1999

Application-Centered Internet Analysis

Tim Wu
Columbia Law School, twu@law.columbia.edu

ESSAY

APPLICATION-CENTERED INTERNET ANALYSIS

Timothy Wu[*]

THERE is a now-standard debate about law and the Internet. One side asserts that the Internet is so new and different that it calls for new legal approaches, even its own sovereign law. The other side argues that, although it is a new technology, the Internet nonetheless presents familiar legal problems. It is a battle of analogies: One side refers to Cyberspace as a place, while the other essentially equates the Internet and the telephone.

In my view, these two positions are both wrong and right: wrong in their characterization of the Internet as a whole, yet potentially right about particular ways of using the Internet. The real problem is that both sides (and indeed, most legal writing) rely on a singular model of the Internet. They take one way of using the Internet as a proxy for the whole thing and conclude "the Internet this" or "the Internet that."

In earlier times, this simplification worked. Then, the Internet was new and less diverse. But today, most noticeably for purposes of legal analysis, the singular model is failing. In actual usage, on which legal questions usually turn, the Internet does not generalize well. The Internet is only the genus, the application, the species; applications can and do vary dramatically. To the user, the Internet comes in many incarnations—email, the World Wide Web, ICQ,[1] and more. A singular model of Internet usage has become too small to capture the dramatic diversity of today's Internet.

---

[*] Clerk to Justice Stephen Breyer, Supreme Court of the United States, 1999–2000. J.D., Harvard Law School, 1998; B.Sc., McGill University, 1995. The author would like to thank Larry Lessig for providing very helpful feedback and the opportunity to develop these ideas; Israel Friedman, Jack Goldsmith, Richard A. Posner, Eric Posner, Robert Sitkoff, and Polk Wagner for extremely helpful comments and suggestions; and the members of the Dirksen Paper Talk Group, where this Essay was first presented.

[1] For a description of ICQ, see infra note 103.

Accordingly, I would like to suggest an upgrade. For most purposes, I think we ought to discard the old talk of the Internet as a whole, for the whole Internet is rarely an appropriate level on which to generalize. Instead, legal thinking can better focus on where the variation that is apparent to the user is actually found: the application layer above the Internet's basic protocols. We need, I think, to focus on the user, not on the network, and that means legal analysis that begins with the application.

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

The crucial point to understand is that the Internet was expressly designed to put the application in charge. (Importantly, by this I mean the application, broadly conceived—the programs themselves (e.g., email, telnet, browsers, etc.) and their associated protocols; in other words, everything above the basic Internet standards.) The Internet, like many networks, has a layered architecture. That is to say, all the tasks necessary to communicating via network are divided among several functional layers, and the programs residing on these layers cooperate in standardized ways. Applications and their associated protocols occupy a layer above the basic Internet protocols that supervise basic data transmission. And so we can see that the designers of the Internet had a real choice about where to place the functionality of the network—how much freedom to give to the application and how much control to maintain through the low level protocols. The monumental choice—expressed famously as a design principle in Jerome Saltzer, David Reed, and David Clark's "end-to-end" design argument[2]—was to make the basic Internet protocols simple, general,

[2] Jerome H. Saltzer et al., End-to-End Arguments in System Design, 2 ACM Transactions in Computer Systems 277 (1984), *reprinted in* Innovations in Internet-

and open, leaving the power and functionality in the hands of the application. As a recent comment by the same authors explains, "Moving functions and services upward in a layered design, closer to the application(s) that use them, increases the flexibility and autonomy of the application designer to apply those functions and services to the specific needs of the application."[3] The impact of the end-to-end design principle, embedded in the architecture of the Internet, is crucial to any analysis of the Internet, and legal analysis is no exception.

To understand this point, just think of the "network" of appliances in your home: They all use the same standard of electricity (the basic protocol), but then widely differ in what they offer the user. A television offers something quite different than the power saw, even though both use 110 volts of electricity. This is the result of a deliberate choice. The design of the electricity "network" puts most of the power to decide functionality in the hands of the appliance designer. The Internet, conceptually, is not all that different. Contrast this with the telephone network, where nearly everything that matters about the telephone comes from the basic standards to which all telephones adhere. The difference between these networks is the result of a deliberate and important decision, and one that cannot but have a decisive impact on the legal analysis of any network. The Interlude between Part I and Part II explains these points in greater detail.

---

working 195 (Craig Partridge ed., 1988). "End-to-end" arguments are referred to as such because they recognize that a class of functions can only be completely and correctly implemented by the applications at each end of a network communication; hence, delegation of this function to lower protocols will generally be redundant. Put another way, end-to-end design arguments recognize that building complex functions into lower levels of a network implicitly optimizes the network for one set of uses but may then increase the costs of the network for uses that were unpredictable or unknown at the time the network is designed. The end-to-end design principle is featured prominently in the helpful summary of "Architectural Principles of the Internet" in RFC ("Request for Comments") 1958 (visited July 13, 1999) <http://www.faqs.org/rfcs/rfc1958.html>; see also infra notes 74–77 and accompanying text (discussing the end-to-end design principle).

[3] David P. Reed et al., Active Networking and End-To-End Arguments, 12 IEEE Network 69, 70 (1998).

The purpose of this Essay is to encourage a legal analysis that is more cognizant of the effects of the Internet's network architecture. That architecture provides, and even encourages, a rich and diverse universe of possible applications, foreclosing simple generalization of the Internet as a whole. For this reason, much legal analysis ought usually begin at the level of the Internet's individual applications, and not at the level of "Cyberspace." What this ultimately means is an analysis that focuses on the user, and how the Internet actually appears to the user, rather than an abstract focus on the network as a whole.

This richer focus on Internet usage makes things a little more complicated. Therefore, the second purpose of this Essay is to suggest coherent ways to think about and to classify the parts of the Internet—to dissect in legally relevant ways the universe of existing and possible Internet applications. Sometimes it makes sense to look at applications individually; other times, applications can be grouped by functional characteristics or by adherence to certain protocols; and in certain cases every application that adheres to the Internet's standards will be affected similarly, making an analysis of the whole Internet reasonable. I suggest two tools for grouping applications in this Essay that correspond to two main areas of Internet law, though the field for grouping applications is open.

Two main areas where the law and the Internet have met—proxies for public and private regulation questions, respectively—demonstrate the great difference that an application-centered analysis makes. Part I considers the First Amendment analysis of the Internet, a discussion that stands as representative for any issue of public regulation of the Internet. Part II brings application-specific methods to the now-historical debate over whether some form of strong self-governance makes sense for the Internet. This discussion, in turn, is representative of questions of private, contractual regulation of the Internet.

* * * * *

Two years ago, in *Reno v. ACLU*,[4] the Supreme Court announced that the Internet receives full First Amendment protection.[5] This proclamation was a tremendous victory; so phrased it tells us that everything at the application level—email, the World Wide Web, Usenet,[6] and "finger"[7]—will receive the most exacting judicial attention. But our enthusiasm ought be realistic. Sooner or later, because these applications (your browser, email, and so on) vary quite dramatically from a functional perspective, *Reno*'s one rule for the entire Internet may begin to lose its luster and perhaps feel ridiculous. The great variation among Internet applications is hard to fit into one First Amendment box. Just as there is no argument that electricity compels similar treatment of the television and the fax machine under the First Amendment, treating every Internet-adherent application as part of a single domain of First Amendment analysis can look a little farfetched.

For an illustration of the problem with the *Reno* simplification, look no further than your email inbox. *Reno v. ACLU* tells us that "'[c]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden.'"[8] But this is only true of some applications. Junk email is invasive in ways that the World Wide Web is not, and hence *Reno*'s simplified treatment of the Internet has little resonance for anyone who suf-

---

[4] 521 U.S. 844 (1997).

[5] See infra Section I.A.

[6] "Usenet" is the name of the largest "discussion group" accessible by the Internet. It consists of electronic bulletin boards devoted to specific topics, where users, using a specific program (a "news reader" client), may read postings or make their own contributions. Usenet and electronic bulletin boards were a dominant feature of the Internet and other networks in the 1980s and early 1990s, but the advent of the commercialization of the Internet and the rise of the World Wide Web have left much (though not all) of Usenet a burnt-out shell full of crass solicitation. There is no shortage of historical studies on this 20-year-old application. See, e.g., Michael Hauben & Ronda Hauben, On the Early Days of Usenet: The Roots of the Cooperative Online Culture (visited July 13, 1999) <http://www.firstmonday.dk/issues/issue3_8/chapter10/index.html>; Tim North, The Internet and Usenet Global Computer Networks (1994) <http://www.vianet.net.au/~timn/thesis/index.html>.

[7] "Finger" is an Internet-compliant application that allows the user to look up the vital stats of another Internet user. Its name is metaphorical: One "fingers" an address in the Internet "white pages."

[8] *Reno*, 521 U.S. at 869 (quoting ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996)).

fers under an invasion of thousands of "get rich quick" schemes (and worse) in their inboxes. When a serious constitutional challenge is made to junk email legislation, it seems inevitable that a reduced level of constitutional scrutiny for email will follow, justified, ultimately, by its invasive nature. And this suggests an easy, if rough, principle for classifying Internet applications for First Amendment purposes. Privacy-invasive applications that deliver content unbidden—most often, "push" applications—should merit reduced First Amendment scrutiny. Yet noninvasive applications—usually "pull" applications that rely on the user to go out and select content—fit *Reno*'s conception of a noninvasive Internet and the analysis that follows.

The distinction between push and pull applications is just an example. The point is that Internet applications vary too greatly to be grouped within one single First Amendment category. And similar overly simplified analysis of the Internet is a problem not only in First Amendment case law, but in much Internet scholarship. Finally, when it comes to debates over filtering, PICS,[9] and similar issues, the effects of the Internet's current network architecture ought not be overlooked.

* * * * *

The discussion in Part II addresses the unusually choleric academic debate surrounding two questions—whether Cyberspace is a "place" and whether it should have its own laws. This debate has reverted to its origins—it has become purely academic, a curiosity of early Internet legal history. Courts and governments have not been shy to exercise jurisdiction over Internet transactions. That, and a lack of any real demand for a general online adjudicatory authority, have scuttled dreams of a Cyberspace nation. But the topic remains of interest. For while Cyberspace, as some sort of imaginary kingdom, is not much more than farcical as a jurisdiction, there are nonetheless places on the Internet where private regimes do exist, and deference to their waiver of real-space rules has some cogency.

---

[9] "PICS" stands for "Platform for Internet Content Selection." For a discussion of PICS, see infra note 62.

Again a focus on the application—and the differences between applications—makes all the difference. A few applications (though not many) are utterly unconcerned with real-space goals, and rarely, if ever, have real-space effects—call them the "Internet as an end." The pure examples are multi-player video games and those online worlds called MUDs ("Multi-User Dungeons").[10] For these kinds of private groups, the normative argument for a private set of rules is strong, just as for any private group in the real world. This is not to say that *mandatory* rules would not be imposed should, somehow, real-space consequences accrue—a conspiracy made online should enjoy no immunity from prosecution. But just as the National Hockey League sets the penalty for "tripping," there is no reason to preempt some similar kind of private order among these groups.

Most Internet applications, however, are used simply as a "means" to do exactly what one wanted to do anyhow. When I buy my train ticket by packet rather than by dial tone it seems ludicrous to imagine that I suddenly become exclusively subject to some strange Cyberlaw. This "ends/means" distinction—although general and very far from infallible—provides guidance as to when any talk of a private order will make any sense at all. And the answer is that outside of a few, game-like examples, it almost never makes sense to speak of a Cyberspace sovereignty that ought normatively to be immune to real world jurisdiction.

