GN Docket No. 09-191, FCC 10-201 (Dec. 23, 2010).

³⁴⁵ *Id.* ¶¶ 117–23.

³⁴⁶ *Id.* ¶ 124.

services;³⁴⁷ its authority under Titles III and VI of the Act to promote orderly development of local television broadcasting and MVPD programming;³⁴⁸ and its authority to protect the public interest through spectrum licensing.³⁴⁹

Verizon and others petitioned the D.C. Circuit for review and sought assignment of the case to the same panel that ruled against the earlier FCC net neutrality order. The court of appeals denied the panel-assignment request on February 2, 2011.³⁵⁰

The FCC also could have responded to the D.C. Circuit's decision by reclassifying Internet access as common-carriage—one of the regulatory options identified as the National Broadband Plan.³⁵¹ If the Commission were to take that approach, it would have to reverse its earlier decisions that Internet access over cable and telephone lines does not constitute “telecommunications” service. Administrative agencies are entitled to change earlier decisions, but they must justify such changes in policy consistent with the Administrative Procedure Act's prohibition of arbitrary and capricious decision making.³⁵²

C. Eclipse of the Public Domain for Knowledge and Art

The Internet has made it possible for artists of all kinds to reach a global population of potential audiences by reducing barriers to entry.³⁵³ The frontier of innovation involves developing business models for intermediaries, and mitigating transaction costs for licensing preexisting content. As Larry Lessig has observed, however, “just as a free market is perverted if its property becomes feudal, so too can a free culture be queered by extremism in the property rights that define it.”³⁵⁴

It was clear at the time of the Harvard Conference that the growth of the Internet as a backbone for commerce, social interaction, and politics would involve the emergence of new intermediaries.³⁵⁵ Twenty years later, the Internet revolution is manifested as much by new rapidly growing Internet intermediaries who are supplanting the role

³⁴⁷ *Id.* ¶¶ 125–26.

³⁴⁸ *Id.* ¶¶ 127–32.

³⁴⁹ *Id.* ¶¶ 133–35.

³⁵⁰ *Verizon v. FCC*, No. 11-1014, 2011 WL 446556 (Feb. 2, 2011) (per curiam).

³⁵¹ *See* Pub. L. No. 111-5, 123 Stat. 513 (2009); *Comcast Corp. v. FCC*, 600 F.3d 642, 645 (D.C. Cir. 2010).

³⁵² *See e.g.*, *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42 (1983) (noting that “an agency changing its course by rescinding a rule is obligated to supply a reasoned analysis for the change” and ultimately invalidating Department of Transportation's change in seatbelt rule).

³⁵³ Henry H. Perritt, Jr., *New Business Models for Music*, 18 VILL. SPORTS & ENT. L.J. 63 (2011) (arguing that new Internet technologies are facilitating access by low-budget musicians); *see* Perritt, *supra* note 56 (arguing the same for moviemakers).

³⁵⁴ LAWRENCE LESSIG, *FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE & CONTROL CREATIVITY* xvi (2004).

³⁵⁵ Henry H. Perritt, Jr. *Jurisdiction in Cyberspace: The Role of Intermediaries*, in *BORDERS IN CYBERSPACE: INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE* 164 (Brian Kahin & Charles Nesson eds., 1997).

of established institutions: Amazon at the expense of Borders, iTunes at the expense of Tower Records, NetFlix at the expense of Blockbuster. This part of the revolution continues and it is uncertain which new intermediation ideas will prove to be the “next big thing,” and which brick and mortar establishments will fall victim.³⁵⁶

As this disruptive change in intermediation continues, the threatened enterprises are employing a variety of measures to thwart the emergence of new Internet-based intermediaries. As Larry Lessig said, “an environment designed to enable the new is being transformed to protect the old.”³⁵⁷ Copyright enforcement is increasingly taking the form of closing off access.

The technology-driven revolution in the popular music industry is a good example of the threat.³⁵⁸ The major labels will not survive in anything like their previous forms. CDs are dead as a distribution medium. Barriers to entry have declined dramatically as the costs of producing top-quality recordings have dropped by a couple of orders of magnitude. Portable music players, such as smartphones, permit consumers to listen to music all the time and this enormously increases the potential demand for music.

“The increased competition and the demise of traditional gatekeepers signal a sharp reduction in prices—approaching zero—for recorded music.”³⁵⁹ Prices for recorded music approaching zero also means that copyright is becoming irrelevant except at the margins of the “new order.”³⁶⁰ “As prices for recorded music decline . . . toward zero [with costs] . . . [t]he costs of copyright enforcement exceed the benefits.”³⁶¹ The result is nearly one in which no one is willing to pay (much) for recorded music.³⁶² “Technology makes it impossible to enforce copyright, but it does not matter, because no one would pay for music from either the originator or a pirate. A pirate cannot construct a viable business model.”³⁶³

Increased supply and demand result in higher search costs. Musicians and their potential fans must be able to find each other. Someone has to perform the match-making function formerly performed by the major labels and the radio station chains. Innovation and experimentation will increase as new kinds of intermediaries seek the best way to connect musicians with their potential fans. A handful of these will become the dominant gatekeepers.³⁶⁴

³⁵⁶ See Perritt, *supra* note 353, at 155–62 (explaining the need for intermediaries in markets for music and arguing that new intermediaries are arising to perform the function of institutions locked into obsolete capital).

³⁵⁷ LAWRENCE LESSIG, *THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD* 6 (2001).

³⁵⁸ Perritt, *supra* note 353, at 65.

