Research Publication No. 2003-01
3/2003

Internet Points of Control

Jonathan Zittrain

INTERNET POINTS OF CONTROL

JONATHAN ZITTRAIN*

Abstract: The online availability of pornography and unauthorized intellectual property has driven Internet growth while giving rise to efforts to make the Internet more regulable. Early efforts to control the Internet have targeted the endpoints of the network—the sources and recipients of objectionable material—and to some extent the intermediaries who host others' content. Recently, attention has shifted to the intermediaries near would-be recipients of content. The U.S. Commonwealth of Pennsylvania permits its attorney general to obtain a court order requiring ISPs to block Pennsylvanians' access to Internet locations designated as containing illegal pornography. If successful, this approach could be employed for other regulatory purposes, such as controlling the online distribution of copyright-infringing materials. While the Pennsylvania law suffers from a number of technical limitations and constitutional vulnerabilities, with some adjustments to Internet architecture and data carriage practices this approach could become a comprehensive scheme for widespread content control that overcomes a number of enforcement barriers and jurisdiction-related objections.

INTRODUCTION

Pornography is said to be among the earliest and most popular uses to which new media are put.[1] The mainstream development of the global Internet carries on that tradition, augmented by the unauthorized swapping of proprietary material. Empirical data is difficult to acquire, but if a packet were randomly plucked and parsed from the data flowing through the Internet's backbones, chances are good that it would be a piece of something prurient, pilfered, or both.[2]

---

* Jack N. & Lillian R. Berkman Assistant Professor for Entrepreneurial Legal Studies, Harvard Law School. I thank Terry Fisher, Megan Kirk, Molly Shaffer van Houweling, and participants in the University of Pennsylvania Legal Studies Workshop for insights on earlier drafts, and Peter Sand in the Pennsylvania Attorney General's Office and Craig Silliman at WorldCom for very helpful discussions.

[1] Peter Johnson, *Pornography Drives Technology: Why Not to Censor the Internet,* 49 FED. COMM. L.J. 217, 217 (1996).

[2] *See* YOUTH, PORNOGRAPHY, AND THE INTERNET 72 (Dick Thornburgh & Herbert S. Lin eds., 2002) ("Compared to the totality of content on the public World Wide Web, adult oriented sites account for a relatively small fraction (about 1.5 percent). However, these

If the overlapping categories of pornography and intellectual property drive public Internet use and growth, they have therefore also created the most powerful pressures to make the Internet and its users more "regulable."[3] Originally designed by academics for quick, cheap and perfect data copying and sharing—without inquiry or worry about its nature, or that of the people on either end of a given transfer—the Internet's architecture has prominently stymied control efforts by those allegedly harmed by its less innocuous uses. If one were to randomly pick a case from a typical cyberlaw course or casebook from within the past five years, chances are good that it would concern attempts to penalize or prevent something prurient, pilfered, or both.[4]

Attempts to control the Internet have met with mixed success amid a vigorous and ongoing debate about the extent to which the comparatively anarchic status quo will prevail.[5] I wish to add to that debate—in which I believe that control will trump anarchy—by examining a recent experiment in control launched by the Commonwealth of Pennsylvania to restrict the flow of illegal pornography available to its residents. This experiment, grounded in a state law by which any Internet service provider (ISP), under threat of criminal liability, can be required to block access by Pennsylvanians to a given Internet destination.[6] The law represents a novel approach, heretofore untried by both anti-pornography champions and their conceptual sibling-in-arms publishers seeking to limit intellectual property piracy.

---

sites account for a significant amount of Web traffic. According to industry statistics, approximately 70 million different individuals per week view at least one adult Web site on a global basis . . . .").

[3] *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS 178–79 (2001).

[4] *See generally, e.g.*, RAYMOND S. R. KU ET AL., CYBERSPACE LAW (2002) (over 70% of the cases involved pilfering or prurient material); MARK A. LEMLEY ET AL., SOFTWARE AND INTERNET LAW (2000) (80% of the cases in the Internet law portion of the book involved pilfering or prurient material); PETER B. MAGGS ET AL., 2002 SUPPLEMENT TO INTERNET AND COMPUTER LAW (over 60% of the cases involved pilfering or prurient material).

[5] On the side of anarchy: see generally, for example, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1367, 1375 (1996); Symposium, *Fundamental Rights on the Information Superhighway: Keynote Address*, 1994 ANN. SURV. AM. L. 355; John Perry Barlow, *The Economy of Ideas,* WIRED, Mar. 1994. On the increasing emergence of control, see generally, Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net,* 14 BERKELEY TECH. L.J. 2 (1999), *available at* http://www.law.berkeley.edu/journals/btlj/articles/vol14/Lessig/html/text.html.

[6] *See* 18 PA. CONS. STAT. § 7330 (2002) (Section 7330 was repealed by 2002, Dec. 16, P.L. 1953, No. 226, Section 2, but it was replaced by an essentially identical set of statutes. 18 PA. CONS. STAT. §§ 7621–30 (2003)).

The experiment is notable for its audacious departure from the Internet's techno-political foundations. It enlists network service providers in a role that has previously—surprisingly, in retrospect—completely eluded the crossfire documented in the courses and casebooks. It is also notable because, after a string of efforts resulting in something far short of total effectiveness, it portends a strategy that will work. ISPs can serve as Internet police, not only cordoning off areas from view when acting as hosts of content, but also more broadly restricting access to particular networked entities with whom their customers wish to communicate—thus determining what those customers can see, wherever it might be online. The publishers, themselves no strangers to creative and cutting-edge (if so far somewhat hapless) approaches to taming the Internet, are no doubt watching closely, and will endeavor to adapt this sort of progress on anti-pornography, should it succeed, for use in their own battles.

A refined Pennsylvania approach—reinforced by the technical tools developed by ISPs conscripted to accommodate it—could cause a sea change in the Internet's regulability. Such a change would bring Internet usage in line much more closely with prevailing legal standards, whether concerning dissemination and use of pornography or intellectual property, or relating to other persistent problems like gambling, spam, privacy infringement, or conflicting jurisdictions. Those who bewail such a change will have to frame their objections persuasively and show that those objections are truly fatal to the adoption of the general strategy of client-side ISP filtering. By sorting the Internet's brief but intense history of content control struggles into a framework of points of technical intervention along a canonical Internet data path, I will explain why the Pennsylvania approach is a significant departure from prior attempts at regulation and explore its desirability should it become commonplace across a range of regulatory purposes. I conclude that although the current implementation will prove unwieldy, a few adjustments to Internet architecture and common practices of data carriage could usher in a comprehensive scheme far more amenable to widespread content control both technically and as a matter of fairness to those censored.

I. A Taxonomy of Network Control Approaches

To understand the most recent approach in the struggle for Internet regulability and its relation to previous tactics, it is important to understand the technical path between two points of communication on the Internet. Boiled down to its essence, the Internet's routes

and protocols see to it that data from a user at one "point of presence"—typically a computer—can find its way to another such node and corresponding user through a series of often distinct intermediaries.