The larger point is that thinking about the Internet as a homogenous whole leads quickly to extreme results, usually stemming from the choice of an analogy that only makes sense for one application. And the same absurdity will often be true of regulation conceived with one application in mind, yet then applied to the entire Internet. For a future likely to be full of new and even more divergent applications, it would be best to effect a hasty disposal of this old, one-size-fits-all way of thinking.

---

[10] For an explanation of MUDs, see infra note 86.

I. WHEN THE INTERNET MET THE FIRST AMENDMENT: PUBLIC INTERNET REGULATION

A

In 1997, the Internet met the First Amendment,[11] and the result of this encounter was the launch of a new rule. In case you are not already well-acquainted, here it is:

"The Internet Gets Full First Amendment Protection."

A great victory, this was, and quite a good rule (especially if the only choice were between it and its logical opposite, "The Internet Gets No First Amendment Protection"). But euphoria ought not blind us to *Reno v. ACLU*'s limits. The spirit and the political message of *Reno*—a reprimand of broad and hastily conceived Internet laws—may prove more significant and lasting than its content. We may come to remember the mid-1990s as a crucial and dangerous time for the Internet's development, a time where strong medicine was needed to control government hysteria.[12] But as a lasting First Amendment principle, the *Reno* rule makes a poor bet, for it groups into one constitutional box a huge range of highly variable Internet usage, and this cannot last forever.

A source of this overinclusive approach is the common generalization, echoed by the Supreme Court, that the Internet is a "medium." Not an unreasonable generalization for a new manner of transmitting information, perhaps, but in the world of the First Amendment the word "medium" carries serious consequences. It is used to draw a line around a group of ways to communicate and to proclaim that a given level of constitutional scrutiny will apply *there*.[13] And so we find, for example, that broadcast radio is a First

---

[11] See Reno v. ACLU, 521 U.S. 844 (1997). A new round of litigation has just begun following the passage of the Child Online Protection Act ("COPA"), a scaled-back version of the Communications Decency Act ("CDA") whose application is limited to commercial purposes, the World Wide Web, and material that is harmful for minors. See 47 U.S.C.A. § 231(a)(1) (West Supp. 1999); infra note 18 (discussing COPA and the current litigation concerning it).

[12] Cf. Dan M. Kahan & Tracey L. Meares, Foreword: The Coming Crisis of Criminal Procedure, 86 Geo. L.J. 1153 (1998) (arguing that the criminal procedure regime erected in the 1960s was a necessary response to the institutionalized racism of that period but one that has largely outlived its utility under current conditions).

[13] This function is similar, in some respects, to judicial delineation of the boundaries of a given public forum. See, e.g., Chicago Acorn v. Metropolitan Pier and Exposi-

Amendment medium, that cable television is a First Amendment medium (different from broadcast television), and that even snail mail[14] can be thought of as a First Amendment medium. All that this means is that every way of communicating encompassed, for example, by the phrase "cable television" gets the same treatment under the First Amendment.

Yet this First Amendment meaning of the word "medium" makes an exceptionally poor fit for the full range of existing and possible Internet applications. A radio is pretty much a one trick pony—a good trick, yes, but in essence there's only one way a person can use a radio. But the Internet, to understate the obvious, can be used in more than one way. Indeed it can even be used just like a radio, telephone, or television—used to replicate the functional characteristics of the existing "media" and then some.[15] If these "media" each merit their own special constitutional consideration, how can the Internet, capable of replicating all of these media and adding some for good measure—be handled by one simple paradigm? The constitutional meaning of "medium" is too small for the Internet. It has outgrown its box.

At the level of case analysis, this problem manifests in a mischaracterization that clouds *Reno*'s analysis. *Reno* relied on the district court's finding that "the Internet is not as 'invasive' as radio or television.... 'Communications over the Internet do not 'invade' an individual's home or appear on one's computer screen

---

tion Auth., 150 F.3d 695 (7th Cir. 1998) (dividing Chicago's Navy Pier into various levels of constitutional scrutiny based on public forum analysis). Indeed, it would be quite plausible to have had the entire initial argument over the First Amendment and the Internet assume the cast of a public forum argument. This has not happened, and, as it stands, neither the Supreme Court nor any federal appeals courts have put the Internet and public forum in the same paragraph. So while it seems a little uncertain whether public forum will ever catch on for Internet analysis, as David Goldstone reminds us, "Rome's forums were not built in a day; cyberspace's will not be either." David J. Goldstone, A Funny Thing Happened on The Way to The Cyber Forum: Public vs. Private in Cyberspace Speech, 69 U. Colo. L. Rev. 1, 4 (1998) [hereinafter Goldstone, A Funny Thing Happened]; see also David J. Goldstone, The Public Forum Doctrine in the Age of the Information Superhighway (Where Are The Public Forums on The Information Superhighway?), 46 Hastings L.J. 335 (1995) (earlier work on the same topic).

[14] That is, regular mail—"snail-like" as compared to electronic mail.

[15] Granted, some of this replication is not so great—especially what I am calling "television"—but the functional features are the same.

unbidden. Users seldom encounter content 'by accident.'"[16] Yet the example of junk email—a terrible and unbidden nuisance—shows that this characterization of the Internet is incorrect, for junk email *does* arrive unbidden and *does* invade a user's inbox.[17] And yet this characterization was apparently critical to Justice John Paul Stevens's conclusion that the Internet (as a whole) was not to be subject to any reduced First Amendment scrutiny. In reality, the invasiveness of the Internet cannot be ascertained at the level of the entire Internet. Rather, the question must be answered at the application level, for some applications are privacy-invasive, and some are not. Praise is due for the first Internet decision of our time, a step in the right direction, but praise ought not blind us to its limits.

So the *Reno v. ACLU* rule looks to be an overgeneralization.[18] But then it is not particularly unusual or unreasonable for case law to begin with an overinclusive or underinclusive rule and then to clarify matters later.[19] It seems only a matter of time before the Internet ceases to be considered as a single, uniform domain of First Amendment scrutiny.[20] Such things are hard to predict, but perhaps the setting for this change will be the first constitutional

---

[16] *Reno*, 521 U.S. at 869 (quoting ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996)).

[17] The statement of facts describing the Internet does talk about email, see id. at 851, but the opinion rests its scrutiny-level analysis on facts that are only true of the World Wide Web, i.e., that nothing appears without the user seeking it and that the user is seldom surprised by unexpected content. See id. at 868–70.

[18] It is doubtful that the latest round of Internet-indecency litigation will challenge this oversight, as COPA was written to apply only to the World Wide Web. See 47 U.S.C.A. § 231(a)(1) (Supp. 1999). So far COPA has been held unconstitutional. See ACLU v. Reno, 31 F. Supp. 2d 473, 476–77 (E.D. Pa. 1999).

[19] Other, non–First Amendment, decisions have been far more application-specific. See, e.g., Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (holding that the use of Compuserve's servers to send junk email without consent is trespass to chattels).

[20] Much of the debate between the rule in *Reno v. ACLU* and what I propose is reflected in the exchange between Justice Stephen Breyer and Justice Anthony Kennedy in Denver Area Educational Telecommunications Consortium, Inc. v. FCC, 518 U.S. 727 (1996). Justice Kennedy supports the adoption of a categorical, all-encompassing approach to the First Amendment, see id. at 780, 784–87 (Kennedy, J., concurring), while Justice Breyer prefers a narrow, hesitant, and technologically specific approach, see id. at 739–44 (Breyer, J., plurality opinion); see also id. at 774–78 (Souter, J., concurring) (rejecting Justice Kennedy's position, chiding, "First, do no harm.") (internal quotation marks omitted).

challenge to the regulation of email (provided a technical or economic solution does not preempt a legal rescue). *Reno*'s assurance that "The Internet Gets Full First Amendment Protection" can look pretty thin when there are 49,000 new messages in your inbox, or when your so-called cyberlife consists of deleting ads for pyramid schemes and porn sites. Nearly everyone hates junk email, even cyberlibertarians (although many take comfort in their superior filtering skills), and there is a pretty simple reason why: Junk email is invasive and offensive. Sound familiar? Indeed, spam[21] may turn out to be "the seven dirty words" of the Internet;[22] in its wake, the monolith that now constitutes Internet First Amendment analysis will witness its first partition.[23]

---

[21] Spam has become a generic term for unwanted content, although it is most frequently used (as here) as a synonym for junk email, typically unwanted solicitations of a salacious or illegal nature. For more on spam, and the many campaigns organized to fight it, see Scott Hazen Mueller, Fight Spam on the Internet <http://spam.abuse.net/> (visited July 13, 1999), and the Coalition Against Unsolicited Commercial Email ("CAUCE") <http://www.cauce.org> (visited July 13, 1999) [hereinafter CAUCE website] ("Take Back Your Mailbox"). The topic of how exactly to fight spam is interesting because it is an open question and something of a race of the modalities of regulation. Will law, the market, social norms, or a technological approach ("the code") be the best weapon for killing spam? External social sanctions were tried first, but they seem to have little effect on the people behind spam, the "cyberpromoters" of the world. Technological solutions have been proposed and implemented: Some people filter, and on Usenet, exotic solutions such as "cancelbots" (robots that find spam postings and delete them) have been popular. The market, combined with social sanctions, may have the final say. See Christopher Jones, Marketers Losing Taste for Spam, Wired News (Nov. 12, 1998) <http://www.wired.com/news/news/business/story/16216.html>. Finally, there is always talk of federal legislation, such as an amendment to the federal "junk fax" law. See, e.g., H.R. 1748, 105th Cong. (1997). Some states, including Nevada, Washington, and California, have actually passed such legislation, although the approaches taken by these states vary. See, e.g., Cal. Bus. & Prof. Code §§ 17511.1, 17538.4, 17538.45 (West 1997 & Supp. 1999); Wash. Rev. Code §§ 19.190.020, 19.190.030 (West 1999). Groups such as CAUCE oppose the type of legislation that merely imposes labeling requirements (such as the California law) to such a degree that they plan to challenge it as compelled speech. See CAUCE website, supra. Obviously, junk email is not a problem ideally handled at the state level; any federal legislation, if or when it is passed, will preempt the state legislation.

[22] Cf. FCC v. Pacifica Found., 438 U.S. 726 (1978) (upholding the possibility of sanctioning George Carlin for his monologue on "the seven dirty words").

[23] For an example of this kind of partition making, see Chicago Acorn v. Metropolitan Pier and Exposition Authority, 150 F.3d 695 (7th Cir. 1998), where the Seventh Circuit carefully divided Chicago's monolithic Navy Pier into several zones of differing First Amendment scrutiny.

If junk email legislation is seriously tested, email will likely be found a fitting place to apply intermediate scrutiny, a balancing test, or an equivalent formula, stemming from a conclusion that regulation of email is justified as a content-neutral time, place, and manner restriction;[24] or that there exists a captive audience,[25] or perhaps even that junk email is commercial speech.[26] Perhaps in their consideration of such a case, courts will rely directly on *Rowan v. United States Post Office Department*,[27] which allowed the state to facilitate the filtering of real mail.[28] Courts might even say that email is a "medium" or "modality" different from the World Wide Web that merits different First Amendment treatment.[29] In the absence of a real case it is hard to say which litigation strategy will work best, but it is the result, and the reason behind the result, that matters here. Email spam is invasive, just like real mail is invasive,[30] incoming calls are invasive,[31] abortion picketing outside your front door is invasive,[32] and so on. The underlying reasoning is important because it lets us forecast the future of the Internet and the First Amendment.