³⁵⁹ *Id.*

³⁶⁰ *Id.* at 66.

³⁶¹ *Id.* at 95.

³⁶² *Id.*

³⁶³ *Id.*

³⁶⁴ *Id.* at 66.

The emerging intermediaries, necessary to perform the matchmaking function, will not work for free.³⁶⁵ Even if a business model is unnecessary for the musicians themselves, it is necessary for the intermediaries.³⁶⁶ Unless such a business model emerges, the new music marketplace will be one in which hundreds of thousands of artists making very good music go essentially unnoticed by those who would enjoy their music.³⁶⁷ For viable business models to exist, entrepreneurs must creatively monetize access to the celebrity, and also develop technologies for classifying music to reduce consumer search costs.³⁶⁸ Monetization will rely less on copyright and more on behaviorally targeted advertising and social networking.

“As with popular music, new technologies of video entertainment have opened the gates to the marketplace for independent (‘indie’) artists and producers, eroding the control of traditional gatekeepers.”³⁶⁹ “[T]echnology is causing the collapse of boundaries separating movies, television, the Internet, and video games—the traditionally separate categories of video entertainment.”³⁷⁰

Digital technologies are now gradually dominating moviemaking, replacing film. Production activities that used to be defined by a medium or channel of distribution now easily cover several.³⁷¹ “The melding of these traditionally separate categories requires rethinking the economics, business strategies, and legal frameworks that shape video entertainment.”³⁷²

Collapsing boundaries and reduced barriers mean a more efficient and competitive industry, with a wider variety of choices for consumers. Large capital costs for production of full-motion video works can be spread over more product lines. Migration of artists and technologists from one industry category into others will disrupt old ways of doing things and reduce capital requirements.³⁷³

Serialization³⁷⁴ may make a comeback because it can reduce the capital costs. Moviemakers can build a fan base and a pool of potential investors with an initial, relatively low cost pilot episode, and then build a revenue stream over time with future episodes. When a work is serialized, “the economic value of the creative effort is more in the characters than in the specific details of a single production. Accordingly, the copyright battleground will shift to protection of characters and basic story

³⁶⁵ *Id.* at 175.

³⁶⁶ *Id.* at 66. The point is not that musicians do not *deserve* to make money; the point is that they will make music whether or not they make money.

³⁶⁷ *Id.* at 66–67.

³⁶⁸ *Id.* at 68.

³⁶⁹ Perritt, *supra* note 56, at 108.

³⁷⁰ *Id.* at 107.

³⁷¹ *Id.* at 108.

³⁷² *Id.* at 107.

³⁷³ *Id.* at 108.

³⁷⁴ “[S]erialization has a long pedigree in popular culture, used by Charles Dickens to bring his novels within the reach of mass audiences.” *Id.* at 110.

features³⁷⁵ The law will have to work harder to allow authors, such as fan-fiction writers, to build new narratives on the work by creators of the originals.³⁷⁶

Crowd sourcing is another possibility for allowing larger numbers of people to collaborate on the creation, production, distribution, marketing, and financing. When collaboration increases, the law of joint authorship becomes more important. Larger creative teams puts stress on default rules for apportioning ownership of intellectual property.³⁷⁷

In these new, expanded markets, however, new entrants will need to license copyrighted music, characters, storylines, or scenes that they incorporate into new movies. This will increase the already-daunting transaction costs for licensing rights.³⁷⁸

New public and private law mechanisms are needed to make the market function more efficiently, by making it easier for creators of new works to (1) find the owners of preexisting content, and (2) overcome other barriers to obtaining licenses, such as strategic behavior, irrational protection of entrenched bureaucracies, and obsolete, embedded capital.³⁷⁹

As the technology-driven revolution continues in the entertainment industry, one of the most dangerous threats to the sustainability of the Internet's open character arises: overreaching by owners of intellectual property—particularly ownership of copyright in entertainment works.³⁸⁰ Rightsholders use civil subpoenas to obtain private information about network users and then file lawsuits by the tens of thousands. They pressure ISPs to discriminate among users of their connection services. That pressure is what triggered the net neutrality debate. They hire contractors to extort settlements by those they accuse of infringement. Copyright law threatens the healthy evolution of the Internet because of expansion of copyright monopolies, abuse of civil litigation, and legislative capture.³⁸¹

1. Expansion of Copyright Monopolies

Expansion of protection for rightsholders and diminished scope for traditional privileges, such as that available under Fair Use, stifles creative innovation because

³⁷⁵ *Id.*

³⁷⁶ *Id.*

³⁷⁷ *Id.*

³⁷⁸ Henry H. Perritt, Jr., *Cut in Tiny Pieces: Ensuring that Fragmented Ownership Does Not Chill Creativity*, 14 VAND. J. ENT. & TECH. L. 1, 4 (2011).

³⁷⁹ *Id.*

³⁸⁰ See generally LESSIG, *supra* note 354 (arguing that copyright law has been used to stifle innovation); LESSIG, *supra* note 357 (arguing that changes in copyright and other forms of intellectual property protection have the potential to choke off publicly held material, which constitute an intellectual commons).

³⁸¹ See generally Henry H. Perritt, Jr., *Property and Innovation in the Global Information Infrastructure*, 1996 U. CHI. LEGAL F. 261 (1996) (arguing that product design can protect against free riding better than copyright law).

it makes it easier for established enterprises with an IP portfolio to discourage or block new creative effort that competes with existing works. Two instances of such expansion involve extending copyright to protect characters and plots, and extension of the term of the copyright monopoly.