Figure 1 shows an abstraction of the path followed.[7]

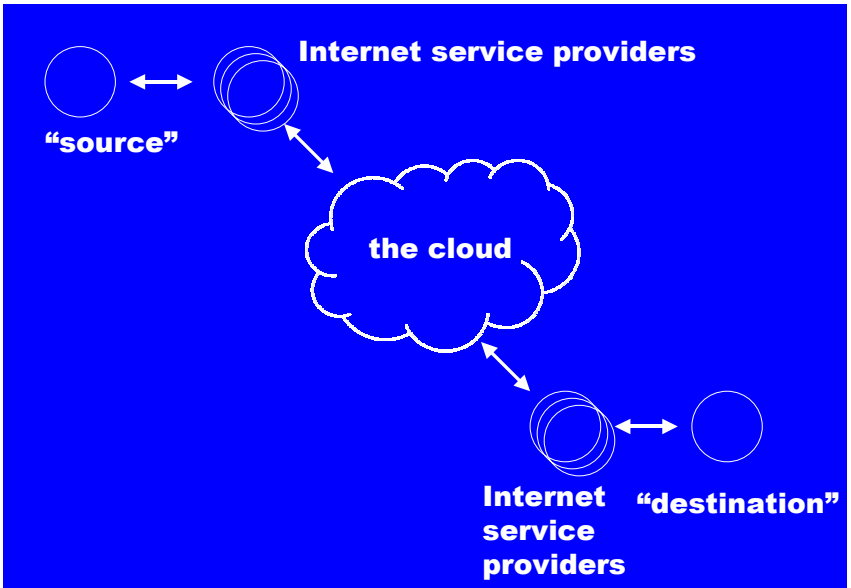

Figure 1: Abstraction of Internet Protocol wide area point-to-point data transmission

Each point of presence on the Internet is assigned at least one unique number—an IP address. That address might be more or less permanent ("static") or assigned only for the duration of that computer's short-lived connection to the Internet ("dynamic"). Dynamic addresses occur most frequently where a computer is attached to the Internet through a dial-up modem connection. A packet of data is passed from the computer whose user created it, with a label indicating that source computer's IP address, to the computer's ISP. Typically each computer has only one ISP, which initiates the packet's journey from the computer to its destination and returns any packets labeled for that computer's IP address. The packet's destination is also identified by its particular IP address.

---

[7] *See generally* Douglas E. Comer, Internetworking with TCP/IP Volume 1: Principles, Protocols, and Architectures (4th ed. 2000) (field's classic text detailing internetworking).

Most ISPs themselves have ISPs—smaller ISPs can either be resellers of a larger ISP's service or simply have one or more "transit" arrangements by which other ISPs agree to pass packets back and forth to the smaller ISP and its customers. Thus Figure 1 includes several overlapping rings where ISPs are concerned, indicating the Matryoshka doll-esque structure of concentric packet-passing that often takes place at either end of a packet's travels.[8]

Such multiple hops are usually necessary because Internet data typically moves in short physical fits and starts, from one router to the next along a chain that ultimately ends in a destination. Simplifying somewhat, it is as if one attempted to reproduce the functions of a country's paper postal service without the use of a postmaster general or accompanying fleets of trucks. Rather, one living on the south side of an east-west street might simply examine the contents of one's mailbox and do one of four things: first, take mail addressed to oneself inside the house; second, take any mail for any westward destination—whether three houses down or miles away—and walk it to the mailbox one house to the left; third, take any mail for any eastward destination and walk it one house to the right; and fourth, take mail for any northward destination and walk it across the street. So long as all homeowners act similarly, even paper mail could be moved in rather staggered fashion across the country one home dweller at a time.

At some point in the path ISPs do not pass packets upward to still larger ISPs. Instead, like the neighbors in the postal mail example, they "peer" with other (often like-sized) ISPs, passing packets laterally when one of the receiving ISP's customers (or customer's customers) appears to be linked to the computer at the packet's indicated destination. A receiving ISP then passes the packet to the relevant client ISP, or, if at the end of the chain, to the destination computer itself. Such peering takes place, in technical terms, within the "cloud," or colloquially, the "middle" of the Internet, where smaller networks come together to logically construct the single Internet.

Thus we might think of typical movement of data on the Internet as having five distinct phases. It begins at (1) a source, passes through (2) the source ISP, continues through transit and/or peering through (3) the cloud, is handled by (4) the destination ISP and then arrives

---

[8] One can watch a report of the path a packet takes from one's computer to a given destination through the use of "traceroute," usually abbreviated as "tracert" in Windows environments.

at (5) the destination. Of course, some journeys are short enough—they might take place between users of the same ISP, for example—that not every step is taken. Even if all the steps are involved, conceptually different phases might still be handled by the same firm. Also, "source" and "destination" are more symmetric network entities than they sound—each is simply a point of presence for the exchange of data, and, unlike television or radio broadcast, both Internet users and Internet servers are in the business of habitually exchanging data. Either one might be the "source" of a given transfer between the two—the Internet user for sending a signal corresponding to a mouse click indicating which file is desired from the server, and the Internet server for offering up the file to the user. Here I take "source" to mean a server or supplier of information on the Internet—either a high-traffic server designed to accommodate many requests for information (e.g., the computers behind nytimes.com), or an individual Internet user who has configured his or her computer to supply data to others (e.g., a user of the Gnutella file sharing network who has accepted that program's default of making some of the user's files available to others). I take "destination" to be an individual user of the Internet who requests and receives data from a source.

Each phase of a packet's travels is usually invisible to the users on both ends of a communication; the Internet's point is to make such basic data movement as automatic and involuntary as breathing. Thus neither computer users nor software developers typically need to concern themselves with the details of Internet routing. Efforts, however, to restrict data flow to limit the transmission of pornography, illegally copied intellectual property, or other undesirable content can be best understood and evaluated bearing such routing in mind. Routing is critical because the phase at which control is attempted is one of the most important factors contributing to a given control strategy's strengths and shortcomings as matters of both engineering and policy.

Within the U.S. legal framework, not only must the data in question be properly labeled "contraband," such as where its possession or transmission could be legally actionable, the entity targeted for legal action must have been properly asked to prevent the data's transfer or use. Various barriers to practical enforcement of any legal requirement also exist. Those seeking to block the illegal content must pressure the entity within the chain of data transfer whose selection maximizes the chances of both legal responsibility and successful enforcement.

A. *Asserting Control at the Source*

The source of a data transfer is a natural locus at which to belay that transfer. Indeed, this naturally happens every time a given point of presence on the Internet erects a password barrier or other firewall to allow some but not all users to access data within the source's files. Those running the servers that make particular data available online are in the most direct position to stop its distribution should they wish—or be compelled—to do so. Furthermore, the source of a communication is almost always most clearly and directly legally responsible for its distribution, at least compared to those further along the transmission chain.[9]

Early efforts to combat illegal Internet-transferred pornography focused on Figure 1's source of the pornographic content.[10] Operators of online bulletin boards who offered subscriptions for access to obscene photographs faced criminal liability under the standard federal anti-obscenity laws, indexed to the destination states' "community standards" for obscenity.[11]

The Communications Decency Act of 1995 (CDA) made it a crime to, among other things, initiate the transmission of "indecent" material to minors.[12] The presumed high impact of the CDA on the behavior of those placing information on the Internet was the source of its constitutional vulnerability.[13] The relevant provisions of the CDA were found unconstitutional precisely because they effectively restricted the material available to children by restricting the material available to anyone.[14] The self-censorship of speakers on the Internet resulting from threatened criminal liability would deprive parents of the ability to fine-tune what their children could see on the Internet. The spillover effects on adults' own access to speech also posed a constitutional problem.[15] The worry was that speakers wishing to avoid

---

[9] *Compare* Playboy Enters. v. Webbworld, 991 F. Supp. 543 (N.D. Tex. 1997) (in which the creator of an Internet site which sold adult images from newsgroups was liable for copyright infringement), *with* Religious Tech. Ctr. v. Netcom On-Line Communications Servs., 907 F. Supp. 1361 (N.D. Cal. 1995) (where an Internet access provider/bulletin board service operator was held not directly liable for copyright infringement, in part because it was considered a "mere conduit" for unaltered information.)