B

The example of junk email suggests a way to group Internet usage (and applications) for First Amendment purposes. By this grouping, I want to specify what we can say, ex ante, based on the technology *alone*; for of course, in individual cases, the content of the speech (indecent speech, for example) will make a difference. I think scrutiny will and should split in accordance with the invasion of privacy attendant to usage, and this, of course, depends on the

---

[24] Cf. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (explaining the time, place, and manner analysis).

[25] Cf. Frisby v. Schultz, 487 U.S. 474, 487 (1988) (explaining the captive audience doctrine).

[26] Cf. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 563 (1980) (explaining the commercial speech doctrine).

[27] 397 U.S. 728 (1970).

[28] See id. at 737–38.

[29] Cf. Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 637–40 (1994) (treating cable and broadcast television as different First Amendment media).

[30] See *Rowan*, 397 U.S. at 737–38.

[31] See Gormley v. Director, Conn. State Dep't of Probation, 632 F.2d 938, 942 (2d Cir. 1980).

[32] See Frisby v. Schultz, 487 U.S. 474, 484–85 (1988).

application being used. This yields a basic and unsurprising split between privacy-invasive and nonprivacy-invasive speech on the Internet, which can be mapped to invasive and noninvasive applications.

The Supreme Court has a collection of "special reasons" to justify reduced scrutiny for a given "medium." Some, like a history of extensive government regulation[33] and a scarcity of available frequencies,[34] have little relevance to the Internet. Yet another justification, stated usually as a communication's "invasive nature,"[35] has teeth, for this justification stands directly at a collision between a recognized individual right and the First Amendment. People like their privacy, and the Supreme Court, perhaps eager to please, recognized a right to privacy.[36] And the data compiled in the United States Reports shows us that when these two rights face off, the First Amendment usually comes out the loser.[37] This is particu-

---

[33] See, e.g., Red Lion Broad. Co. v. FCC, 395 U.S. 367, 399–400 (1969) (relying on the spectrum scarcity of broadcast television to justify reduced scrutiny).

[34] See id.; see also Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 637–39 (1994) (noting the inapplicability of the scarcity rationale in the context of cable).

[35] See, e.g., FCC v. Pacifica Found., 438 U.S. 726, 748–50 (1978) (stating that broadcast radio is invasive and accessible to children).

[36] See Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965).

[37] For Supreme Court cases in which the First Amendment lost out to asserted privacy interests, see Kovacs v. Cooper, 336 U.S. 77 (1949) (sound trucks); Rowan v. United States Post Office Department, 397 U.S. 728 (1970) (unsolicited mail); FCC v. Pacifica Foundation, 438 U.S. 726 (1978) (radio broadcast to the home); and Frisby v. Schultz, 487 U.S. 474 (1988) (focused picketing of a certain house). For cases in the lower courts, see Gormley v. Director, Connecticut State Department of Probation, 632 F.2d 938, 942 (2d Cir. 1980) (harassing phone calls); Destination Ventures v. FCC, 46 F.3d 54 (9th Cir. 1995) (junk faxes); and Moser v. FCC, 46 F.3d 970 (9th Cir. 1995) (telemarketing). For the only instances in which the First Amendment has really won invasion-of-the-home cases, see Martin v. Struthers, 319 U.S. 141 (1943) (distinguished endlessly—see, for example, Frisby v. Schultz, 487 U.S. 474, 485 (1988)), and, more significantly, the publicity cases. See Florida Star v. B.J.F., 491 U.S. 524 (1989); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975); Time, Inc. v. Hill, 385 U.S. 374 (1967). These cases show that privacy interests, while formidable, can still be taken to task by the real heavyweight champion of First Amendment case law, the media defendant (especially when he asserts the "public's right to know"). See, e.g., Richmond Newspapers v. Virginia, 448 U.S. 555 (1980) (media's right to open trials). But two other cases, Erznoznik v. City of Jacksonville, 422 U.S. 205, 210–11 (1975), and Cohen v. California, 403 U.S. 15 (1971), reinforce the focus on privacy, holding that when someone is out for a drive or wandering around the courthouse, privacy claims do not hold water and one needs to avert her gaze. For a nice overview of much of this unsavory business, see Michael W. Carroll, Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations, 11 Berkeley Tech. L.J. 233 (1996).

larly true when the right to privacy enjoys the home team advantage: Annoying people in their homes is a cardinal sin in the world of the First Amendment. The Supreme Court becomes likely to say things like "protecting the well-being, tranquility, and privacy of the home is certainly [an interest] of the highest order in a free and civilized society."[38] As the sound trucks, ride-along journalists, and bulk mailers of the world operate under a serious First Amendment handicap, so will their equivalents in Cyberspace.

This perennial tension between privacy interests and the First Amendment seems destined to play a starring role in the story of Internet regulation. And since the Internet, as a whole, cannot be branded privacy-invasive or noninvasive, the distinction has to be made where the variability lies: the application. The tension between these two big rights seems likely to play out in a distinction between applications that in usage are privacy-invasive and those that are not.

This conclusion really only poses the question: Which applications are privacy-invasive and which are not? Luckily, we are not without guides. Internet users like to use the words "pull" and "push" to distinguish between content that you "go and get" and that which "arrives unbidden."[39] And while hardly a perfect division, it serves as a rough proxy for which types of Internet applications are privacy-invasive and which are not. Even though everything "enters the home" (if your computer is at home), pull materials by definition come bearing your specific invitation. That is, because a user actively "goes out and visits" websites, when he clicks on "The Starr Report," the consequences ought be no surprise. So pulled material *cannot* be invasive, the argument goes, because the invasion is consensual, and an invasion of privacy requires a lack of consent. The idea is similar to the tort law principle that consent negates liability for invasion of privacy.[40] Push applications, on the

---

[38] Carey v. Brown, 447 U.S. 455, 471 (1980) (dicta).

[39] Among major applications this breaks down roughly as follows: The World Wide Web (the HTML portions at least), Usenet, telnet, talk, and similar programs are pull, while email, push channels, and most media streamers are push. But this is far from a perfect dichotomy—consider, for example, when you click on a media streamer from within the World Wide Web. The distinction is a starting point more than the final word.

[40] See Restatement (Second) of Torts § 892B (1977); id. cmt. c, illus. 1 (demonstrating that consent cures trespass liability).

other hand, by definition, deliver materials *without* your specific consent, as most email users (and all America Online ("AOL") users) well know. You do "set up" an email address or a push channel, but only in the most meaningless way imaginable does *that* mean you intended to consent to "Mr. Barlow has 15,308 new messages."

This guide does not give all the answers. Reasonable people can spend a long time disagreeing over what "consent" and "privacy" really mean on the Internet; whether custom and common understandings can play a role; whether, for example, subscribing to a certain listserv[41] means you get everything you deserve, and whether the World Wide Web really *is* privacy-invasive because of the occasional surprises that it delivers (have you visited www.whitehouse.com[42] lately?) And it also misses out on some important invasions of privacy that are to be found outside of push applications. But it suggests a guide for regulation of existing and future Internet applications.

So what would a privacy-centered and application-specific First Amendment law for the Internet look like? The rule would be simple: Privacy-invasive technologies shall be subject to reduced First Amendment scrutiny. And the results would be as follows. Regulation of incoming junk email would be subject to reduced scrutiny, especially if directed at commercial junk email. Regulation of the various data "forms" on the World Wide Web (actually,

---

[41] A "listserv" (also called an "email exploder") refers to a discussion group that works over emails distributed to every member of a group. Listservs have a well-known but unfortunate tendency to degenerate into spiteful and lengthy personal spats between members, known as "flame wars." Since listservs operate by email, a subscriber may return from a weekend away and find her mailbox clogged with hundreds of messages full of all manners of personal invectives including, invariably, cheap comparisons of adversaries to various leaders of the Third Reich.

[42] <http://www.whitehouse.com> is a pornography site. Search engines and directories play an interesting role in all of this, as they frequently expose users to unexpected content. Note, for example, how a search for "AOL" in Yahoo turns up not only AOL's websites but also protest sites like "Why AOL Sucks" and "The AOL Haters Mecca." Indeed, search engine result pages are among the very few means on the World Wide Web by which small scale protest and dissenting voices actually reach the public. If public forum doctrine were functionally based rather than hopelessly linked to historical analysis then directory result pages might be called the World Wide Web's public fora.

CGI scripts[43]) that solicit personal information, and the treatment of that personal information, would also be balanced for reasonableness (especially when the solicitation is directed at minors). Similarly, all of the applications ancillary to the World Wide Web that process personal financial information for transactional purposes would be subject to intermediate scrutiny. Next, and perhaps obviously, any "speech" that involves an unauthorized invasion of another's system would be regulated, and indeed is already criminalized, under computer crime laws.[44]

At bottom, the issue that bothers people on the Internet is privacy invasion. People seem to want the help of their governments, and experience tells us that the First Amendment buckles when privacy interests are threatened.[45]

C

The Supreme Court's opinion in *Reno v. ACLU* is the most obvious example of overly general Internet First Amendment analysis. But the same problem tarnishes much of the voluminous academic attention given to this topic, limiting the value of this analysis.[46]

---

[43] "CGI" stands for "common gateway interface," and "CGI scripts" are miniature applications that can be associated with an HTML web page. The forms commonly used on the Internet to collect user information usually rely on CGI scripts to process the form and deliver the user's data to a host computer.

[44] See 18 U.S.C. § 1030 (1994).

[45] Unless fortified by the presence of a media defendant in the ring, that is. See supra note 37.

[46] For a representative sample of articles in which this oversight is obvious and explicit, see, for example, Robert M. O'Neil, Free Speech on the Internet: Beyond "Indecency," 38 Jurimetrics J. 617 (1998) (cataloging Internet First Amendment cases with little regard to application-level variation); Glen O. Robinson, The Electronic First Amendment: An Essay for the New Age, 47 Duke L.J. 899 (1998) (comparing, en masse, the electronic and print versions of the First Amendment); Mark S. Kende, The Supreme Court's Approach to the First Amendment in Cyberspace: Free Speech as Technology's Hand-Maiden, 14 Const. Comment. 465 (1998) (criticizing a posited abandonment of First Amendment principle in the face of technological development); Robert Reilly, Mapping Legal Metaphors in Cyberspace: Evolving The Underlying Paradigm, 16 J. Marshall J. Computer & Info. L. 579 (1998) (calling for an "organic" model of Cyberspace that would "view cyberspace as a place where a society of people exist"); Thomas G. Krattenmaker & L.A. Powe, Jr., Converging First Amendment Principles for Converging Communications Media, 104 Yale L.J. 1719 (1995) (envisioning a First Amendment doctrine essentially oblivious to context).