One area of expansion extends copyright protection to plots and characters. Protection of characters and the derivative work right have been explored in recent litigation involving fan fiction.³⁸² Two recent cases involving fan fiction used Judge Hand's abstractions test to afford copyright protection to fictional characters; one involved Holden Caulfield from *Catcher in the Rye*, while the second involved the *Harry Potter* series.³⁸³ "In *Salinger v. Colting*,³⁸⁴ the district court granted a preliminary injunction barring publication of an unauthorized sequel to *Catcher in the Rye*, finding probability of success on [a] prima-face copyright infringement [claim] and unlikelihood of success on a fair use defense."³⁸⁵ The court concluded that the Holden Caulfield character was "distinctively delineated" in *Catcher in the Rye* and therefore qualified for copyright protection.³⁸⁶

³⁸² Perritt, *supra* note 377, at 15.

"Fan fiction" refers to a phenomenon in which persons other than the author of a work write their own stories about characters created by the original author, usually making no pretense that the characters are different. Fan fiction is an exploding genre, fueled by the ease with which new works by unknown authors can be disseminated on the Internet. "Mary Sue fiction" creates stories in which minor characters from earlier works star in new works or in which entirely new characters are inserted. "Slash fiction" takes male characters from earlier works and puts them in gay contexts. "Real person slash fiction" takes real people and puts them in stories involving gay relationships or encounters.

Perritt, *supra* note 56, at 179; see William W. Fisher III, *The Implications for Law of User Innovation*, 94 MINN. L. REV. 1417, 1420–21 (2010) (describing the phenomenon of fan fiction and suggesting several different varieties); see also Anupam Chander & Madhavi Sunder, *Everyone's a Superhero: A Cultural Theory of "Mary Sue" Fan Fiction as Fair Use*, 95 CALIF. L. REV. 597, 598–601 (2007); Sonia K. Katyal, *Performance, Property, and the Slashing of Gender in Fan Fiction*, 14 AM. U. J. GENDER SOC. POL'Y & L. 461, 481–97 (2006); Aaron Schwabach, *The Harry Potter Lexicon and the World of Fandom: Fan Fiction, Outsider Works, and Copyright*, 70 U. PITT. L. REV. 387, 388–91 (2009); Rebecca Tushnet, *Legal Fictions: Copyright, Fan Fiction, and a New Common Law*, 17 LOY. L.A. ENT. L.J. 651, 655 (1997).

³⁸³ *Salinger v. Colting*, 641 F. Supp. 2d 250 (S.D.N.Y. 2009); Warner Bros. Entm't Inc. v. RDR Books, 575 F. Supp. 2d 513 (S.D.N.Y. 2008); Perritt, *supra* note 56, at 179 n.298.

³⁸⁴ 641 F. Supp. 2d at 250, *vacated*, 607 F.3d 68, 83 (2d Cir. 2010) (holding that district court erroneously presumed irreparable injury in granting preliminary injunction under eBay, Inc. v. MercExchange, LLC, 547 U.S. 388 (2006)).

³⁸⁵ Perritt, *supra* note 377, at 15.

³⁸⁶ 641 F. Supp. 2d at 254 (quoting 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.12 (2009)) (explaining the standard for protection of fictional characters).

The second fan fiction case, *Warner Bros. Entertainment Inc. v. RDR Books*,³⁸⁷ involved a claim of copyright infringement by J.K. Rowling, the author of the *Harry Potter* series, against the developers and publishers of a “Harry Potter Lexicon,” which provided supplementary information on the characters and events in the *Harry Potter* books.³⁸⁸ The district court found that the Lexicon contained “direct quotations or paraphrases, plot details, or summaries of scenes from one or more of the *Harry Potter* novels.”³⁸⁹ The defendant copied fictional facts invented by Rowling, “such as the attributes of imaginary creatures and objects, the traits and undertakings of major and minor characters, and the events surrounding them.”³⁹⁰ “[S]uch invented facts constitute[d] creative expression protected by copyright,” according to the court.³⁹¹

Another defacto expansion of copyright is exemplified by the rise in right-of-publicity claims under state law.³⁹² Many such claims should be found to be preempted by the federal Copyright Act.³⁹³

The Copyright Extension Act is another example of an effort by established rightsholders to extend their monopolies. In *Eldred v. Ashcroft*,³⁹⁴ Justice Stevens’s dissent criticized the abandonment by the Court of its responsibility to protect the public interest in free access to the products of artistic genius.³⁹⁵ Justice Breyer’s dissent characterized the extension as making the copyright term virtually perpetual, in violation of the constitutional requirement that it be limited, and that granting the extended term to “heirs, estates, and corporate successors” of authors vitiated the constitutionally required purpose of promoting “Science”—indeed it inhibited the progress of science by interposing obstacles to access to copyrighted works.³⁹⁶

2. Abuse of Civil Litigation Process

As new technologies have stressed traditional business models, aggressive litigation by traditional rightsholders has materialized, as evidenced by analysis

³⁸⁷ 575 F. Supp. 2d 513 (S.D.N.Y. 2008).

³⁸⁸ *Id.* at 517, 519–20.

³⁸⁹ *Id.* at 535.

³⁹⁰ *Id.* at 536.

³⁹¹ *Id.*

³⁹² *See, e.g.,* *Keller v. Elec. Arts, Inc.*, No. C 09-1967 CW, 2010 WL 530108, at *11 (N.D. Cal. Feb. 8, 2010) (denying motion to dismiss professional football player’s right-of-publicity claim against video game producer).