[10] *See* 18 U.S.C §§ 1462, 1465 (2000). *See generally* U.S. v. Thomas, 74 F.3d 701 (6th Cir. 1996).

[11] *See generally Thomas*, 74 F.3d at 710, 711.

[12] *See* 47 U.S.C § 223(a)(1)(B)(ii) (2000).

[13] *See id.*

[14] *See* Reno v. ACLU, 521 U.S. 844, 874 (1997).

[15] *See id.* at 874–75.

liability for transmitting material illicit with respect to children might choose to forego publishing such material entirely, rather than availing themselves of the law's safe harbor through implementation of credit card verification systems, which were thought to serve as a crude method to distinguish adults from children.[16] Thus, the law's deleterious effect on the availability of material not constitutionally proscribable for adults was fatal to the provisions.[17]

The CDA's constitutional infirmity might be confined to the distinct problem of "dual use" content—proscribable with respect to some viewers but completely protected with respect to others—but the more general lesson is that legal duties placed upon the source of Internet content can have powerful effects.[18] Indeed, other legal requirements on sources of pornographic material, regardless of the viewer, appear to be widely respected, at least among corporate purveyors of pornography. For example, federal law requires those in the pornography business to keep records about the identities and ages of people featured in their materials, and to advertise their compliance with the law's provisions.[19] A Web search on a citation to the law's provision, "18 U.S.C. 2257," yields approximately 113,000 results[20]—the overwhelming majority of which appear to be statements of compliance with the law offered by pornographic Web sites.[21]

Other federal regulatory efforts focus quite naturally on the source of an Internet communication. For instance, the U.S. Food and Drug Administration has long held medical and pharmaceutical Web sites responsible for their claims,[22] as have the Securities and Exchange Commission,[23] and the Federal Trade Commission.[24]

Apart from public agencies' application of statutory and administrative law, aggrieved private parties and attorneys general have also

---

[16] *See id.* at 876–77.

[17] *See id.* at 874.

[18] Congress has taken at least one additional (still constitutionally unsuccessful) stab at regulating Internet speakers in this area, passing the Children's Online Protection Act. *See* 47 U.S.C. § 231(a)(1) (2000). COPA limits its reach to commercial speech and narrows the standard of covered material from indecency to that which is "harmful to minors," and litigation over the provisions continues. *See generally* Ashcroft v. ACLU, 535 U.S. 564 (2002); ACLU v. Ashcroft, 322 F.3d 240 (3d Cir. 2003).

[19] *See* 18 U.S.C § 2257 (2000); 28 C.F.R. § 75 (2002).

[20] Search performed on Google using "18 U.S.C. 2257" (Dec. 10, 2002).

[21] *Id.*

[22] *See* FDA, *Advertising / Labeling Definitions*, *at* http://www.fda.gov/cder/handbook/adverdef.htm (last visited Apr. 30, 2003) (definition of advertising).

[23] *See generally, e.g.*, SEC v. SG, Ltd., 265 F.3d 42 (1st Cir. 2001).

[24] *See generally, e.g.*, FTC v. Ken Roberts Co., 276 F.3d 583 (D.C. Cir. 2001).

sought redress against the sources of Internet content. Injured parties can bring actions for defamation,[25] trade secret misappropriation,[26] and other common law torts. as well as copyright infringement actions, both civil and criminal.[27] In the latter case, after a narrow interpretation of the scope of the statute providing for criminal copyright infringement,[28] Congress amended the law to provide for criminal penalties for those who willfully infringe copyrights by distributing such works electronically, even without financial gain.[29]

Although private civil actions against the source of the offending material can effectively cause behavioral changes and directly target the "real wrongdoer in interest," a source-focused approach runs into several consistent enforcement difficulties that have pushed aggrieved parties to seek intervention in other phases of the transmission. First, to the extent that the would-be defendant is an individual rather than a firm, it may be difficult to pressure the defendant into restricting his or her behavior. Individuals can be made to react to threatened sanctions—indeed, perhaps with fewer reservations than corporations with legal departments capable of mounting a thorough defense or at least independent evaluation of legal claims asserted against them. But in the absence of a specific threat, they may simply behave as they wish, especially if they view the alleged wrong as *malum prohibidum* rather than *malum in se*. When they are one of apparently many engaging in the objectionable behavior—such as swapping illicit pornography or copyrighted material with other Internet users—the absence of an alert corporate compliance department may preclude them from believing that they have crossed an actionable legal line or that they face imminent sanction. Therefore they do not change their behavior prospectively.[30] Analogously, consider the relative ease with which state sales tax can be collected from a merchant, compared to the corre-

---

[25] *See, e.g.*, Blumenthal v. Drudge, 992 F. Supp. 44, 51 (D.D.C. 1998).

[26] *See, e.g.*, Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995).

[27] *See generally* U.S. v. Rothberg, No. 00CR85, 2002 WL 171963 (N.D. Ill. 2002) (finding criminal copyright infringement); Kelly v. Arriba Soft Corp., 77 F. Supp. 2d 1116 (C.D. Cal. 1999) (finding civil copyright infringement).

[28] *See generally* U.S. v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994).

[29] *See* No Electronic Theft Act, 17 U.S.C §§ 101, 506, 507 (2000); 18 U.S.C §§ 2319, 2319A, 2320 (2000), *available at* http://www.usdoj.gov/criminal/cybercrime/17–18red.htm (reversing the state of the law as interpreted in *LaMacchia*, 871 F. Supp. 535).

[30] *See* Steve Silberman, *Caught in the Kid Porn Crusade,* WIRED, Oct. 2002, *available at* http://www.wired.com/wired/archive/10.10/kidporn_pr.html; *see also* Declan McCullagh, *DOJ to Swappers: Law Is Not on Your Side*, CNET NEWS.COM, Aug. 20, 2002, *available at* http://news.com.com/2100-1023-954591.html.

sponding use tax owed but rarely paid by an individual purchaser for an out-of-state item sold by a seller unreachable by the state's power.[31]

Second, the technical ability to link objectionable source materials to a particular individual's identity is often difficult, adding expense and effort to an already cumbersome individual prosecution or private lawsuit. In some cases a user's ISP has been enlisted to assist in identifying the user.[32] For government action against illegal pornography, informal practice is augmented by common law warrant and statutory mechanisms through which ISPs can be enlisted to help identify sources of obscenity or other criminal activity.[33] ISPs can even help the government eavesdrop on packets of data from the source that might assist in an investigation or prosecution.[34]

Early attempts to obtain information from ISPs in private cases involved individuals seeking to identify the proper defendant of a personal defamation action or companies seeking the identities of employees or others alleged to be transmitting trade secrets or defamatory material.[35] This requires varying degrees of online detective work by the ISP itself, and, at least for private causes of action, ISPs have sought to be exempted from having routinely to provide such information.[36] More recently, the copyright industries have also attempted

---

[31] *See generally* Austan Goolsbee & Jonathan Zittrain, *Evaluating the Costs and Benefits of Taxing Internet Commerce*, 52 NAT'L TAX J. 413 (1999).

[32] *See, e.g.*, Melvin v. Doe 789 A.2d 696, 697 (Pa. 2001), *appeal granted by* 805 A.2d 525 (Pa. Aug. 20, 2002); Carl S. Kaplan, *Companies Fight Anonymous Critics with Lawsuits*, CYBER L.J., Mar. 12, 1999, *available at* http://www.nytimes.com/library/tech/99/03/cyber/cyberlaw/12law.html.