The problem can also be more subtle: It is when the Internet-wide assumptions are implicit that even the most careful analysis has gone astray. Consider, for example, that scholars studying speech on the Internet often take for granted that the Internet (as a whole) is a great equalizer for matters of speech. Writers, most famously Eugene Volokh, rest substantial portions of their analysis on the notion that the Internet is a ready medium of "cheap speech."[47] They are certainly correct that the minimal conception of the Internet as a connection between every networked computer does make many things cheaper for everyone. But, in reality, the idea that speech is cheap and that all speakers are equally heard

---

There are some notable exceptions to this generalization. Lawrence Lessig has been careful to distinguish among applications, famously cautioning against the all-encompassing analogy. See Lawrence Lessig, The Path of Cyberlaw, 104 Yale L.J. 1743 (1995) [hereinafter, Lessig, The Path]. Most recently, he has emphasized the distinction between push/pull and discriminatory/nondiscriminatory applications. See Lawrence Lessig, What Things Regulate Speech: CDA 2.0 vs. Filtering, 38 Jurimetrics J. 629 (1998) [hereinafter Lessig, What Things]. David Goldstone's careful search for public "cyber forums" on an application-specific basis is another exception. See David J. Goldstone, A Funny Thing Happened, supra note 12, at 1, 4. Finally, careful, code-specific thinking is also found in Andrew L. Shapiro, The Disappearance of Cyberspace and the Rise of Code, 8 Seton Hall Const. L.J. 703 (1998).

[47] See, e.g. Eugene Volokh, Cheap Speech and What It Will Do, 104 Yale L.J. 1805 (1995) (arguing that cheap speech enabled by the Internet will bring a much more democratic and diverse environment than we see now); Jerry Berman & Daniel J. Weitzner, Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media, 104 Yale L.J. 1619 (1995) (arguing that the Internet removes barriers to entry into the marketplace of ideas that previously interfered with full realization of the First Amendment's aims); Edward A. Cavazos, The Idea Incubator: Why the Internet Poses Unique Problems for the First Amendment, 8 Seton Hall Const. L.J. 667 (1998) (Internet lowers "speaker burden"); Robert Kline, Freedom of Speech on the Electronic Village Green: Applying the First Amendment Lessons of Cable Television to the Internet, 6 Cornell J.L. & Pub. Pol'y 23, 24–25 (1996) (maintaining that the Internet, by serving as "a wide-open, interactive frontier that has no central control figure" and by allowing low-cost speech "provides for the exchange of ideas on a massive scale on a variety of topics limited only by the human imagination"); Kathleen M. Sullivan, First Amendment Intermediaries in the Age of Cyberspace, 45 UCLA L. Rev. 1653, 1669–71 (1998) (studying the disintermediation in Internet communication while acknowledging that the relative equality of Internet speech is a feature of the present only); Lee Tien, Who's Afraid of Anonymous Speech? *McIntyre* and the Internet, 75 Or. L. Rev. 117 (1996); Fred H. Cate, Indecency, Ignorance, and Intolerance: The First Amendment and the Regulation of Electronic Expression, 1995 J. Online L. 5, ¶ 66 (Dec.) <http://www.wm.edu/law/publications/jol/cate2.html> (arguing that the structure of the Internet makes it an egalitarian medium where "the real test of expression and ideas is their own value, not the status or affiliation of their source").

increasingly depends on what application you are talking about. The World Wide Web is the deviant, for the impact of a message on the World Wide Web has already begun to depend heavily on the identity (that is, mostly the wealth) of the speaker. The impact of a website depends quite a bit on how good your web design (or web designer) is, what domain name you manage to get,[48] how many banner advertisements you can buy, and what kind of fancy plug-ins you can afford to support. (Indeed, media streamers like realplayer[49] may be the *most* "unequal" applications adhering to the Internet.) And as search engines inevitably begin to charge for "priority" listings, and heavy Java programming becomes increasingly standard, the impact of the stereotypical little person's site will likely continue to decrease. Add to this the increase in competition stemming from the great financial incentives of owning a high-traffic site, and the results look troubling for high-impact web-based cheap speech. This is not to say that there are not exceptions (with Matt Drudge's website serving as the archetype[50]) or that things have not changed, but that describing today's World Wide Web as a free and open forum of *equal* speech is a bit delusional.

These disparities do not hold true for forums like email listservs. On a successful listserv everyone still basically looks the same.[51] Everyone gets her turn, and the impact of a message is still more or

---

[48] Here, in addition to money, the ownership of a registered trademark makes a difference, because the owner of the registered trademark may challenge the "illegitimate" owner of that domain name. See, e.g., Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999) (senior trademark user granted preliminary injunction on junior user's use of trademark as domain name); Giacalone v. Network Solutions, Inc., No. C-96 20434 RPA/PVT, 1996 WL 887734 (N.D. Cal. June 14, 1996) (granting injunction in favor of trademark holder to prevent another from using domain name identical to that trademark); see also, e.g., Network Solutions' Domain Name Dispute Policy, Dispute Policy § (8)(a) (visited July 22, 1999) <http://www.jmls.edu/cyber/docs/dnpol3.html> (providing that owner of exactly matching trademark may challenge owner of domain name).

[49] Media streamers use certain clever algorithms to send live sound or video in real-time (i.e., without waiting for the entire file to download) whenever the viewer wants. The result, given present bandwidth constraints, is a good "pull" version of radio, but, at least for the present, is a very pale imitation of television's frame rate and picture size. For more information, see <http://www.realplayer.com> (visited July 13, 1999).

[50] Matt Drudge runs a famous gossip column of low budget yet high impact that can be found at <http://www.drudgereport.com/matt.htm> (visited July 13, 1999).

[51] It is true that email addresses can be more or less prestigious, but this is a minor point.

less correlated with the value (or lack of value) of what the speaker has to say rather than with her net worth. On a listserv, it is still true that no one knows you're a dog. This disparity between listservs and the World Wide Web proves a larger point: The lines of the application control the question of speech-equality, and it has become increasingly meaningless to speak generally of the Internet as a whole as a medium of equal speech. Scholarship that blindly brands the Internet or Cyberspace as this or that kind of place for speech is missing the point.

This is not to downplay the impact the World Wide Web has had on the way people get information. The disintermediation effects of the World Wide Web (speakers being able to reach listeners without the aid of intermediaries) are real,[52] although one ought to notice, parenthetically, that search engines are serious, if benign, controllers of the power of listeners to actually find speakers in the first place. The point is that these questions need to be sensitive to their application context and not projected on the Internet as a whole.

Lawrence Lessig, among writers, must be said to be particularly sensitive to the importance of the application; he urged the rejection of the single controlling analogy early on[53] and has continued to focus on differences in speech-vending technology as between applications.[54] Yet when it comes to one crucial, and favorite, topic—change in the architecture of the Internet—he downplays the saliency of application autonomy built into the Internet's architecture. Lessig tends to assume that change in the architecture of Cyberspace will affect all applications simultaneously and similarly. But for most purposes, it seems that few things (outside of a change in the fundamental protocols and cross-application technologies, considered below) would *necessarily* cause differing parts of the Internet to change at the same speed or in the same direction. This is a consequence of the layered architecture: The modular design generally allows applications to change independently of one another and the basic protocols. And I think it would be no surprise to find different parts of the Internet changing in different direc-

---

[52] On disintermediation, see Sullivan, supra note 47.

[53] See Lessig, The Path, supra note 46, at 1745–47.

[54] See, e.g., Lessig, What Things, supra note 46, at 644–45 (placing Internet applications into one of four categories based on push/pull and discriminatory/nondiscriminatory axes).

tions, in response to the different demands. Financial websites will never be big on user anonymity, but why a change to more secure online trading cannot coexist with the anonymous MUD culture is unclear to me. Instead, I think the more important the Internet becomes, the more one might expect diversity in the features of what it offers, as a reflection of the underlying demands of society.

But Lessig's arguments are deeper than this. He focuses on certain technologies—of which digital certificates[55] are the best example—with broad cross-application applicability. And such technologies, set up as an auxiliary to all usage of the Internet, could create a new baseline of regulability.[56] In the digital certificate example, if using robust digital self-identification became expected in every aspect of Internet usage, then the former default of a basically anonymous Internet would be replaced with an Internet where basic information is known.

And so, this kind of change is a real possibility. A change as fundamental as adding self-identification to every application operates at a level relevant to all Internet usage. But the possible and the probable are not the same thing, and it is important to notice some of the obstacles. To represent a wholesale change, there must be an agreed-upon standard that becomes a default requirement for all the major applications, so that users who wish to use the Internet need to obey the standard or face annoying transaction costs (the method of most regulation). Independent requirements are not the same—if your bank forces you to keep its implementation of digital certificate technology on your computer, this is a change, yes, and is even a net increase in Internet regulability, but it lacks the significance of an Internet-wide change. But setting up such a necessarily public standard presents collective ac-

---

[55] Digital certificates are a system, based on an underlying public key encryption technology, for robustly confirming the identity of the party with which you are transacting—a need most obviously pressing when the transaction is financial in nature. For more on digital certificates, see the ABA's Section of Science and Technology, Electronic Commerce Division, Information Security Committee, Digital Signature Guidelines (1996) (visited July 13, 1999) <http://www.abanet.org/scitech/ec/isc/dsgfree.html>; A. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Or. L. Rev. 49, 49 (1996).

[56] See Lawrence Lessig, Code, and Other Laws of Cyberspace 42–48 (1999) (unpublished manuscript, on file with the Virginia Law Review Association).

tion problems; the self-interests of private parties will mitigate toward proprietary technology. Such problems are of course solvable—but I think it is clear that the crucial question is whether government will take action.

Finally, the application-centered approach to thinking about the Internet is nothing so denigrating as the school of thought best described by its slogan: "the law of the horse."[57] The basic idea is that there is no real utility to the study of Cyberspace law as one field, in particular because (1) law professors do not understand computers ("the blind are not good trailblazers")[58] and (2) the best way to study specialized topics is to study general rules.[59] To the extent that the "law of the horse" moniker is a criticism of overly general Cyberspace writing, it echoes the ideas stated here. The problem with this school of thought is that it ignores the analysis and regulation that *does* make sense at the level of the whole Internet. The big picture is sometimes worth thinking about—the Internet, after all, can be thought of as nothing more than a global agreement to use the same information transmission protocols. For a network to be part of the Internet, it needs to "agree" to use the basic and open Internet protocols, and lawyers like nothing better than studying large agreements and their consequences.[60] Just as the Administrative Procedure Act anchors administrative law and the tax code anchors tax law, study of the Internet also works from a sufficiently general common denominator: the set of standards that define the Internet.[61]

---

[57] This is the moniker usually used to belittle overheated Internet scholarship. Its source is Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 U. Chi. Legal F. 207. For one thing, electricity was a great advance over the horse. See also Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach, 112 Harv. L. Rev. (forthcoming Fall 1999).

[58] Easterbrook, supra note 57, at 207.

[59] See id.

[60] Just consider all the time spent studying the agreement "to form a more perfect union."

[61] In addition, even though I urge that we have to be careful to think about the Internet in a technically rigorous and application-specific manner, there is a lot going on even within the confines of given applications. The World Wide Web and its myriad of associated applications are a big topic; as I said earlier, *Reno v. ACLU* is a great World Wide Web decision, and it seems there will be more to follow.

D

No discussion of the Internet/First Amendment tryst would be complete without some mention of the issues surrounding filtering and the Platform for Internet Content Selection ("PICS"). Filtering technologies generally allow users to block out unwanted content according to either a fixed database or self-set preferences (a preference system, of course, requires a standard rating system and actual rating of all the content on the Internet).[62] Filtering issues are at present mainly relevant to the two most popular Internet applications—email and the World Wide Web—although the concept and technology has relevance to future and other existing applications. There are two big questions in filtering. First, even without government involvement, whether labeling of all content under one standard will become the norm. Second, if the government does try to push filtering, whether its actions will be constitutional. What does an application-centered analysis tell us?