³⁹³ *See Jules Jordan Video, Inc. v. 144942 Canada Inc.*, 617 F.3d 1146, 1154–55 (9th Cir. 2010) (finding that the actor’s right-of-publicity claim against unlicensed distribution of his performances was preempted).

³⁹⁴ 537 U.S. 186 (2003).

³⁹⁵ *Id.* at 242 (Stevens, J., dissenting).

³⁹⁶ *Id.* at 243 (Breyer, J., dissenting).

throughout this Part. The enforcement methods used by rightsholders threatens core Internet characteristics when rightsholders mobilize legal or economic pressure on intermediaries such as ISPs to block traffic that facilitates infringing activities—as defined by rightsholders, who naturally take an expansive view of what constitutes infringement of copyright,³⁹⁷ and through their litigation strategies.

I have been an occasional participant in the Electronic Frontier Foundation's efforts to block abuse of civil process.³⁹⁸ The Recording Industry Association of American (RIAA)'s litigation typically proceeded like this: The RIAA would serve basketfuls of subpoenas on ISPs, demanding personally identifying information for individuals linked to IP addresses that the RIAA believed to be involved in exchanging unlicensed music files. Once it obtained the information, it transferred it to contractors who would send demand letters threatening litigation and emphasizing statutory damages running into the hundreds of thousands or millions of dollars. The contractor then would offer to settle for what it estimated was in the target's bank account. Most recipients, frightened, settled.³⁹⁹ This organized extortion has mostly survived challenges, although grudgingly, the courts are placing limitations on it. In *Lahiri v. Universal Music & Video Distribution Corp.*,⁴⁰⁰ the court of appeals affirmed an award of \$247,397.28 in attorneys' fees and \$10,808.76 in costs, under 28 U.S.C. § 1927, against an attorney who represented an individual who maintained frivolous copyright infringement actions.⁴⁰¹

In *Capitol Records, Inc. v. Foster*,⁴⁰² the district court awarded attorneys' fees to a defendant who had been sued for alleged infringement of musical works owned by the plaintiff occurring through her Internet account.⁴⁰³ The court found that:

The plaintiffs failed to allege any facts in their complaint that would support Ms. Foster's secondary copyright infringement liability. The complaint is devoid of any suggestion that Ms. Foster knew third parties were using her account to infringe the plaintiffs' copyrights or that she substantially participated in any infringing activities. Also absent from the complaint is any allegation that Ms. Foster profited from a direct infringement.

³⁹⁷ See *supra* Part II.B (discussing net neutrality).

³⁹⁸ See, e.g., *Facebook Plaintiffs Seek to Consolidate Tracking Cookie Cases in California*, PRNEWswire (Oct. 17, 2011), <http://prnewswire.com/news-releases/facebook-plaintiffs-seek-to-consolidate-tracking-cookie-cases-in-california-retain-professor-of-law-and-former-dean-of-chicago-kent-college-of-law-henry-h-perritt-jr-as-expert-advisor-132013918.html>.

³⁹⁹ See Henry H. Perritt, Jr., *Music Markets and Mythologies*, 9 J. MARSHALL REV. INTELL. PROP. L. 831, 833 (2010).

⁴⁰⁰ 606 F.3d 1216 (9th Cir. 2010).

⁴⁰¹ *Id.* at 1218, 1223.

⁴⁰² No. Civ. 04-1569-W, 2007 WL 1028532 (W.D. Okla. Feb. 6, 2007).

⁴⁰³ *Id.* at *6.

Additionally, neither the parties' submissions nor the Court's own research has revealed any case holding the mere owner of an Internet account contributorily or vicariously liable for the infringing activities of third persons.⁴⁰⁴

Moreover, the court questioned the good faith of the plaintiffs, finding that it appeared that the "plaintiffs initiated the secondary infringement claims to press Ms. Foster into settlement after they had ceased to believe that she was [the] direct or 'primary' infringer."⁴⁰⁵ The evidence indicated that the defendant's estranged husband or her adult daughter may have been responsible for the alleged infringement.⁴⁰⁶

In a decision significant for a broad category of disputes over "theft" of protected signals or copyrighted content, the Court of Appeals for the Ninth Circuit affirmed dismissal of a Racketeer Influenced and Corrupt Organizations Act (RICO) action against a satellite television broadcaster.⁴⁰⁷ Plaintiffs alleged that the broadcaster sent more than 100,000 letters to purchasers of satellite-signal decryption equipment, threatening criminal prosecution and civil litigation unless the recipients paid thousands of dollars to settle claims that they unlawfully intercepted and viewed encrypted satellite television broadcasts.⁴⁰⁸ The suit claimed that the broadcasters made no attempt to discern whether recipients of the demand letters were actually engaged in illegal conduct, and telephone calls by the recipients protesting their innocence were rebuffed with renewed demands for payment of money to settle the claims; therefore, the pattern of sending the letters constituted extortion because they induced fear, made unsupported factual allegations, and misstated the law, thus constituting fraud.⁴⁰⁹

In *Recording Industry Ass'n of America, Inc. v. Verizon Internet Services, Inc.*,⁴¹⁰ the Court of Appeals for the D.C. Circuit reversed the district court. The court avoided constitutional challenges to the DMCA subpoena provision⁴¹¹ and held that § 512(h) of the statute did not authorize subpoenas compelling an ISP to disclose information as to which the "ISP act[s] only as a conduit for data transferred between two internet users, such as persons sending and receiving e-mail or, as in this case, sharing P2P files."⁴¹²

Another type of abuse of process by rightsholders involves frivolous takedown notices under the DMCA. Frivolous DMCA takedown notices can inflict serious

⁴⁰⁴ *Id.* at *3.