[33] *See* 18 U.S.C §§ 2702–2703 (2000); 47 U.S.C § 551 (2000).

[34] *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C §§ 2701–2711(2000); Cable Communications Policy Act, 47 U.S.C §§ 521–611 (2000); U.S. v. Kennedy, 81 F. Supp. 2d 1103, 1107, 1111–14 (D. Kan. 2000). *But see* Wiretap Act, 18 U.S.C. §§ 2510–2522 (2000); *id.* §§ 3121–3127 (regarding pen registers and trap and trace devices); *In re* Application of United States of Am. for an Order Pursuant to 18 U.S.C § 2703(D), 157 F. Supp. 2d 286, 288–92 (S.D.N.Y. 2001) (concluding that the government disclosure provision in § 551(h) of the CCPA does not apply to internet service provided via cable).

[35] *See, e.g.*, Melvin v. Doe 789 A.2d 696, 697 (Pa. 2001), *appeal granted by* 805 A.2d 525 (Pa. Aug. 20, 2002); Carl S. Kaplan, *Companies Fight Anonymous Critics with Lawsuits*, CYBER L.J., Mar. 12, 1999, *available at* http://www.nytimes.com/library/tech/99/03/cyber/cyberlaw/12law.html.

[36] *See generally, e.g.*, *In re* Subpoena Duces Tecum to Am. Online, Inc., No. 40570, 2000 WL 1210372 (Va. Cir. 2000). The fights over ISP assistance in uncovering and divulging the identities of users alleged—but not proven—to have engaged in actionable behavior is becoming known as the "John Doe" problem. *See* Chilling Effects, *John Doe Anonymity*, *available at* http://www.chillingeffects.org/johndoe (last visited Apr. 22, 2003); CyberSLAPP.org, *Homepage*, *available at* http://www.cyberslapp.org/intro.cfm (last visited Apr. 22, 2003).

to use this approach. Currently the Recording Industry Association of America (RIAA) and Verizon, in its role as an ISP, are litigating whether the RIAA can enforce a subpoena upon Verizon demanding identification of a Verizon user alleged to be illicitly sharing copyrighted material through Verizon using a peer-to-peer service.[37] As a consequence of specific federal legislation on the subject, the publishers appear to have the strongest case among various types of complainants.[38] 17 U.S.C. 512(h) appears to require a company like Verizon to respond to such a subpoena, and the doctrinal support for Verizon's refusal seems to rest upon a fairly tortured reading of the statute at issue.[39] Indeed, the trial court granted the RIAA's motion, ruling that "the subpoena authority of section 512(h) applies to all service providers within the coverage of the Act, including Verizon and other service providers falling within subsection (a)."[40]

Further, apart from the added effort of identifying a person behind a communication's source, some would-be defendants may simply be physically remote from the complaining jurisdiction. They may, therefore, be able to ignore an adverse judgment, or may interpose legal arguments based on jurisdiction, choice of law, or comity concerns. Reciprocal barriers between jurisdictions seem to exist in at least some circumstances. For instance, for First Amendment reasons a U.S. federal court indicated an aversion to enforcing damages flowing from a French court's finding of liability for transmission by a U.S. company into France of material that is illicit there.[41]

Finally, some private actors considering focusing efforts on data interdiction at the source may want to be more circumspect in interfering with users' data transfers. Government attorneys working to indict possessors of child pornography likely have little concern for offending them, but music companies and bands may wish to avoid alienating their fans through assiduous filing of lawsuits against them.

---

[37] *See* Recording Indus. Ass'n of Am. v. Verizon Internet Servs., 240 F. Supp. 2d 24 (D.D.C. 2002), *available at* http://www.techlawjournal.com/courts2002/riaa_verizon/20030121.asp; Motion to Enforce July 24, 2002 Subpoena Issued By This Court to Verizon Internet Services, Inc. and Memorandum in Support Thereof, *In Re*: Verizon Internet Services, Inc., (D.D.C. 2002) (No. 1:02MS00323), *available at* http://www.riaa.com/pdf/RIAAMotionToEnforce.pdf; RIAA, *RIAA Asks Court to Enforce Limited Information Subpoena*, Aug. 20, 2002, *available at* http://www.riaa.com/News_Story.cfm?id=547.

[38] *See* 17 U.S.C. § 512(h) (2000).

[39] *See id.*

[40] *See RIAA*, 240 F. Supp. 2d at 44.

[41] Yahoo! v. La Ligue Contre Le Racisme Et l'Antisemitisme, 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001).

Those in entertainment industries may want to be especially judicious about lawsuits when the pecuniary award is likely to be low relative to the burden of bringing the suit. Private parties have not typically pursued such cases unless to vindicate values apart from a purely economic calculus of loss, such as the Church of Scientology's actions to squelch online critics through claims—perhaps true—of copyright infringement.[42]

B. *Asserting Control upon the Source ISP*

Soliciting or forcing cooperation in blocking data transmissions at the next stage in Figure 1's data transfer—by interceding with the ISP of an offending source of Internet content—results in a different matrix of hurdles from that of going after the source itself. Aggrieved plaintiffs discover a generally more difficult legal position with a slightly easier enforcement prospect should the legal position be vindicated.

To explain, one must first distinguish between ISPs and online service providers (OSP). As ISPs, firms simply serve as a link between a particular client entity (such as an individual customer or a smaller, "downstream" ISP) and the Internet at large. But ISPs often do more than simply pass along packets as illustrated in Figure 1; they, along with other entities, also host content that is placed on their servers by others and thereby act as online service providers. In network terms, online service providers can properly be thought of as sources of packets. Legally speaking, however, the liability of OSPs for content hosted on their servers is a separate issue from the liability of the person who posted the material to the OSP's server, and the liability of a source's ISP, qua ISP, is another issue altogether. In the United States, legal attempts to place responsibility upon OSPs for others' content have met with mixed results, and the legal analyses employed typically vary with the type of content that is at issue.

Illegal pornography is, unsurprisingly, nearly uniformly contrary to the "acceptable use policies" of domestic OSPs, such as Yahoo! Geocities and Angelfire that maintain general purpose bulletin

---

[42] *See, e.g.*, Jim Lippard & Jeff Jacobsen, *Scientology v. the Internet: Free Speech & Copyright Infringement on the Information Super-Highway*, 3 Skeptic 3, 35–41 (1995), *available at* http://www.skeptic.com/03.3.jl-jj-scientology.html; Declan McCullagh, *Google Yanks Anti-Church Sites*, Wired News, Mar. 21, 2002, *available at* http://www.wired.com/news/politics/0,1283,51233,00.html.

boards, chat rooms, and home page hosting services.[43] Once alerted to the claimed existence of illegal pornography OSPs usually act expeditiously to remove it.[44] While the law may provide for responsibility for an intermediary's continued hosting of obscene content,[45] so far there has been no documented attempt by government authorities within the United States to hold OSPs responsible for illegal pornography placed on their servers by third parties in the absence of the OSP's specifically encouraging, participating in, or being clearly aware of the activity. For example, a recent investigation of illegal child pornography circulating within Yahoo! Groups appears to have resulted in no charges against or other repercussions for Yahoo! itself.[46] Outside the United States, charges of transmitting illegal pornography were once brought against the head of CompuServe's German subsidiary by Bavarian provincial prosecutors because CompuServe made available external Internet "newsgroup" feeds to its German customers that included such illegal material, but the resulting conviction was overturned by an appellate court.[47]

For the purpose of limiting illegal pornography, the most useful function accomplished by the existence of a source OSP distinct from the source of a communication may be that it routes data across state lines, even if both endpoints are within a state. This could be a predicate for invocation of obscenity importation statutes, and has been found so in at least one case of a communication between an Ohio

---

[43] *See* Yahoo! GeoCities, *Terms of Service*, *available at* http://docs.yahoo.com/info/terms/geoterms.html (last visited Jan. 11, 2003); Lycos (Angelfire), *Terms and Conditions*, *available at* http://info.lycos.com/legal/legal.asp (last visited Jan. 11, 2003).