---

[62] PICS is of particular interest, and the following is a short introduction. For more thorough explanations of PICS technology, see Paul Resnick & James Miller, PICS: Internet Access Controls Without Censorship, 39 Communications of the ACM 87 (1996) <http://www.w3.org/PICS/iacwcv2.htm>; R. Polk Wagner, Filters and the First Amendment, 83 Minn. L. Rev. 755, 759–69 (1999) [hereinafter Wagner, Filters]; Jonathan Weinberg, Rating the Net, 19 Hastings Comm. & Ent. L.J. 453 (1997). PICS, as a format to facilitating labeling and, ultimately, filtration, has two distinguishing features. First, PICS itself is described as "value-neutral" because the content of the labels and the criteria by which filtration occurs are not specified by the PICS format itself. This, proponents claim, means that PICS can facilitate individual choice instead of circumscribing it—the user may choose the rating agency of his choice, as one might choose a movie critic. The second interesting feature of PICS is that it may be used at any level, or is "vertically neutral." Thus, a PICS-based filtration system may exist at the browser level, resident in software such as Internet Explorer or Netscape Navigator. It is equally at home, however, at the server level, and can be used to filter content available in an intranet or to the users of an Internet Service Provider ("ISP").

No legislature has yet acted to legislate any form of labeling or blocking system, although some state actors, of course, such as libraries, use blocking software. See Mainstream Loudoun v. Board of Trustees, 2 F. Supp. 2d 783, 787 (E.D. Va. 1998). At present there are different PICS-compliant labeling standards that enjoy varying levels of use. See, for example, Net Shepherd, which has its own standard, at <http://www.netshepherd.com> (visited July 13, 1999). There are also many less sophisticated blocking programs available that are designed mostly to protect children from viewing indecent conduct and allow some customization. See, for example, the programs available at <http://www.netnanny.com> (visited July 13, 1999); <http://www.safesurf.com> (visited July 13, 1999); and <http://www.cybersitter.com> (visited July 13, 1999).

First, notice that the incentive story differs by the type of Internet usage (i.e., application) at issue. The full picture of the incentives for every party to the filtering scene—content providers, users, Internet Service Providers ("ISPs"), rating sites—is complex. For our purposes it shall suffice to make a few observations. First, notice that content providers have little independent interest in self-labeling (but of course will respond to new incentives: If enough users, or ISPs, block out unrated content, by default, content providers will need to self-label to be heard). The onus, ultimately, to create self-labeling pressure, or public ratings, is on the users. But then which users are strongly interested in filtering depends on the usage in question. For an individual user—by this I mean someone using the Internet for herself—the utility of filters is in selecting desired content and avoiding unwanted content. Hence, filters are very useful for email and other invasive applications (like ICQ) because the user lacks many other methods for avoiding unwanted content. But the situation is quite different on the World Wide Web. For the Web, unlike email, there are powerful substitutes for achieving the goal of content selection. For example, on the Web, search engines are a better developed substitute to filtering technologies for getting what you want and avoiding what you do not. At a more basic level, that browsers put the decision of whether to download content in the user's hands means, basically, that the user can filter for herself. So in contrast to email or other invasive applications, the user in her individual capacity has little interest in World Wide Web filtering.

Web filtering, rather, is beloved of those who want to control what content is available to others. These are people like parents, libraries, companies, and governments—in other words, paternalists (though this is not meant in a pejorative sense). And for the Web, whether labeling of content will become the norm depends on the efforts of these paternalistic users. Yet two things make it unlikely that these users will either provide public ratings of the entire Web or try seriously to force individuals to self-label. First, a collective action problem lurks behind any provision (or compulsion) of a single, public set of ratings. That is, even for the listeners who want a single standard for filtering, it is rational to free-ride off of either the public ratings of others or the efforts of others to force content providers to self-label. Second, the availability of

private filtering services, based on private databases, may be a cheap and good enough substitute to erode the incentives of these users to devote efforts toward establishing a public rating system or enforcing self-rating. And it is perhaps these factors—the lack of an incentive among individual users, the collective action problem, and the appeasement effects of private database filtering services—that have stunted, and will continue to stunt, the emergence of a single, public, and free rating of the World Wide Web.

That is, unless it is government that makes things happen. The government has the power to push the architecture to an easily filterable World Wide Web, or even to the entire Internet. But, of course, when the government gets involved, so does the First Amendment. And then everything depends on two issues: (1) the type of action the government takes, and (2) the scope of Internet usage affected (in other words, which applications are subject to this type of regulation). The writing on this topic has focused on the first issue[63] and virtually ignored the second.

The second question, however, matters. Again, a split can be seen between invasive and noninvasive applications. If government limits its filtering legislation to facilitating the filtering of privacy-invasive applications (say, email), it will be far less likely to run into First Amendment problems. Of course, certain types of government action to regulate email will raise larger First Amendment questions under doctrines like the compelled speech doctrine.[64] But the point is that no matter what the government action is, it will have an easier case with a privacy invasion on its side. Whatever the exact constitutional theory turns out to be, cases from *Rowan v. United States Post Office Department*[65] onward have allowed the government to protect citizens against harassment and torment in their homes. It is hard to imagine why an email inbox

---

[63] See, for example, the thorough survey of governmental actions in Wagner, Filters, supra note 62, at 769–812, and ACLU, Fahrenheit 451.2: Is Cyberspace Burning?: How Rating and Blocking Proposals May Torch Free Speech on the Internet (1997).

[64] See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (holding as unconstitutional a requirement that campaign literature identify the speaker); Wooley v. Maynard, 430 U.S. 705 (1977) (holding as unconstitutional a requirement that citizens display slogan on license plate).

[65] 397 U.S. 728 (1970) (permitting the post office to facilitate user-directed filtration of real mail).

ought be much different. And so I think the various antispam bills floating around state and federal legislatures, banning or facilitating filtration of junk email, should survive First Amendment scrutiny if drafted properly.

Broad-based regulation that reaches the World Wide Web poses a harder question. Nearly everything depends entirely on what government actually does to "help out" filtering—each type of action leads to a different constitutional analysis.[66] And so it is fairly ridiculous to make the broad argument that PICS is or is not unconstitutional. A better prediction follows the golden rule that underlies First Amendment scrutiny (and constitutional scrutiny in general): The more indirect and indeliberate the government action, the better.[67]

A word, finally, on Lawrence Lessig and PICS. Lessig has not been the greatest fan of PICS. He has at one point urged a reincarnation (though not a resurrection) of the CDA as a kind of short-term sacrifice to solve the indecency problem without side-effects.[68] This concession might be no small sacrifice. Could such an avowedly mild-mannered standard really be so dangerous to all that is good about the Internet?

Lessig argues that filtration-facilitation by government would inexorably lead to a wholesale change in the Internet architecture, to an architecture that facilitates speech discrimination.[69] This is an important warning. Unintended, even awful, consequences could follow a theoretical model of coercive state-sponsored filtration—including a tip-over into a closed World Wide Web envirоument more reminiscent of the corporate Intranet model. This could be especially true if a PICS rating requirement, meant for end-user fil-

---

[66] See the sources cited supra note 63 for analyses of possible government action and attendant constitutional consequences.

[67] This conclusion is echoed by Wagner, Filters, supra note 62, at 812. On the point that constitutional scrutiny needs to be driven by governmental purpose, see, for example, Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) ("The government's purpose is the controlling consideration."); Edmond v. Goldsmith, No. 98-4124, 1999 WL 458618, at *6 (7th Cir. July 7, 1999) (governmental purpose behind roadblocks is essential to determining constitutionality).

[68] See Lessig, What Things, supra note 46, at 650–51.

[69] See id. at 665–70 (arguing that lack of narrow tailoring will doom general filtering legislation).

tering, metastasized into widespread centralized filtration by dangerous parties like large ISPs or search engines.

Yet there are reasons to doubt that PICS will be such a worry. Ironically, third-party private rating services for the Web may be a primary obstacle, because any move to create a universal rating scheme that becomes understood as a default requirement needs to be both demonstratively better and cheaper to set up and maintain than paying for a private service. Even with indirect government support, it is not immediately obvious that the incentives exist to prompt a quick move to a fully self-rated (or publicly rated) World Wide Web, let alone Internet. Drastic government action would do the trick—for example, a law that mandated self-rating of all content under a single standard would change the Internet overnight. But such direct government action has a much higher chance of being unconstitutional. It is also unclear that any such drastic legislation is on its way.

So PICS may not amount to a repeal of the law of gravity. But there is no denying that it is part of the general trend towards Internet normalization (especially of the World Wide Web) in response to the perceived needs of normal, rather than expert, users. A persistent mistake has been to assume that the Internet will not change, while assuming society will, and radically. On the contrary, we have changed the Internet more than the Internet has changed us; the Earth's gravitational pull on Cyberspace has been mightier than the reverse.

INTERLUDE: HOW THE NETWORK ARCHITECTURE OF THE INTERNET AFFECTS LEGAL ANALYSIS

Scrutiny of all things Internet flows smoothly when it heeds the architecture of the Internet in a rigorous way. Understanding this structure, admittedly, is not always easy. But think of the topic as akin to understanding the structural allocation of power among government institutions—knowing who is allowed to do what usually takes priority over substantive discussion. Similarly, since the network architecture of the Internet can be perceived as effecting a delegation of the power to code, understanding this architecture can be essential *before* reaching the merits. Luckily, the Internet's architecture is simpler than the government's, and, as we will see, the design of the Internet evidences a clear choice. It grants great

power over functionality—a proxy for usage—to the designers of applications. And since aspects of human usage are the facts that ultimately drive Internet analysis, the application is the beginning of most legal analysis.

To understand this point, two comparatively simple but important structural features of the Internet loom large. These are (1) the "layered" architecture of the Internet, and (2) the "end-to-end" design principle. Quite obviously these two design features were not chosen for their legal consequences. Rather, concerns of efficiency, modularity, scalability, and future flexibility drove the design of the Internet. But these choices nonetheless have a critical impact on any legal analysis.

A Layered Architecture

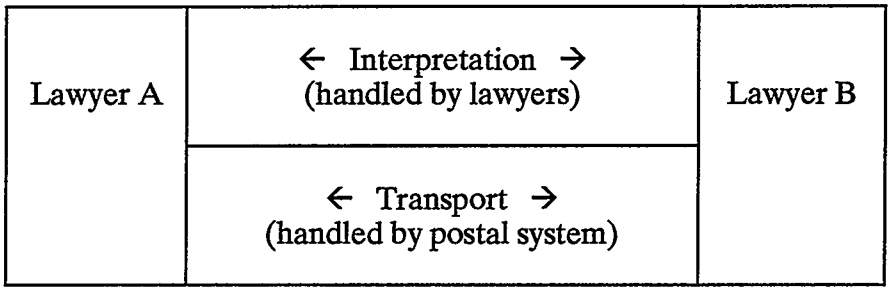
What it means for a network to have a layered architecture, viewed all at once, can be at first difficult to grasp, yet the idea is so clever that it merits understanding.[70] A network communication between computers is a very complex operation. The essence of network layering is a grand simplification by delegation to functional submodules, the layers.[71] Dividing one large task among several layers has numerous advantages—it allows specialized efficiency, organizational coherency, and future flexibility—and is something we constantly see in the real world yet consider unremarkable. Consider, as a way to understand this, what happens when one lawyer uses the postal system to mail a legal argument to another lawyer. The postal system is structured so that no one in

---

[70] What follows is a highly simplified explanation. A more thorough explanation of network architecture in general and layered architectures in particular can be found in any basic data network text. See, e.g., Uyless Black, Data Networks: Concepts, Theory, and Practice 269–88 (1989); John McConnell, Internetworking Computer Systems: Interconnecting Networks and Systems 14–31 (1988); Andrew S. Tanenbaum, Computer Networks (3d ed. 1996). While these sources focus on the International Organization for Standardization's Open Systems Interconnection (OSI) Model, a model seven-layer network architecture useful for comparison and categorization purposes, the underlying concepts are the same as those for the two-layer architecture described here.