⁴⁰⁵ *Id.* at *4.

⁴⁰⁶ *Id.* at *1.

⁴⁰⁷ *Sosa v. DIRECTV, Inc.*, 437 F.3d 923 (9th Cir. 2006) (involving claims under RICO, 18 U.S.C. §§ 1961–1968).

⁴⁰⁸ *Id.* at 925–26, 942.

⁴⁰⁹ *Id.* at 939–40 (characterizing claims by plaintiffs).

⁴¹⁰ 351 F.3d 1229 (D.C. Cir. 2003).

⁴¹¹ 17 U.S.C. § 512(h) (2006).

⁴¹² *Recording Indus. Ass'n of Am.*, 351 F.3d at 1233.

harm on persons denied access to e-commerce as a result.⁴¹³ The DMCA provides a remedy for such notices.⁴¹⁴

In *Design Furnishings, Inc. v. Zen Path, LLC*,⁴¹⁵ the district court preliminarily enjoined a furniture designer from submitting DMCA takedown notices to eBay. The defendant claimed that the plaintiff's outdoor patio furniture infringed on her designs, although the Copyright Office had denied defendant's copyright application.⁴¹⁶ The court began with the proposition that:

The DMCA provides that "[a]ny person who knowingly materially misrepresents under this section . . . that material or activity is infringing . . . shall be liable for any damages . . . incurred by the alleged infringer . . . who is injured by such misrepresentation, as the result of the service provider . . . removing or disabling access to the material or activity claimed to be infringing"⁴¹⁷

The court found that the defendant's furniture was not likely entitled to copyright protection, and found the "knowingly misrepresents" element satisfied by the defendant's failure to respond to the plaintiff's demand that it prove its intellectual property rights—three months before the defendant even applied for a copyright registration.⁴¹⁸

The court found "irreparable harm," although damages alone are usually insufficient:

[T]he court concludes that, if defendant continues to submit notices of copyright infringement to eBay, it is likely that eBay would terminate listings, temporarily restrict plaintiff from selling on one or both of its accounts, or suspend or terminate plaintiff's accounts. eBay's responses to defendant's notices would likely deter prospective customers and adversely affect plaintiff's reputation and goodwill on a web site from which it generates 95 percent of its revenues. Plaintiff's accounts' policy violation ratings would also likely decrease if plaintiff continues to sell the furniture and defendant continues to submit notices to eBay. The decrease in the policy violation ratings would also cause irreparable harm.⁴¹⁹

⁴¹³ See Michael P. Murtagh, Note, *The FCC, the DMCA, and Why Takedown Notices Are Not Enough*, 61 HASTINGS L.J. 233, 253–57 (2009).

⁴¹⁴ See § 512 (g)(3) (explaining the counter notification mechanism).

⁴¹⁵ No. CIV 2:10-2765 WBS GGH, 2010 WL 5418893 (E.D. Cal. Dec. 23, 2010).

⁴¹⁶ *Id.* at *2.

⁴¹⁷ *Id.* at *4 (quoting § 512(f)).

⁴¹⁸ *Id.* at *5–6.

⁴¹⁹ *Id.* at *7 (citation omitted).

3. Legislative Capture

The likelihood of effective legislative action to redress the balance between new creativity and the property rights of past creators is small because of legislative capture by the established interests who oppose innovation and competition. The legislative process leading up to enactment of the DCMA⁴²⁰ reflects one of the political realities of copyright policy making: when rightsholders were unable to persuade Congress to enact their legislative priorities, they went to international treaty organizations, drafted treaty language that was adopted, and then returned to Congress, saying, in effect, “You have to enact legislation; it’s the obligation of the United States under international law.”⁴²¹ The ensuing legislative process also provided an opportunity to amend copyright law in other respects as well. The political power of Walt Disney Company, other movie studios, and record labels makes any effort to reform copyright law legislatively perilous.⁴²²

D. Behaviorally Targeted Advertising

Behaviorally targeted advertising offers advantages to both advertisers and consumers. Advertisers need not pay high prices for undifferentiated access to large numbers of potential customers through television, print, or billboard advertising. Instead they can pay, often only if the target looks at (clicks on) the ad, for advertisements targeted narrowly to persons likely to have a propensity to purchase their products.⁴²³ Consumers see only—or mostly—advertisements aligned with their interests. Behaviorally targeted advertising is possible only by using large stores of information about the Internet behavior of millions of consumers.

E-commerce is well established. Early concerns about payment systems, order fulfillment, and trust are but distant memories. Big e-commerce sites, such as Amazon and eBay, make it easy for small entrepreneurs to reach a global customer base.⁴²⁴

⁴²⁰ Pub. L. No. 105-304, 112 Stat. 2861 (1998).

⁴²¹ I participated in discussions in the Clinton White House about how to rein in Bruce Lehman, Under Secretary of Commerce for Intellectual Property and Commissioner of Patents and Copyrights, who was perceived as pursuing expansion of copyright in international negotiations.

⁴²² See generally LESSIG, *supra* note 357, at 11 (describing the copyright wars as being about basic American values, necessitating a balance between property interests and the opportunity for creators to build on the past).

⁴²³ See Perritt, *supra* note 398, at 852.