[44] *See* Declan McCullagh, *Yahoo! in Porn Foe's Sights,* WIRED NEWS, Jun. 19, 2001, *available at* http://www.wired.com/news/politics/0,1283,44619,00.html.

[45] An argument to this effect might be based on the distributor function that both OSPs and bookstores serve. There is at least some prospect that bookstores could be held responsible for carrying obscene books. Under *Roth v. U.S.*, obscenity is not protected speech. 354 U.S. 476, 492 (1956). In that case, both (1) possession of obscene materials for sale and advertising and (2) mailing obscene materials, as in a mail-order business, were at issue. *Id.* at 480–81. The Court determined that states could prohibit these activities. *Id.* at 492–94. *Paris Adult Theatre I v. Slaton*, reiterated this notion, and specifically mentioned adult bookstores. 413 U.S. 49, 67–69 (1973). *Paris* suggested that, if a bookstore carried obscene materials, access to the bookstore could be restricted or even wholly denied. *Id.* at 58 n.7.

[46] *See generally* Silberman, *supra* note 30.

[47] *See* Edmund L. Andrews, *German Court Overturns Pornography Ruling Against CompuServe,* N.Y. TIMES, Nov. 18, 1999, *available at* http://www.nytimes.com/library/tech/99/11/biztech/articles/18compuserve-germany.html.

defendant and an Ohio minor that took place through a Virginia ISP/OSP.[48]

For common law claims, some close cases under state defamation law in the early 1990s[49]—some favorable to OSPs, others less so—sparked a movement by OSPs to urge Congress to create a pocket of immunity. Congress did so in section 230(c) of the Communications Decency Act of 1995.[50] Section 230(c) provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[51] Section 230(c) provides that such declaration should have no effect on intellectual property law or federal criminal or telecommunications law, but that "no cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[52] This provision has been construed broadly for state common law claims, effectively cutting off any redress for those alleging harm resulting from an OSP's continued hosting of defamatory or other content actionable under common law.[53] The provisions were not challenged and therefore not struck down in the earlier litigation over the separate pornography-related aspects of the law and therefore remain in effect.[54]

For intellectual property, the doctrine is murkier. A patchwork of cases generally eschews claims of direct copyright infringement for OSP intermediaries who host allegedly infringing material provided by others,[55] at least so long as the OSP did not appear to have a hand in selecting or otherwise more carefully processing the work.[56] Part of

---

[48] *See* State v. Maxwell, 767 N.E.2d 242, 248–50 (Ohio 2002).

[49] *See generally, e.g.*, Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont v. Prodigy Serv. Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. 1995).

[50] 47 U.S.C. § 230(c) (2000).

[51] *Id.*

[52] *Id.*

[53] *See, e.g.*, Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980, 984–86 (10th Cir. 2000); Zeran v. Am. Online, Inc., 129 F.3d 327, 330–34 (4th Cir. 1997); Blumenthal v. Drudge, 992 F. Supp. 44, 49–52 (D.D.C. 1998); Jonathan Zittrain, *The Rise and Fall of Sysopdom*, 10 HARV. J.L. & TECH. 495, 509–12 (1997).

[54] *See, e.g.*, Zittrain, *supra* note 53, at 506–12.

[55] *See generally* Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distrib., 983 F. Supp. 1167 (N.D. Ill. 1997) (the real party in interest that created a Web site might be held liable for copyright infringement, but not the OSP hosting that Web site); Sega Enter. Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996); Religious Tech. Ctr. v. Netcom On-Line Comm., 907 F. Supp. 1361 (N.D. Cal. 1995).

[56] *See Playboy*, 991 F. Supp. at 549 (in which the OSP acted more as a simple commercial portal, retrieving copyright images from elsewhere on the Internet and selling them to

the Digital Millennium Copyright Act of 1998 (DMCA), without speaking to the ultimate issue of substantive liability for infringement by those hosting others' content, provides a "safe harbor" process of immunity from damages should OSPs act expeditiously to remove allegedly infringing content once notified in a particular structured fashion.[57] It also allows for a further process of "counter-notification" whereby the source of the content can assert back to the OSP that the material is in fact not infringing.[58]

When intermediaries do not themselves host content, but are merely conduits for it—as both the source and destination ISPs in Figure 1 would be—they are flatly immune from damages arising from domestic copyright infringement claims,[59] and at least as immune as OSPs within the other doctrinal areas.[60] To find otherwise spawns an *ad disasterum* argument by which ISPs would find themselves in a comparable position to telephone companies asked to take responsibility for the illegal content of calls traversing their networks—leaving them possibly out of business, and facing an impossible (and possibly itself lawbreaking)[61] task of monitoring subscribers' communications.

For the purposes of limiting the unauthorized distribution of intellectual property, the DMCA's statutory immunitv for ISPs is carefully structured to block only actions for damages.[62] Another section of the Act provides for a process bv which a court, under certain conditions, can grant injunctive relief.[63] In the case of a source ISP, there may be an order requiring a termination of the offending source's account with the ISP or a termination of the rest of the world's access to the user's assigned Internet destination, if the infringing material resides there.[64] For an OSP, an injunction may be framed as an order requiring termination of the OSP user's account or removal or blocked access to the material on the OSP's servers.[65]

---

its own subscribers); Playboy Enters. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993) (in which the defendant appeared to be processing the contents of his bulletin board service in a more hands-on way than a typical large-scale OSP).

[57] 17 U.S.C. § 512(c) (2000).

[58] *Id.* § 512(g).

[59] *Id.* § 512(a).

[60] *See, e.g.*, Lunney v. Prodigy Servs. Co., 723 N.E.2d 539, 541 (1999) (defamation).

[61] *See* 18 U.S.C § 2511 (2000).

[62] *See* 17 U.S.C § 512(a).

[63] *See id.* § 512(j).

[64] *See id.*

[65] *See id.*

It may be this prospect of injunctive relief that has led to publishers' practice of asking ISPs to monitor and police activity taking place on their networks. For example, the Motion Picture Association of America (MPAA) sent a letter to Harvard University complaining of allegedly infringing material hosted by someone on the Harvard network.[66] Harvard, in turn, discovered that the material in question was hosted by an undergraduate on his own computer attached to the Harvard dormitory network.[67] Harvard sent a letter to the student alerting him that such hosting was in violation of its network policies and threatening sanctions should the student continue to host such material.[68] Notices by publishers to ISPs seeking action by the ISPs against individual users have become routine, with firms springing up to accept the outsourced task of identifying points of infringement within a network and generating complaint letters to the relevant ISPs.[69] Some publishers have even attempted to get source ISPs—universities, in particular—to change network architecture to prevent the use of peer-to-peer networking completely.[70] While most have declined to do so, at least one university, in the same week it sent a letter to a publisher refusing to take action, announced a network bandwidth conservation policy that clamped most outgoing Internet traffic

---

[66] Letter from Courtney Bickel Lamberth, Allston Burr Senior Tutor, Winthrop House, Harvard University, to Aaron Koller, Undergraduate Student, Harvard University (Oct. 17, 2001) (on file with author), *available at* http://www.chillingeffects.org/copyright/notice.cgi?NoticeID=212.