[71] Those familiar with computer programming will recognize the logical parallel between a layered architecture and the basic programming technique known as structured programming (dividing a given program's tasks among functional modules with clearly defined inputs). For a formal comparison of structured techniques and network layering, see Black, supra note 70, at 273–75.

the postal system needs to understand law (the language of the lawyers) for the message to be successfully delivered. And, similarly, neither lawyer need do anything more than understand the rules on addressing and postage. This makes for a simple two-layer network. The function of understanding the contents of the letter has been delegated to a "higher" layer (in this case lawyers), and the function of delivering the letter has been delegated to a "lower" layer (the postal system).



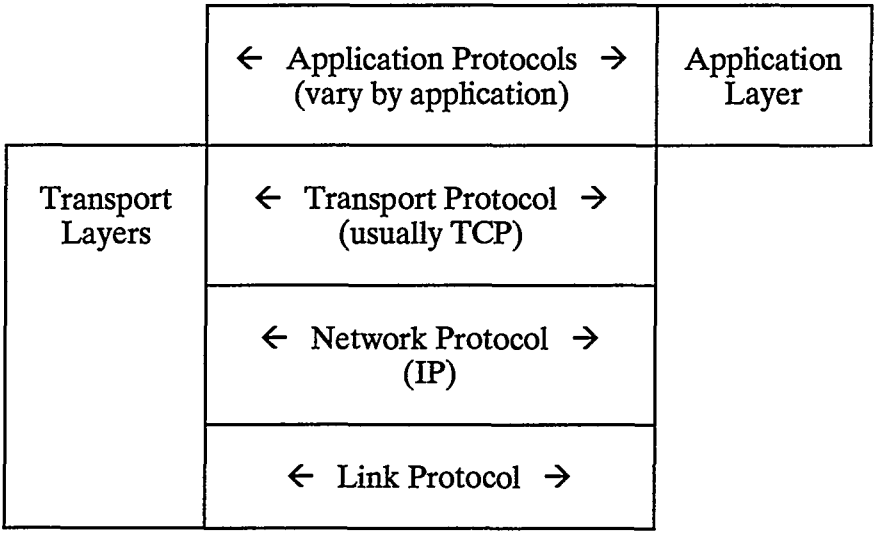
In this example, the postal level is called "lower" because it can be seen as more fundamental. The lawyers need the postal system or they cannot communicate at all; yet if the lawyers did not exist, the postal system would continue to carry mail for doctors, scientists and other interpreters of strange lingo. Notice also that the postal system is more fundamental in the sense that it can set standards that apply to everyone in the higher levels, regardless of who they are. For example, the postal service could require that all envelopes be blue. The higher-level users of the system would have no choice but to comply.

Notice several things about a network so structured. First, it allows an efficient specialization: That the postal system need not understand law (or the content of *any* of the messages it carries) dramatically reduces the burden on the post office and allows it to focus on one task: delivering mail. Second, the system is very flexible: The postal system can carry any type of message, and the communication will be successful, provided that the person on the other side understands it. This makes the postal system useful for a wide variety of applications. Finally, the layers are modular: Were the postal system to begin using spaceships to deliver its mail, the

lawyers would be unaffected so long as the rules for postage and writing addresses remained the same.

The Internet shares this same basic structure. Internet applications—email and so forth—operate separately from and above the set of basic Internet protocols, known as TCP/IP. The Internet's network architecture gives applications their own layer to interpret the data they send to each other without worrying how it got there. And the basic Internet protocols (with some exceptions not important here) are invariable and are used by all applications, much in the way that lawyers, plumbers, and doctors all use the same postal system.

The basic network structure of the Internet looks as follows:



So while there are actually four layers in the Internet architecture, for many purposes the most important distinction is between the transport layers, the set of (mostly[72]) constant Internet protocols that handle the basic data transmissions, and the interpretation layers, the huge variety of possible applications that make use of the data sent around by the transport layers. A reminder again that

[72] It should be here admitted that there is actually more than one protocol that serves the "packaging" function of TCP. The description I give is a simplification; the various datagram packaging protocols serve essentially the same function.

this description represents only the most basic aspects of the design; readers who are interested in precisely how the TCP/IP protocols function together are directed to the sources in the footnote.[73]

End-to-End Design

The decision to adopt a layered network architecture does not answer the subsequent question: where, exactly to place network function within this architecture. The architecture, alone, is an empty shell—it suggests that the duty to code function *will* be delegated among layers, but not *how*. Many functions could have been made a part of the basic Internet protocols, or have been left to the application layer. For example, most of what makes up the email system could be made a part of the basic transmission protocols of the Internet or left for the application designer to decide.

Hence, the importance of the end-to-end design principle. This principle, formally described as an argument in a famous paper twenty years ago,[74] holds that, wherever possible, function should *not* be placed at the lower-levels of a network system—rather, everything possible should be left to the applications at the "ends." In other words, the lower-level protocols should focus only on the minimal function of transmitting data, and in all other respects be kept as simple, umintrusive, and open as possible. This design philosophy, along with a few others, underlies the architecture of the Internet.

---

[73] More in depth, yet still readable, introductions to TCP/IP include Peter Rybaczyk, Novell's Internet Plumbing Handbook (1998), and Matthew Flint Arnett et al., Inside TCP/IP (2d ed. 1995). An online introduction is Charles L. Hedrick, General Description of the TCP/IP Protocols (1987) <http://oac3.hsc.uth.tmc.edu/staff/snewton/tcp-tutorial/sec2.html>. A more thorough TCP/IP reference is Douglas E. Comer, Internetworking with TCP/IP: Principles, Protocols, and Architecture (3d ed. 1995); a more general computer network reference is Tanenbaum, supra note 70. Detailed technical descriptions of the TCP/IP protocols are contained in the following Requests For Comments ("RFC"), the standards "legislation" of the Internet: RFC 793 (visited July 13, 1999) <http://www.faqs.org/rfcs/rfc793.html> (TCP); RFC 791 (visited July 13, 1999) <http://www.faqs.org/rfcs/rfc791.html> (IP); RFC 894 (visited July 13, 1999) <http://www.faqs.org/rfcs/rfc894.html> (Ethernet and IP); RFC 882 (visited July 13, 1999) <http://www.faqs.org/rfcs/rfc882.html> (name servers).

[74] See Saltzer et al., supra note 2.

The original end-to-end paper, written by Jerome Saltzer, David Reed, and David Clark, pressed the end-to-end argument as a narrow issue of efficiency. It argued that placing function at lower levels would be redundant whenever the function in question could not be achieved without the participation of the applications at the "ends" of the connection.[75] One can see intuitively that the less the "engine" of any network needs concern itself with, the faster and cheaper the network will be.

But an end-to-end design has deeper effects.[76] The principle amounts to a salutary delegation of the coding power in the Internet structure to the desiguers of applications. It grants the maximum possible application autonomy, giving to the application writers the freedom to achieve application goals in whatever manner they see fit, and innovate whenever and however they like. And at the same time, by confining the network itself to simple functions of broad usage, the desigu avoids blocking out future applications unknown or unpredictable at the time of desigu. For example, the World Wide Web was only a theoretical construct even at the time the modern Internet protocols were adopted on January 1, 1983.[77] And at least in part as a result of these features, this decade has witnessed an astonishing development both of Internet applications existing at the beginnings of the Internet (like email) and totally new and extremely innovative applications. All of this might have been impossible, or at least difficult, if the Internet had not had an end-to-end design.

The Internet's layered architecture and embedded end-to-end desigu have created an Internet where coding power resides among the desiguers of application. It allows—even encourages—an astoundingly large set of possible applications and ensures that there is very little that is *necessarily* true about the Internet as a whole. Hence, talk of the Internet as a whole will often be nonsensical, if not now, then soon. This architectural reality strongly suggests that meaningful legal analysis needs to focus on the level where variation, and the power to code function, are found. In other words, legal analysis of the Internet need begin to take application diversity seriously.

---

[75] See id.

[76] See Reed et al., supra note 3, at 72.

[77] See id.; Rybaczyk, supra note 73, at 26.

II. PRIVATE ORDERING: THE CURIOUS HISTORY OF CYBERSPACE SOVEREIGNTY

Is Cyberspace a place? Should it have its own rules? These questions once served as the focus of deeply acrimonious debate.[78] One side called Cyberspace sovereign, while the other equated the Internet with the telephone. Both, I want to suggest, were wrong and right; wrong for the entire Internet, yet potentially right about certain applications. The error was the same on both sides: mistaking one way of using the Internet for the entire Internet itself.

Today, the sovereignty debate has become academic. The popularity of the Internet and the onset of serious commercial activity has led directly to real legal disputes; real, that is, in the sense of tangible injury and benefit. And, without terrible fuss, courts in this country and elsewhere have proved neither incapable of nor shy in deciding Internet cases.[79] These predictable develop-

---

[78] See, e.g., Llewellyn J. Gibbons, No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace, 6 Cornell J.L. & Pub. Pol'y 475 (1997); Jack L. Goldsmith, Against Cyberanarchy, 65 U. Chi. L. Rev. 1199 (1998) [hereinafter Goldsmith, Against Cyberanarchy]; Jack L. Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty, 5 Ind. J. Global Legal Stud. 475 (1998); Steven M. Hanley, International Internet Regulation: A Multinational Approach, 16 J. Marshall J. Computer & Info. L. 997 (1998); David R. Johnson & David Post, Law and Borders—The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367 (1996) (stating the case for Cyberspace sovereignty); Lawrence Lessig, The Zones of Cyberspace, 48 Stan. L. Rev. 1403, 1407–10 (1996) [hereinafter Lessig, Zones] (criticizing Johnson & Post, supra); Henry H. Perritt, Jr., The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance, 5 Ind. J. Global Legal Stud. 423 (1998); David G. Post, The "Unsettled Paradox": The Internet, The State, and the Consent of the Governed, 5 Ind. J. Global Legal Stud. 521 (1998) (delving into international relations theory); Shapiro, supra note 46; Timothy S. Wu, Note, Cyberspace Sovereignty?—The Internet and the International System, 10 Harv. J.L. & Tech. 647 (1997) (attacking the descriptive assumption that the Internet is impossible to regulate). For a collection of some of these and other articles, see Borders in Cyberspace: Information Policy and the Global Information Infrastructure (Brian Kahin & Charles Nesson eds., 1997). For a quick overview of this debate, see the "Brain Tennis" exchange between David Post and Jack Goldsmith in the Hotwired Archive <http://www.hotwired.com/synapse/braintennis/97/34/nc_left_intro.html> (visited July 13, 1999).