⁴²⁴ See, e.g., *Selling on Amazon*, AMAZON, <http://www.amazonservices.com/content/sell-on-amazon.htm?ld=AZFSSOA#!how-it-works> (explaining how to set up a presence on amazon.com) (last visited May 1, 2012); *eBay Seller Information Center*, EBAY, <http://pages.ebay.com/sellerinformation/ebayforbusiness/essentials.html> (explaining how to set up a seller presence on eBay) (last visited May 1, 2012).

E-commerce exhibits a wide variety of business models. Sellers of information content have tried subscription models, similar to that used by cable television services. Many others, such as portals providing indexing and pointers value, used an advertising model like that originally employed by newspapers and television and radio broadcasting.⁴²⁵ Still others charge a fee for each sale, resembling the business model long used by brokers. Both the advertising and the data-collection models benefit from giving content away for free.⁴²⁶ They are thus the most interesting for the future of e-commerce, in an environment in which consumers are accustomed to access without payment, fueled by the large number of providers who are willing to volunteer their services and give away the fruits of their services, as on most blogs in many collaborative offerings, such as Wikipedia.⁴²⁷

The technology of the Internet permits many of these business models to be combined. For example, advertisements can be “clickable,” signifying that one may not only read the advertisement, but also click on the image of the advertisement and automatically be connected to the advertiser’s website. This possibility enables those selling advertising to charge not only for ad placement, but also for user clicks. Some e-mail services are free to consumers who agree to receive graphical display ads with their email.⁴²⁸ Consumers also must agree to the release of personal information that they supply with their subscription applications to the advertisers.

The central role of advertising in most business models has accelerated the use of behaviorally targeted advertising. Providers of content and value-added features can collect data about the behavior and interests of people who access their services, and then sell that data. The value of such consumer transaction data is in helping product suppliers and marketing personnel to target advertising and direct mail solicitation through conventional media much more narrowly. It also benefits consumers because they are more likely to get advertisements that they are interested in, similar to Amazon’s and Netflix’s “recommendations.” Obviously, this opportunity for selling and using data raises major personal privacy concerns.⁴²⁹ The controversy is likely

⁴²⁵ See Robert Samuelson, *The Five Business Models of E-Commerce*, CLICKZ (Dec. 23, 1998), <http://clickz.com/clickz/column/1718210/the-five-business-models-e-commerce>.

⁴²⁶ See Chris Anderson, *The Economics of Giving It Away*, WALL ST. J. (Jan. 31, 2009), <http://online.wsj.com/article/SB123335678420235003.html>.

⁴²⁷ See *Wikipedia: The Promise and Perils of Crowdsourcing Content*, ECONOMIST (Jan. 13, 2011), <http://www.economist.com/node/17911276>.

⁴²⁸ See *The Economics of Free: Nice But Tricky*, ECONOMIST (July 16, 2009), <http://www.economist.com/node/14030161>.

⁴²⁹ See Kenneth A. Bamberger & Dierdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 283 (2011) (referring to the controversy over Doubleclick’s plan to combine clickstream information with other consumer data); Samantha L. Millier, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 545–47 (2009) (raising alarms about Facebook’s collection of data for behaviorally targeted advertising); William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195,

to grow over private collection and use of personal data, although the more significant threat is that the government will get access to the information, if it is collected.

If the law impedes private-sector use of personal data for behaviorally targeted advertising, it will discourage one of the most promising possibilities for providing revenue to replace that lost by over-expansive definitions, or over-aggressive enforcement, of intellectual property rights. On the other hand, the law should be vigilant in blocking the government from spying on its citizens by easy access to the store of personal data.

E. Cybersecurity

The Internet is a powerful tool for spying, and an appealing target for criminals, vandals, and terrorists. How the law limits the tools and protects the targets will have a powerful effect on the future of the Internet.

1. Police States, Cyberactivism and Embargos

The Internet makes it more difficult for totalitarian regimes to control their populations, but it also makes it easier for them to spy on their populations. The Arab Spring demonstrated that insurgents can use a variety of tools, many of them depending on Internet connectivity, to communicate plans and coordinate activities to circumvent governmental efforts to crush dissent.⁴³⁰ But it also demonstrated the fallacy of the belief that the Internet cannot be shut down by the government. The regimes in Egypt, Lybia, Iran, and Syria succeeded, when political crises bloomed, in disabling Internet connectivity within their territories.⁴³¹ As intelligence agencies get more sophisticated, they can monitor Internet trails, providing better intelligence on the activities of dissidents. Traffic analysis, even without access to communications content, can reveal the identity of leaders, their whereabouts, and their plans.

2. Power of Traffic Analysis

Transactional data about communications, not involving access to content, enjoy a less protected position than content in the combinations of legal controls adopted by Congress. Less protection for such data flows from the reasoning of the *Smith*

1220–21 (2010) (describing collection of personal data for use in targeted advertising; suggesting the activity violated the SCA).

⁴³⁰ See William Saletan, *Springtime for Twitter: Is the Internet Driving the Revolutions of the Arab Spring?*, SLATE (July 18, 2011), http://www.slate.com/articles/technology/future_tense/2011/07/springtime_for_twitter.single.html.