[67] *Id.*

[68] *Id.*

[69] For example, NetPD provides "protection services to copyright owners whose material is being pirated through the internet." NetPD, *History*, *available at* http://www.netpd.com/a.htm (last visited Jan. 11, 2003). NetPD employs patented search technology to locate infringing material online, and "[s]earch results are used for detailed strategic planning, to assist in tactical execution, for evidence in support of major litigation, and/or as the basis of a copyright control program." *Id.* Automated removal of infringing material is also possible: "[a]t the client's request, NetPD uses an automated process to carry out rapid, bulk removal of infringing files being offered for free downloading. The process is capable of being controlled by filters which can ensure a 'fan friendly' approach in which different actions can be taken against sites based on the profile of the site. If and when the files reappear, the infringing sites are detected, challenged and removed again." *Id.*

[70] *See, e.g.*, Letter from Howard E. King, Attorney, on behalf of Metallica and Dr. Dre, to Neil L. Rudenstine, President, Harvard University (Sept. 6, 2000), *available at* http://www.itcom.itd.umich.edu/mp3/mp3ltr.html. Similar letters were sent to Columbia University, University of Virginia, Stanford University, Boston University, Georgia Institute of Technology, Massachusetts Institute of Technology, Princeton University, University of Michigan, University of California at Berkeley, University of California at Los Angeles, and approximately fifteen other large universities.

from student dormitories, effectively dampening the university's contribution to worldwide file sharing/piracy.[71]

For enforcement purposes, it may be easier to find and engage an ISP regarding its legal responsibilities than a single subscriber of that ISP. But if a revelation of subscriber identity is sought, success merely pushes the enforcement problem back to dealing with a potentially unreachable source. Moreover, when the ISP in question is located overseas, cooperation of any sort is fraught with as many barriers as those for faraway individual sources of illicit material. Indeed, to the extent that particular activities are driven away from mainstream ISPs, they may find a home in more obscure places and through more obscure hosts—still only a click away from most consumers of content around the world. This is precisely the behavior we see with senders of unsolicited bulk email. They are difficult to track down individually and while they may be shunned as clients by mainstream ISPs (who in turn do not want to be penalized by other ISPs as part of informal group enforcement of norms against spamming), they can often use ill-configured or intentionally permissive overseas servers as sending points for spam.[72]

C. *Asserting Control at the Destination*

The "destination" end of Figure 1 has witnessed intensive attempts to intercept certain categories of Internet content under specific circumstances. Attempting to block illicit material at the moment just prior to a given Internet user's exposure to it has been attempted when there is a disjunction between the destination computer's owner and user, and the computer owner desires that the user avoid certain Internet destinations, as parents might wish for children. Personal computer filtering software allows a computer owner to control or at least monitor some aspects of the computer's use, and some filtering software is even built directly into Internet Web browsers.[73] Most fil-

---

[71] *See* Kate L. Rakoczy, *Computing Services Restricts Outbound Traffic on Network,* HARV. CRIMSON, Feb. 16, 2001, *available at* http://www.thecrimson.com/article.aspx?ref=103233.

[72] David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 363, 367 (2001).

[73] *See, e.g.*, Microsoft Internet Explorer, *Configuring Content Advisor Settings*, *available at* http://www.microsoft.com/windows/ie/using/howto/contentadv/config.asp (last visited Jan. 10, 2003); N2H2, *Homepage*, *available at* http://www.N2H2.com (last visited Jan. 10, 2003); Net Nanny, *Homepage*, *available at* http://www.netnanny.com (last visited Jan. 10, 2003); Secure Computing, *Homepage*, *available at* http://www.securecomputing.com/index-js.shtml (last visited Jan. 10, 2003); SurfControl, *Homepage*, *available at* http://www.surf-

tering efforts are devoted to identifying and screening out pornographic material, illegal or not, though the taxonomy of sites filtered can be quite extensive.[74]

Government attempts to force computer owners to configure their computers to screen out illicit content have been primarily limited to laws conditioning federal funding on particular screening by computers in schools and libraries,[75] or decisions by such public entities themselves to implement screening for their students and patrons.[76] In the United States, these efforts have met stiff, still unresolved, First Amendment challenges, grounded largely in filtering software's inaccurate categorization and therefore overbroad blocking of Web sites.[77]

Many corporate environments have voluntarily adopted filtering software for pornography,[78] in part due to fears of liability for suborning a hostile work environment.[79] Copyright-infringing material is now being rooted out via the same channels. The Software and Information Industry Association encourages corporate workers to re-

---

control.com (last visited Jan. 10, 2003); Websense, *Homepage*, *available at* http://www.websense.com (last visited Jan. 10, 2003).

[74] *See, e.g.*, Secure Computing, *Products-at-a-Glance*, *available at* http://www.securecomputing.com/index.cfm?sKeys=86 (last visited Jan. 10, 2003); SurfControl, *URL Category List*, *available at* http://www.surfcontrol.com/products/content/internet_databases/url_category_list/default.aspx (last visited Jan. 10, 2003); Websense, *Advanced Filtering with Premium Group Categories*, *available at* http://www.websense.com/products/premiumgroups/index.cfm (last visited Dec. 5, 2002); Websense, *Websense Master Database: Categories*, *available at* http://www.websense.com/products/about/database/categories.cfm (last visit-ed Dec. 5, 2002).

[75] *See generally* Children's Internet Protection Act, Pub. L. No. 106–554, 114 Stat. 2763A–335 (2002) (conditioning libraries' receipt of grants under the Library Services and Technology Act, 20 U.S.C §§ 9101–9176 (2000), and "E-rate discounts" for Internet access and support under the Telecommunications Act, 47 U.S.C § 254 (2000)).

[76] *See* Mainstream Loudoun v. Bd. of Trs. of Loudoun County Library, 24 F. Supp. 2d 552, 556, 570 (E.D. Va. 1998).

[77] *See id.* at 566–68, 570; *see also* Am. Library Ass'n v. U.S., 201 F. Supp. 2d 401, 436–50, 470–96 (E.D. Pa. 2002).

[78] An April 2000 American Management Association Research Report found that 63% of large and medium-sized businesses monitor their employees' Internet use, and 40% block access to unauthorized or inappropriate Web sites. *See generally* Terry Carter, *Untangling the Web: Law Firms Seek to Avoid Injudicious Use of Internet Resources*, A.B.A. J., Sept. 2001, *available at* http://www.websense.com/company/news/misuse/01/090101.cfm; *see also* David Greenfield, *Web@Work Employer Survey 2001: Termination and Litigation*, *available at* http://www.websense.com/company/news/research/webatwork-employer2001.pdf (indicating that 71% of companies block pornography).