[79] A Westlaw search shows 191 reported federal cases after 1995 that raise Internet-related issues (the cases were isolated by searching the texts of Westlaw's synopses and digests). These cases cover a huge spectrum, from trademark law to personal jurisdiction questions to obscure tort doctrines such as "trespass to chattels." See, e.g.,

ments, and the lack of any serious demand for a Cyberspace-based legal authority, have stillborn dreams of a Cyberspace nation.

From the beginning, it was clear that the descriptive argument—the claim that Cyberspace cannot be regulated—would fall moot.[80] This old cyberlibertarian bromide self-destructs under the glare of technical scrutiny[81] and the simple recognition that regulation need not be perfect to be effective—that regulation works through transaction cost rather than hermetic seal.[82] Consider for a moment the observation that a lock may be picked; interesting, no doubt, but not a convincing demonstration that a lock cannot serve any regulating function. Cyberlibertarians, some of whom have the Internet skills equivalent to the real-space locksmith, generalize from their own experience to conclude that no regulation of Cyberspace is possible.[83] But neither the theory nor the results are con-

---

Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999) (trademark law); Bensusan Restaurant Corp. v. King, 126 F.3d 25 (2d Cir. 1997) (personal jurisdictional questions); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (trespass to chattels). Significantly, in none of these cases did a court decide that it lacked subject matter jurisdiction. This painless exercise of adjudicatory jurisdiction has been paralleled by a similar lack of reluctance to exercise administrative and prescriptive jurisdiction.

Courts outside the United States seem to have similarly exercised jurisdiction with little hesitation. See, e.g., 1267623 Ontario Inc. v. Nexx Online, Inc., No. C 20546/99, 1999 Ont. C.J. LEXIS 1289 (Ontario Super. Ct. June 14, 1999) (lawsuit in Canada against a bulk emailer); Queneau v. Leroy, [1998] ECC 47 (T.G.I. 1997) (European Court case of Internet copyright); British Telecomm. v. One In A Million Ltd., [1999] 1 W.L.R. 903 (C.A. 1998) (lawsuit in England against a fraudulent domain name dealer); Alan Cowell, Head of German Web Sentenced for Pornography, N.Y. Times, May 29, 1998, at A3.

[80] For a thorough explanation of my view on this point, see Wu, supra note 78. That note examines the technology behind Internet regulation and concludes that, as a descriptive issue, regulation of the Internet is clearly possible (most effectively, using laws that compel the adoption of a certain architecture, as Singapore and China have done), and that the interesting issue is whether or not states will want to impose regulation on the Internet.

[81] The strongest evidence that this descriptive argument is essentially a grand hoax comes from any examination of firewall technology, the highly developed security technology that already walls off much of the Internet. See id. at 653. For a good introduction, see John P. Wack & Lisa J. Carnahan, Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls (National Inst. of Standards and Tech. Special Publication No. 800-10, 1995) <http://csrc.ncsl.nist.gov/nistpubs/800-10/>.

[82] See Wu, supra note 78, at 650. This point has been oft-made. See, e.g., Goldsmith, Against Cyberanarchy, supra note 78, at 1224–25; Lessig, Zones, supra note 78, at 1405.

[83] Jeffrey Schiller makes the interesting argument that, because ordinary users can quickly gain access to the security cracking tools of an expert, everyone on the Inter-

vincing—if regulation is impossible, then what are criminal hackers[84] doing in prison?[85]

So what of this debate is left behind? I want to suggest that the interesting questions about self-governance on the Internet remain collected around particular parts of the Internet, often particular applications, and not around "Cyberspace" as some kind of fantasy kingdom. Notice that the normative case for state regulation of the Internet depends on the application you have in mind. If you decide to log onto an airline website to buy a plane ticket, there doesn't seem to be any terribly convincing reason to treat this any differently than the phone call that could have been made in its stead. But for a group of MUD[86] users whose environment is en-

---

net can quickly become an expert security evader. See Jeffrey Schiller, Internet Rights versus Internet Security, Talk Sponsored by the M.I.T. Technology and Culture Forum (Mar. 18, 1997). I think this conclusion rests on a fundamentally erroneous assumption about how much time and energy an ordinary user is willing to commit to mastering arcane expert hacking tools for deeply modest returns.

[84] There exists a valiant, but perhaps hopeless, effort to try to preserve the term "hacker" as a reference to those whose skill with computers exceeds the common user's, and to distinguish "criminal hackers" as those who abuse their superhuman powers.

[85] See United States v. Thomas, 74 F.3d 701 (6th Cir. 1996) (operators of obscene bulletin board system sentenced to federal prison); United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (Bob Morris, originator of the Internet worm, sentenced to fine and probation); Andrew Blankstein, Hacker Sentenced to Prison, Told to Avoid High Technology, L.A. Times, June 29, 1997, at B3 (famous hacker Kevin Mitnick sentenced to prison); Paula Span, Modem Operandi: Phiber Optik, the Bad Boy Hacker, Out of Stir and On-Line, Wash. Post, Jan. 13, 1995, at B1; infra notes 102, 104–05 and accompanying text (death threat by email, defamation, and securities fraud).

[86] A MUD is a program running on a remote server that creates a virtual environment that can be accessed by remote users, who assume the identity of characters in that world. MUDs vary. Some are actually games, some are purely social, and many have special themes (e.g. everyone plays an animal or perhaps a Star Trek character.) A MUD user typically has a high degree of control over her own identity as it appears to other users, and can walk around the "world" interacting with other users or other objects situated in the MUD, usually organized by "room." At a higher level, users can create and program their own objects, including the possibility of creating (somewhat) artificially intelligent objects (robots). Finally, there are many MUD-type programs with similar names, such as MOO (MUD, Object Oriented), MUSH (Multi-User Shared Hallucination), TinyMUD and TinyMOO, and LPMUD (role-playing MUD).

What makes MUDs particularly interesting is that they offer human interaction in an entirely user-created world, with user-created identities. Since the powers that characters have can lead to abuse of others, there are typically rules or laws in a MUD, enforced, if necessary by "Wizard" figures who have greater (technical) pow-

tirely virtual and who perhaps see their physical lives as distinctly secondary, allowing this group of people to make their own rules does not seem outrageous. It is the crossover that is outrageous: the suggestion that my online ticket purchase becomes governed by some weird law of Cyberspace because I used a packet instead of a dial tone or the idea that the U.S. Congress ought to enact the membership rules of LambdaMOO (a popular MUD).[87]

But make no mistake about the bottom line. The second, self-contained type of Internet usage is only a fraction of total usage—and, more importantly, a type of Internet usage deeply unlikely to trigger any legal consequence. Much Internet usage, rather, has significant real-space effects, and with such effects comes the normative case for jurisdiction.[88] Even if there were a parallel authority in Cyberspace (beyond that created by contract), the existence of concurrent jurisdiction is nothing particularly surprising to a twentieth century legal system.[89] So only the few applications with

---

ers to do things such as delete a certain character from the MUD. MUDs also offer the possibility of an environment and identity ultimately customizable to individual preference; for these reasons, a well known MUDism holds that users see their real lives as just another, less interesting window.

Social scientists have an unsatiable fascination with MUDs, and the literature on the sociology of MUDs is vast—there is even a refereed academic MUD journal. For some of the most famous writings on MUDs, see Sherry Turkle, Life on the Screen: Identity in the Age of the Internet (1995) (providing an excellent introduction); Julian Dibbell, A Rape in Cyberspace, Village Voice, Dec. 21, 1993, at 36. The *Journal of MUD Research* can be found at <http://journal.tinymush.org/~jomr/> (visited July 13, 1999), and a lengthy collection of MUD-related academic papers can be found in the "Lost Library of MOO" at <http://lucien.berkeley.edu/moo.html> (visited July 13, 1999).

[87] The telnet site from which to enter the famous LambdaMOO (running out of Xerox Park) is <telnet://lambda.moo.mud.org> port 8888, and visiting there is definitely a worthwhile experience. It must be warned, however, that the expert users already there have a tendency to be somewhat impatient and abusive with newcomers. As their gateway page itself states:

> LambdaMOO is a new kind of society, where thousands of people voluntarily come together from all over the world. What these people say or do may not always be to your liking; as when visiting any international city, it is wise to be careful who you associate with and what you say.

Id.

[88] Cf. Restatement (Third) of the Foreign Relations Law of the United States §§ 402(1)(c), 403, 421(j) (1987) (stating that "substantial effect" is a basis for prescriptive and adjudicatory jurisdiction).

[89] This is not to say that concurrent jurisdiction does not raise tough issues, but it is nonetheless a nearly unavoidable fact of life in a world with more than one legal jurisdiction, and events that implicate more than one state. See Mark W. Janis, An In-

basically no real-space effect—mostly, consensual fantasy worlds like MUDs—have any serious normative claim to immunity for things that happen "there." And so we can see that the manipulation of the MUD model into an analogy for all of Cyberspace is what created this fallacious debate in the first place. It makes a perfect example of mistaking the features of an application for those of the entire Internet, and the whole discussion seems destined to become a curious relic of early Internet history.

This is actually an exceedingly generous treatment of the issue, for it makes the kindly assumption that the development of some kind of general Cyberspace regulatory authority is somewhat plausible.[90] It is hard to even consider granting comity to "Cyberspace" lacking anyone to grant comity to. And as it happens, this assumption is more for fun than anything else; *Star Wars* without hyperspace would be a boring movie. But in this galaxy the prospects are remote at best. There will, of course, always be some private ordering—internal rules for web hosting, MUD codes of conduct, domain names, and so on. But a Cyberspace-wide authority that regulates every transaction that happens to run through the Internet looks about as likely as a city on the bottom of the ocean. Like the ocean city, the main problem is that somebody has to want it. No one does. Telling is the humorous fate of the "Virtual Magistrate" project: The Virtual Magistrate has apparently retired from Cyberspace adjudication, and ironically has become a font for advice on real-space law.[91]

---

troduction to International Law 249 (1988) ("There actually are countless such cases of concurrent jurisdiction ...."). Complex rules have evolved to attempt to handle problems of concurrent jurisdiction. See, e.g., Restatement (Third) of the Foreign Relations Law of the United States §§ 401–33 (1987).

[90] On the feasibility of a Cyberspace-based legal authority, see Margaret Jane Radin & R. Polk Wagner, The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace, 74 Chi.-Kent L. Rev. (forthcoming 1999). These authors stress the lack of a realistic mechanism for enforcement of any Cyberspace regime's rules.

[91] The Virtual Magistrate is, according to its website, "a specialized, on-line arbitration and fact-finding system for [online] disputes" run by the Villanova Center for Information Law and Policy <http://vmag.vcilp.org/> (visited July 13, 1999). Unfortunately, the Virtual Magistrate appears to have taken an extended recess (three years and counting), with no indication of when he might return. In his more active days the VM did arbitrate one case ordering AOL to remove an advertisement for junk email from its system, yet it is unclear whether AOL ever actually complied with the order, or what the VM would have done if AOL didn't. The site has instead become, for unknown reasons, a forum for terse legal advice on a variety of issues—

So there is no case for deference to Cyberspace as some kind of empire of our imagination. But I think there are nonetheless instances where particular types of Internet usage constitute the kind of private regime, familiar in our world, that can waive all but mandatory regulation by states—in effect, a private contractual order. And in such cases states and courts ought to respect generally the waivers and the rules set up by these private regimes, as they do for any private order set up by any private group. But where, on the Internet, is this appropriate?