⁴³¹ See Ido Kenan, *e-Censorship and the Arab Spring*, MA'ARAV EDITORIAL (Nov. 17, 2011), <http://www.maarav.org.il/english/2011/11/e-censorship-and-the-arab-spring>.

case⁴³²—that little expectation of privacy for such data exists because the data are disclosed to and used by third-party service providers. Even if that proposition is correct for dialed telephone numbers, it is not true for the inferences that may be drawn from large quantities of data about patterns of communication available from modern telecommunications networks. Traffic analysis of IP packets to and from a particular target can reveal a blueprint of the target's human associations. It can reveal subject matter interests through analysis of web browsing. Analysis of geographic information from cell phone connections can detail target movements, minute-by-minute.⁴³³

Advances in technology facilitate such traffic analysis because they facilitate acquisition of transactional data, as from IP packet headers, and they also facilitate machine analysis of patterns revealed by the acquired data. In many cases, traffic analysis may actually be more valuable to law enforcement and intelligence agencies than the content of a handful of messages. Traffic analysis may also be more revealing about the private conduct and thoughts of a target than content.

Suppose a criminal intelligence agency acquires information about every cell phone call made or received by a target for a period of six months. Through relatively inexpensive and widely available techniques, the agency can collect information on the date and time of every call made or received and the other telephone number to or from which a call is attempted or established. Call-duration data is also available. By analyzing the patterns of cell phone communication by the target, the monitoring agency could determine, for example, that the target communicates at least daily with a suspected drug dealer and, regularly, on a weekly basis, with another individual in the target's hometown. From these data the agency could infer that the target is himself a drug dealer, or at least a drug user, and also could infer that the individual with whom the target communicates weekly is a good friend or, possibly, someone with whom the target has a romantic involvement.

A foreign intelligence agency might obtain data on a target, which could reveal that the target has regular communication with a particular telephone number in Iran and places many calls to different individuals in a geographic area with a substantial Muslim population. From these data the foreign intelligence agency might infer that the target is involved in raising money for an activity directed from Iran, or that the target is involved in organizing some form of collective activity related to Iran. At the very least, these inferences might constitute sufficient probable cause to allow the agency to obtain a judicial order for acquisition of the content of these communications.

⁴³² See PERRITT, *supra* note 73, § 13.05[A] (analyzing *Smith v. Maryland*, 442 U.S. 735 (1979)).

⁴³³ “Although acts performed in ‘public,’ especially if taken singly or in small numbers, may not be confidential, at least arguably a right to privacy may nevertheless be invaded through extensive or exhaustive monitoring and cataloguing of acts normally disconnected and anonymous.” *Nader v. Gen. Motors Corp.*, 255 N.E.2d 765, 772 (N.Y. 1970) (Breitel, J., concurring).

The overall effect is analogous to physical surveillance of the target—following the target everywhere and identifying all the people with whom the target communicates face to face.

A newer form of traffic analysis is potentially even more useful and even more intrusive: monitoring a target's web browsing. Information about every URL visited by a target is readily collectible by intercepting IP traffic to and from the target's IP address under a Pen/Trap order, which does not require probable cause.⁴³⁴ Alternatively, and at far less cost, a criminal intelligence or a foreign intelligence agency can obtain much of the same kind of information by obtaining records maintained by search engines, such as Yahoo! and Google, which would reveal every web page a user/target searches for. Because most web browsing involves regular resort to search engines to find the URL for web pages of interest, data from search engines represents a substantial subset of web browsing activity.

Analysis of this type of traffic not only reveals other people with whom a target has communication, but is analogous to a type of physical surveillance—entirely impracticable to effectuate—which would have someone looking over the target's shoulder as the target browses newspapers, magazines, or possible selections in a bookstore. It is thus closer to revealing the target's interests and thoughts, even if the target never chooses to reveal these to anyone else.

Here lies the problem: the usefulness of the new kinds of traffic analysis that the technologies of surveillance and target communication make possible is enormous. It should not be difficult to convince legislators and judges that there is a compelling need to engage in these newly productive types of surveillance, especially when the surveillance can be justified as necessary for the “War on Terrorism.” But the risks to personal liberty and personal autonomy that lie at the core of liberty, while unprecedented, are likely to be overlooked when framed within legal concepts developed under the impact of past technologies to distinguish areas in which people have a “reasonable expectation of privacy” from areas where they do not.

Furthermore, legislative and judicial decisions about striking the right balance between surveillance and privacy almost always tend to assume that the government will maintain the confidentiality of everything that it collects. In fact, experience shows that individual government officials and agents do not necessarily respect confidentiality obligations.⁴³⁵ The investigation of the Vice President's office with respect to disclosing the identity of CIA agent Plame, FBI Director J. Edgar Hoover's use of wiretap conversations to undermine the credibility of Martin Luther King, the role of FBI executive Mark Felt as Deep Throat in the Watergate controversy, FBI leaks about an individual suspected for a time of being the Atlanta Olympics bomber, and many other instances demonstrate that when even the most secretive government

⁴³⁴ See 18 U.S.C. §§ 3121–3127 (2006).

⁴³⁵ See generally STEPHEN HESS, *THE GOVERNMENT/PRESS CONNECTION: PRESS OFFICERS AND THEIR OFFICES* 75–94 (1984) (regarding “leaks and other informal communications”).

agencies have explosive information about individuals, the temptation to leak it is strong.

Consider further what would be in the information pool subject to possible leaks if widespread traffic analysis is performed, either monitoring e-mail communications and cell phone communications, or monitoring web browsing. The pattern-matching tools are imprecise, and it is inevitable that someone engaging in perfectly innocuous activities would occasionally come under suspicion. Heightened suspicion means that more data would be collected and more attention paid to it. And minimization does not work very well in these new contexts. So communications and web browsing associated with suspect persons or subjects would be accompanied by data on other matters of a sensitive nature to the target, albeit unrelated to national security threats or to criminal activity, obviously including sexual relationships or interests that the target legitimately may not want exposed to others. The temptation to leak these kinds of traffic would be especially strong to a leaker who wants to injure the target, because the leaks would not jeopardize legitimate national security or criminal intelligence.