[79] *See* N2H2, *Internet Usage and Legal Liability*, *available at* http://home.zen.co.uk/assets/pdf/liability_whitepaper.pdf (last visited Jan. 11, 2003).

port the use of unlicensed copies of software within companies to bring infringement suits and accompanying demands for settlements.[80] And further, at least one filtering manufacturer has announced a "Liability Protector Module" for its software, by which companies can scan their employees' computers for illicit software, music, and other digital content.[81]

Certainly, controlling access to illegal content by using filtering software only works when the computer's owner is convinced or compelled to install it, and that is not an easy task when the user owns the computer. A number of digital rights management initiatives seek to solve this problem by designing computers that inherently manage content according to publishers', rather than users', wishes. Such computers would include limitations, if not outright filtering, in users' operating systems and software so that sympathetic third-party ownership of users' computers is not necessary. Successful implementation, however, remains months, if not years, away. Furthermore, U.S. implementation might not take place in the absence of controversial, possibly constitutionally suspect, federal legislation designed to compel hardware and software makers to agree with content producers on the standards for such systems and to make the resulting standards mandatory.[82] In an apparent attempt to avoid passage of standard-setting legislation, in January 2003 two computer industry groups and the RIAA issued a joint statement on policy principles that focused on their willingness to work together on digital rights management.[83] Notably absent from the inter-industry accord, however, was the MPAA, another key voice on the publisher's side of the debate.[84] It remains to be seen whether the push to pass legislation on this issue will be renewed by the MPAA or other interested parties.

To be sure, possession of illicit pornography or the receipt of unauthorized copyrighted material can be actionable in its own right,

---

[80] *See* SIIA, *Anti-Piracy: Report Piracy*, *available at* http://www.siia.net/piracy/report/default.asp (last visited Dec. 6, 2002) (providing web forms to report piracy).

[81] *See* Websense, *Macrovision and Websense Announce New Partnership to Prevent Unauthorized Digital Material in the Workplace*, *available at* http://www.websense.com/company/news/pr/02/100702b.cfm (last visited Jan. 11, 2003).

[82] *See* Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. (2002); Security Systems Standards and Certification Act, Draft Senate Bill 107th Cong. (2001); Jonathan L. Zittrain, *Taming the Consumer's Computer*, N.Y. Times, Mar. 11, 2002. at A21.

[83] *Technology and Record Company Policy Principles, available at* http://www.bsa.org/usa/policvres/7_principles.pdf (last visited Feb. 12, 2003).

[84] *See id.*

but the threat of liability may have attenuated effects on individuals as consumers of content, just as it has its limits with individuals as sources of such content.[85] And apart from any deterrent effect, prosecutions would have to proceed laboriously against one user at a time to make progress on the problem. The publishers have had little stomach to mount copyright infringement actions against mere recipients of protected material without further evidence of a desire and capacity to traffic in it.[86] Government prosecutors targeting possession of illegal pornography appear to pick their individual prosecutions carefully to conserve resources—focusing on people in positions of special trust or responsibility.[87]

D. *Asserting Control upon the Destination ISP*

The "destination ISP" has been perhaps the most neglected of Figure 1's possible points of control. Attempts to fix on ISPs legal responsibility for content that they carry from the network at large to their own customers are rare, and legal authority to do so is nearly nonexistent.[88] Source ISPs benefit from a relationship with a particular subscriber and have a distinct ability to control that subscriber's behavior through the crude lever of terminating the subscriber's account. Destination ISPs, however, are simply "off ramps" for others' data solicited by the destination ISPs' customers and are remote from faraway activities engaged in and/or hosted by others.

Destination ISPs are functionally equivalent to source ISPs with respect to providing identifying information about their own subscribers to those who might have a legal claim against them—such as when a claim might be made for possession of illicit content, rather than distribution of it, or when one might view the destination as "importing" such data, much as a source could be viewed as "exporting" it. There is, however, no instance of a destination ISP being found liable in its own right for passing along digital contraband requested from a remote source by one of its customers.

Attempts are now underway to change the apparent immunity of destination ISPs, perhaps because exercising control through the des-

---

[85] *See generally* Silberman, *supra* note 30.

[86] *See id.*

[87] *See id.*

[88] From a legal perspective, an attempt to hold a destination ISP responsible for the content it carries would likely be viewed as functionally equivalent to attempting to enforce liability against source ISPs since both ISPs are acting as "mere conduits." *See supra* notes 54–55 and accompanying text.

tination ISP is comparatively appealing from an enforcement point of view. Destination ISPs are by their nature local, easing jurisdictional concerns since ISPs will have equipment and assets within the reach of the interested jurisdiction. ISPs will conform their activities to fit legal requirements and incentives, and while there are many ISPs, the vast majority of Internet subscribers in the United States with Internet access obtain their access from a small handful of providers.[89] Further, many smaller providers are themselves resellers of larger providers' services, such that pressure applied strategically to the concentric ISPs serving smaller ISPs—one or two "dolls" up in a Matryoshka sequence of destination ISPs—can cover large swaths of subscribers. In essence, stopping a set of packages at the sender's drop box has its own efficiencies but involves the difficulties of reaching a faraway sender and his or her drop box. In a world in which there are only a handful of international couriers entering one's jurisdiction, stopping such identifiable packages after they have left the drop box but before they have reached their respective destinations might prove more effective, even if the sender's packages fan out across multiple delivering firms from their single initial point of entry into the flow of carriage.

Imposing controls on destination ISPs has been the approach of governments that wish to control the flow of content over the Internet but who cannot project that control beyond their boundaries. For example, both Saudi Arabia and China have country-wide filtering regimes in place.[90] While the filtering regimes are far from perfectly effective at preventing access to undesired data, they represent the most effective point of blockage along the path of data from faraway places

---

[89] Based on year-end 2000 revenue figures, the top ten ISPs in the U.S. accounted for more than 66% of the total market share; the top four companies accounted for just over half of the market share. Denise Pappalardo, *The ISP Top Dogs*, NETWORK WORLD INTERNET SERVICES NEWSLETTER, May 30, 2001, *available at* http://www.nwfusion.com/newsletters/isp/2001/00846039.html. According to India Infoline Sector Reports on Internet Service Providers AOL is the largest retail ISP, with over 22 million subscribers and 40% of that market segment. *India Infoline Sector Reports: Internet Service Providers*, *at* http://www.indiainfoline.com/sect/itsp/ch05.html (last visited Apr. 30, 2003). AOL's share is more than the next twenty ISPs' shares combined. *Id.* UUNet has a 26% market share in the business segment, 43% in the wholesale segment, and 17% in the value-added services market; UUNet has around double the market share of its nearest competitor in all three segments. *Id.*

[90] Jennifer 8. Lee, *Companies Compete to Provide Saudi Internet Veil*, N.Y. TIMES, Nov. 19, 2001, at C1–4, *available at* http://www.websense.com/company/news/companynews/01/111901.cfm.

into the personal computers of Internet users within those countries, and they are maintained regularly by those countries.[91]

II. Filtering Objectionable Content Using Destination ISPs: The Pennsylvania Maneuver

The first sustained effort in the United States at content control through destination ISPs is now under way. The Commonwealth of Pennsylvania has, in essence, sought to replicate the Chinese filtering scheme within Pennsylvania's borders, substituting the narrow category of alleged illegal child pornography for the much broader range of material that China censors via destination ISPs.

A law passed in February 2002 adds a section to the Pennsylvania criminal code that, among other things, provides the following:

> GENERAL RULE.—An internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the internet service provider is notified by the Attorney General pursuant to subsection (g) that child pornography items reside on or are accessible through its service.[92]

The law is careful to state that the destination ISP is not under any affirmative obligation to monitor the flow of data through its routers for child pornography.[93] But once notified by the state attorney general according to a structured process that "child pornography items" can be found at a faraway source, the ISP must disable access to that source within five business days under threat of criminal penalty.[94] Noncompliance constitutes a misdemeanor for the first two offenses and a felony for subsequent ones.[95]

---

[91] *See* Michael S. Chase & James C. Mulvenon, You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies, at xii (2002), *available at* http://www.rand.org/publications/MR/MR1543/; Lee, *supra* note 90, at C1–4; Jonathan Zittrain & Benjamin Edelman, *Documentation of Internet Filtering Worldwide*, *available at* http://cyber.law.harvard.edu/filtering (last updated Apr. 3, 2003).