The easiest thing to do is to look at the Internet usage in question and ask what, exactly, the parties have agreed to through that usage. But generally, the variation, unsurprisingly, is found between applications. The observed variance in how "contained" an application is suggests a useful guide. It suggests a basic distinction between what can be called the Internet as a means and the Internet as an end.[92]

By the Internet as a means, I have in mind the more mundane use of the Internet to serve as an alternative (perhaps an enhanced alternative) to a preexisting means of achieving a preexisting objective. The crucial issue is the presence of tangible, real-space effect. So you might buy a plane ticket through the World Wide Web, issue a death threat by email, or make an Internet phone call. You happen to use Internet packets to do so instead of using preexisting means; hence, the Internet as a means. By Internet as an end, I mean usage directed towards ends created by the online environment itself. As a result, real-space consequence is minimal. The really "pure" examples of this are the popular online games like Ultima Online[93] or network Quake,[94] which are multi-user versions

---

from leaseholds to sexual harassment—from parties of unclear associations. See Virtual Magistrate Discussion Area, Conference Room 109 (visited July 13, 1999) <http://www.cilp.org/cgi-secure/confcenter/109/>. For another virtual court proposal, see Henry H. Perritt, Jr., Jurisdiction in Cyberspace, 41 Vill. L. Rev. 1, 100–01 (1996) (proposing a "United States District Court for the District of Cyberspace" but conceding that the Seventh Amendment issues would be troublesome).

[92] An alternative nomenclature might be the distinction between Cyberspace (Internet as an end) and Internet (Internet as a means), but this also might cause more confusion than it cures.

[93] Ultima Online allows thousands of players (currently 90,000) simultaneously to play the same multi-user fantasy based game, all taking place in the same, large world (Britannica). The programmers attempted to write into the Ultima code a complicated social structure that would provide rewards for altruism to maintain social order and to create an online economy (although these attempts, in the first editions,

of computer video games. Real-world goals aren't terribly important to players of Ultima Online (in that capacity); the goals are created by the game itself, and, for example, no one sues another character if she dies. MUDs are a strong secondary example and are often more interesting because of their highly developed set of social norms and "Wizard"-enforced rules based on repeated interactions. Lesser examples are various types of chatrooms and discussion groups like Usenet. But notice that for all of these types of activities, the moniker "Cyberspace" suddenly has a resonance that just seems lacking when I use email to schedule my dentist appointment.

Obviously this is an imperfect dichotomy. First, of course, even the "Internet as an End" applications have some real-space effects. So long as we retain a physical manifestation, there will be no total escape from real-world consequences. And this helps explain why the normative case for *full* immunity is so weak.

Second, and more interestingly, there is a huge category of Internet usage that achieves preexisting goals in new ways—ways that change the way we think of things and perhaps even the way we need to regulate things.[95] And because laws and other forms of regulation are usually premised on a set of assumptions about the context in which they will operate, a change in a technological

---

have largely been a failure). See Thierry Nguyen, Origin's Epic Online Game Is Snared by Bugs and Design Problems, Computer Gaming World, Feb. 1, 1998, at 162. But the product is making money, and at a recent press conference Origin, the company that created Ultima Online, revealed that usage averages out to 3.5 hours per user per day. See Omar L. Gallaga, Ultima Online's Success Better Than Expected: Origin's Garriott Says He's Comfortable on the Business Side of Gaming, Austin Am.-Statesman, Oct. 8, 1998, at C1.

Interestingly, Ultima Online has not been immune to real world law. A group of disgruntled gamers has sued the publisher of Ultima Online for providing a game that allegedly failed to live up to its hype. See Michael Hawash, The UO Lawsuit: Gamers Sue Electronic Arts, Origin Systems, Saying Ultima Online Was Misrepresented, Computer Gaming World, Nov. 1, 1998, at 46. The Ultima Online website is at <http://www.owo.com> (visited July 13, 1999).

[94] Quake is a popular and less sophisticated "shoot 'em up" game that can be played over the Internet; it also has online "clans" associated with it and a certain etiquette that prohibits, among other things, using robots to aim for you. See Network Quake Newbie Guide (visited July 13, 1999) <http://www.gamers.com/features/1997-12/14-quake_newbie/home.asp>.

[95] Lawrence Lessig has explored these issues in great depth. For a representative example, see Lawrence Lessig, Reading the Constitution in Cyberspace, 45 Emory L.J. 869 (1996).

"fact," even if apparently unrelated to the law, may nonetheless have large unexpected effects on the operation of that law. "Internetization" typically results in a massive reallocation of transaction costs; this tends to lay bare those laws that (unknowingly) relied heavily on those costs as a kind of regulatory "crutch."[96] This effect has been demonstrated with great clarity by the example of online porn, which we might think of as regular porn minus transaction costs. But although these effects cloud the picture, they still, in my view, do not create any constant normative presumption against "regular" laws, other than for reasons of prudence and ripeness.[97]

So this just suggests that the normative case for a distinct regime of rules depends on what usage or application on the Internet you are talking about. But descriptively, we know that very few existing usages of the Internet have a good normative case for immunity to real-space law. It is true that members of LambdaMOO ought be the ones to set the rules of their world; it makes little sense for the government to try to legislate the law of Lambda because most MUD activity affects only the people involved. Like any group of individuals, they ought be allowed to make their own rules for their activities, just as the National Hockey League, not the Attorney General, sets the penalties for "high-sticking." And, of course, this isn't particularly different from saying that it probably works better if we let any special group set its own rules, be it the member LambdaMOOers or the Shasta County Cattlemen.[98] After all, Robert Ellickson tells us that these group norms will be welfare maximizing.[99] This being said, agreeing that people ought to make their own rules for their own game does not compel any conclusion that participants should gain some shield from mandatory law

---

[96] As was pointed out earlier, laws usually operate to increase the costs of a given activity rather than to somehow prevent that activity entirely.

[97] On this point, see Denver Area Educational Telecommunications Consortium, Inc. v. FCC, 518 U.S. 727, 774–78 (1996) (Souter, J., concurring) (arguing for gradualist regulation of new technology); Lessig, The Path, supra note 46, at 1745 (stating that "if we had to decide today . . . just what the First Amendment should mean in cyberspace . . . we would get it fundamentally wrong").

[98] The norms governing the relations of the Shasta County Cattlemen are studied in great depth in Robert Ellickson, Order Without Law (1991).

[99] See id. at 167–87.

(such as the criminal laws), other than from consent.[100] To the extent that, for MUDs, outside effects are a rarity—a function of the application—the presence of mandatory law is barely felt.[101]

But here as there, as soon as signs of real-world consequences begin to show up, the case for any distance from territorial regulation weakens correspondingly. And finally, when a death threat arrives by email instead of by letter[102] nobody bothers to argue that the Virtual Magistrate ought to jump in and preempt territorial criminal law (or that she is even capable of doing so).

All of this strongly suggests that talk of a thick Cyberspace sovereignty is really convincing only when talking about MUDs, video games, or other exercises of fantasy, because it is only when using these kinds of programs that the Cyberlibertarian point about self-contained online activity makes any sense. Move along to chat rooms and real-time "talk" applications like ICQ,[103] and the normative argument for private order begins to thin; certainly an antitrust conspiracy made over ICQ has no special shield. Enter discussion groups or anything else that looks like one-to-many communication, and suddenly things like defamation laws[104] or securities

---

[100] Jack Goldsmith, drawing on conflicts law, points out the default law/mandatory law distinction, noting that default laws can be modified to fit the needs of the parties, but mandatory laws cannot. See Goldsmith, Against Cyberanarchy, supra note 78, at 1209–12.

[101] For extensive study of the relationships between formal law and informal norms, see the work of Lisa Bernstein. See, e.g., Lisa Bernstein, Merchant Law in a Merchant Court: Rethinking the Code's Search for Immanent Business Norms, 144 U. Pa. L. Rev. 1765 (1996); Lisa Bernstein, Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry, 21 J. Legal Stud. 115 (1992).

[102] See, e.g., United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997) (reversing threat conviction but without regard to use of email as means of communication); Thao Hua, Ex-Student Sentenced for Hate E-Mail Courts: Richard Machado is Fined $1,000, Put on Probation for Threatening Asian American Students, L.A. Times, May 5, 1998, at A24. See generally Brooke A. Masters, When E-Mail is a Weapon, Victims Struggle for Protection, Wash. Post, Nov. 1, 1998, at B1 (listing cases of email harassment and threat convictions).

[103] ICQ ("I Seek You") is a program that facilitates online chat by allowing users to search for friends and associates online and then chat via a shared window. For more see the materials at <http://www.icq.com> (visited July 13, 1999).

[104] See, e.g., Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (lawsuit against Internet columnist Matt Drudge for allegedly defamatory remarks made about Sidney Blumenthal).

laws[105] begin to make their presence felt. When an application has spillover—real-space effects—the jurisdictional questions are all too familiar to the student of international law.[106]

The debate over Cyberspace sovereignty has been swallowed by recent history. Cyberspace, as one unit, is not about to become a sovereign jurisdiction, not in this galaxy at least. But what application-centered analysis tells us is that there are interesting questions about private ordering on the Internet, and that they revolve around particular usages and applications. The application level is where the open architecture of the Internet leaves real room for private regimes. But the overarching lesson from this historical curiosity is that manipulation of analogy; one concept of what the Internet "is" can lead quickly to total nonsense.

CONCLUSION

Let me end this Essay with a less serious observation, one that has been expressed before in different ways.[107] The latest rounds of Internet sloganeering have been the talk of a funny kind of vested interest—not the usual suspects, but a kind of Madisonian notable of the computer age best known as the "expert user."[108] The fight over these slogans and over First Amendment scrutiny exposes an interesting running battle between these entrenched expert users (and those who consider themselves such) and newcomer normal users. Expert users like the slogans. Why? Because expert users suffer least and benefit most from an unregulated Internet. Remember, after all, who actually uses encryption software and who still needs help opening attachments; who knows what mp3s are and how to get them and who just pays more for CDs at the store; and,

---

[105] The Securities and Exchange Commission ("SEC") appears to have become very active in its enforcement of securities laws online. In October 1998 the SEC announced the results of the first nationwide Internet securities fraud sweep, involving charges being filed against 44 people in 23 actions, mostly for stock touting online. See SEC Does a 'Net Sweep and Charges 44, Nat'l L.J. Nov. 9, 1998, at A9. For details on these lawsuits, see SEC Litigation Releases <http://www.sec.gov/enforce/litig.htm> (visited July 13, 1999).

[106] See Goldsmith, Against Cyberanarchy, supra note 78, at 1212–39.

[107] See, e.g., Jonathan Zittrain, The Rise and Fall of Sysopdom, 10 Harv. J.L. & Tech. 495 (1997).

[108] For more on Madisonian notables, see Roberto Mangabeira Unger, What Should Legal Analysis Become? (1996).

of course, who knows how to disable Microsoft Explorer's domination of the desktop and who ends up stuck with it. The truth is that normal users might one day (or perhaps now) want the help of their government in some or all of these areas. Or they might not. The problem is that the constitutional law of Cyberspace, as it is, wants to make this choice in advance and encase it in concrete. The sentiment is well-intentioned and also well-argued. But to stick everyone with the constitution of the expert user may, in the long run, prove the inexpert move, as it may do more to close out the Internet than flexibility ever would.