3. Cybercrime and Cyberterrorism

The growing awareness, not only by governments but also by the general public, of the magnitude of the threat posed by cyberterrorism will make it easier to impose technological controls that undermine the essential features of the Internet architecture and that subject everyone to more intrusive government surveillance. The cyberterrorism threat not only involves Internet use to organize physical terrorist acts, as al-Qaeda has done, but it also provides a platform for effectuating attacks.⁴³⁶ If an attacker could disable access to bank records or corrupt data, interfere with military command and control systems, disable the intelligence that manages the electricity grid, or bring down the air traffic control system, the level of resulting chaos could exceed that resulting from a nuclear attack on a few cities and defense installations. It is right to worry about this and to take steps to mitigate the threat.

But, too often, the terrorism experts do little beyond wringing their hands about the limited power of governments to control the Internet. Implicitly, they yearn for a return to the technological environment of the mid-1950s, when a cozy relationship between intelligence agencies and one telephone company, one domestic telegraph company, and a handful of international cable carriers was all governments needed to keep an eye on things and, occasionally, to disrupt communications tying potential attackers together.

⁴³⁶ See Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 74 (2010).

It is likely that focused public relations campaigns can shift public opinion to favor more controls on the Internet and a relaxation of the legal barriers to eavesdropping. Not only that, but some of the boundaries that have historically restricted some types of eavesdropping more than others—access to the content of communications, as opposed to communications transaction date—are becoming less relevant. The enormous amount of transactional data now available that reveals location, communications patterns, and web browsing histories present a new opportunity for traffic pattern analysis that rivals access to content in what it reveals about individual activities and intentions.⁴³⁷

CONCLUSION: APPLYING THE LESSONS LEARNED: ROLE OF LAW, INNOVATION,
MARKETS, DISPUTES

The Internet's success has validated the central features of its constitution, embodying important ideologies that define Western society: the efficiency of market-based competition in allocating resources, and the power of grassroots democracy. Human rights have benefitted.⁴³⁸ Human rights abuses are more likely to come to the attention of those who can do something about the violations. Grassroots democratic movements are more possible. The individual freedom that comes with being able to start one's own business, perform music for the masses, or tell stories through books or movies enjoys a new life.

Markets and democracy have been newly empowered by the Internet's decentralized architecture and its global scope. The smallest entrepreneur can specialize in what he knows best and rely on others to perform other necessary functions, linking all the inputs together through standardized interfaces and protocols. The weakest voice has an enormous megaphone represented by the World Wide Web.

Competition and democratic discourse, however, have always threatened established orders and elites. When new technologies increase, both motive and means exist to block or divert the new technologies. This may occur through changes in the content of the law or its enforcement mechanisms, as manifested by the efforts of large copyright owners to broaden liability for infringement, some successful, some not yet successful. It also may occur by economic or social pressure brought to bear on institutions controlling key bottlenecks, as in the case of rightsholders pressuring ISPs to throttle traffic that they perceive as facilitating infringement.

The best public policy is one that recognizes the harmful potential of new regulation of the Internet, made more likely by the asymmetry of political power favoring established institutions. At the same time, legal initiatives may be appropriate

⁴³⁷ See *supra* Part II.B (discussing behaviorally targeting advertising).

⁴³⁸ See Rhoda E. Howard-Hassmann, *The Second Great Transformation: Human Rights Leapfrogging in the Era of Globalization*, 27 HUM. RTS. Q. 1, 38–40 (2005) (discussing human rights growth, generally, in the twenty-first century).

to restrict the exercise of private power that can be as harmful as undue regulation. Telling the difference is hard; advocates for blocking competition can always dress up their campaigns as effort to block the exercise of private power they characterize as harmful to the public interest.

A growing source of private power is that of proprietary empires.⁴³⁹ Big intermediaries are drawn into regulatory roles because they represent bottlenecks where it is relatively easy to regulate the conduct of people at the edge of the Internet. Whether and how these private regulators are subject to the constraints of due process is an important question of Internet policy.⁴⁴⁰

Governmental regulation may be more transparent and have more features of due process than private regulation, especially when private regulation is implemented through technological measures that automatically determine a “violation” of “rules” and automatically impose penalties such as excluding a user from Internet resources.⁴⁴¹

Developing new legal responses should follow the course that law usually has taken in the Anglo-American tradition: lawmakers should not try to anticipate what will happen in the marketplace. Rather, they should wait and see which entrepreneurs succeed and which fail; they should wait for consumers to decide what is the next new thing. Then, they should wait a while longer to allow actual disputes to emerge, disputes significant enough for the disputants to sue each other. Then, they should allow the courts to resolve the disputes by adapting well-established legal principles. Only when the pattern of judicial decisionmaking seems to have gone awry should legislators intervene. This has been the course generally followed in connection with the Internet, and it has been successful.

⁴³⁹ See, e.g., Henry H. Perritt, Jr., *Economic and Other Barriers to Electronic Commerce*, 21 U. PA. J. INT’L ECON. L. 563, 566 (2000).

⁴⁴⁰ See *id.* at 576–80 (identifying different categories of intermediaries, assessing the source of their enforcement power, and possibilities for imposing due process obligations).

⁴⁴¹ See Henry H. Perritt, Jr., *Lawrence Lessig, Code and Other Laws of Cyberspace*, 32 CONN. L. REV. 1061 (2000) (reviewing LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999)).