[92] 18 Pa. Const. Stat. § 7330(a) (2002) (Section 7330 was repealed by 2002, Dec. 16, P.L. 1953, No. 226, Section 2, but it was replaced by an essentially identical set of statutes. 18 Pa. Cons. Stat. §§ 7621–30 (2003)).

[93] *See id.* § 7330(b).

[94] *Id.* § 7330(a), (c).

[95] *Id.* § 7330(c).

The first publicly known demand for a block under the statute happened in July 2002, when an official in the state attorney general's office sent a series of "informal notices" to ISP WorldCom demanding that particular Internet sources of data be made inaccessible to Pennsylvania WorldCom subscribers.[96] WorldCom refused to block the sites on the basis of those informal notices.[97] As a result, the state attorney general obtained a formal order from a state criminal trial judge requiring WorldCom to disable access to five Internet points of presence found by the judge—on the basis of affidavits supplied by the attorney general—to have "probable cause" to contain child pornography.[98] Several days later, WorldCom notified the attorney general's office that a few of the sites listed in the order had already been disabled at the source—perhaps as a result of WorldCom's alerting the remote hosting OSP that the material violated the OSP's terms of service.[99] Two sites not blocked at the source were then blocked by WorldCom.[100]

If a constitutional challenge were brought against Pennsylvania's statute, it might be struck down for a variety of reasons. Some of its potential infirmities may inform a more general discussion of the constitutional prospects for other forms of control of destination ISPs for other purposes, such as to limit the unauthorized movement of copyrighted material, and also shed light on the propriety of such control as a public policy matter.

A. *Objections Arising from Locally-Mandated Control of a Global Network*

WorldCom insists that it does not have the technical ability to discriminate in its packet routing between Pennsylvanians and non-Pennsylvanians as customers; thus the mandated blocks have been

---

[96] *See* Marnie Affidavit of Probable Cause, In the Matter of the Application of D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania for an Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography (July 2002) (No. Misc. 689) (on file with author).

[97] *Id.*

[98] *See* Sept. 17, 2002 Order of Court of Common Pleas of Montgomery County, Pennsylvania, In the Matter of the Application of D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania for an Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography (July 2002) (No. Misc. 689) (on file with author).

[99] Letter from Craig Silliman, Director of Technology and Network Legal, WorldCom, to John J. Burfete, Jr., Chief Deputy Attorney General, Office of Attorney General of Pennsylvania (Sept. 23, 2002) (on file with author).

[100] *Id.*

implemented for all WorldCom subscribers, regardless of location.[101] The prospect of local regulation overreaching because of an all-or-nothing impact on Internet users has led at least one court to strike down such regulation on dormant commerce clause grounds.[102]

The law in question was a New York State sibling to the Federal CDA, and without reaching the First Amendment questions later resolved against the CDA by the United States Supreme Court, a federal district court issued an injunction blocking enforcement of the state law because, among other reasons, "the unique nature of cyberspace necessitates uniform national treatment."[103] To be sure, the New York law imposed responsibilities on out-of-state sources of Internet transmissions that could arrive at New York destinations and Pennsylvania's law seeks to limit its reach only to the activities of ISPs within the state. To the extent that WorldCom's technical claim is credited, however, a court might be skeptical of a law that would necessarily affect WorldCom customers outside Pennsylvania's jurisdiction.[104]

While WorldCom's technical claim of all-or-nothing filtering may be literally true, it also may be subject to change with the application of technical expertise. Routing protocols and hardware built by people can be revised by people: a change to the code could permit "zoning" previously not possible.[105] Indeed, a panel of experts convened by a French judge to evaluate the prospect of OSP Yahoo! limiting the online distribution of displays of Nazi memorabilia within France—while not limiting such display to non-French parties—concluded that such geographic zoning was possible, at least when attempted by an OSP seeking to categorize the locations of its visitors.[106] Their findings paved the way for the French court to ask that Yahoo! block the illegal material, secure that France would not be necessarily imposing its own laws de facto on the rest of the world should Yahoo! accede.[107]

---

[101] *Id.*

[102] *See* Am. Library Ass'n v. Pataki, 969 F. Supp. 160, 183–84 (S.D.N.Y. 1997).

[103] *Id.* at 184.

[104] *See id.* at 183–84.

[105] *See generally, e.g.*, Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996).

[106] *See* Interim Court Order, County Court of Paris, France (Nov. 22, 2000), *available at* http://www.cdt.org/speech/international/001120yahoofrance.pdf (containing the Opinion of the Consultants Ben Laurie, François Wallon and Vinton Cerf, La Ligue Contre Le Racisme Et l'Antisemitisme and L'Union Des Etudiants Juifs De France v. Yahoo!, Inc. and Yahoo France).

[107] *See id.*

B. *Objections Arising from Process*

The substantive regulation of child pornography, as a form of obscenity, is generally outside the ambit of First Amendment review.[108] The categorization of material as obscene, however, is itself fraught with First Amendment implications. Pennsylvania's law contemplates a judge's finding that there is "probable cause" that the material to be blocked is child pornography.[109] But the finding is made ex parte and the source of the material, the real party in interest, is not notified that the material is slated for state-mandated interception.[110] By analogy, if the government ordered teamsters ferrying newspapers from the printing presses to newsstands to divert their cargo to the town dump because it was deemed in an ex parte proceeding to have "probable cause" of containing obscene material, the order would be a prior restraint subject to the highest level of scrutiny.[111] The newspaper publisher could likely object further on due process grounds if not alerted to the order and given a chance to object.[112] Further, blocking a given destination under Pennsylvania's law has no particular time limit.[113] This, then, is as if the government banned not only a

---

[108] *See generally* New York v. Ferber, 458 U.S. 747 (1982) (classifying child pornography as a category of material outside the protection of the First Amendment).

[109] *See* 18 PA. CONST. STAT. § 7330(f) (2002).

[110] That the determination may be made ex parte is provided in 18 PA. CONST. STAT. ANN. § 7330(f). While there is detailed provision for the targeted ISP to get notice of an action under this statute, there is no provision in § 7330 for notification of the source of the offending material. *See* 18 PA. CONST. STAT. § 7330(g).

[111] Under *Near v. Minnesota ex rel. Olson*, prior restraints were found to be highly disfavored. 283 U.S. 697 (1931). The only exception the Court allowed to the unconstitutionality of prior restraints was the "troopship exception," which is roughly equivalent to very strict scrutiny. *See id.* at 715–16. The disfavored character of prior restraints was also evident in the Court's decision in *New York Times v. U.S.*, where two justices found an absolute bar to prior restraints, one justice indicated that they would be subject to strict scrutiny, and two justices recognized that U.S. constitutional law provides "extraordinary protection against prior restraints." 403 U.S. 713, 714–15, 726–27, 730 (1971).

[112] The ex parte procedure employed in this hypothetical would run afoul of the Court's holding in *Freedman v. Maryland*, that certain procedural protections were required to avoid the unconstitutionality of a prior restraint. 380 U.S. 51, 60 (1965). Among other procedural considerations, the *Freedman* Court indicated that a judicial determination in an adversary proceeding must be available before the restraint has finality. *See id.* at 59. Since putting the papers in the dump would likely be considered "final," the ex parte proceeding would probably not pass constitutional muster. *See id.* at 60. Also under procedural due process law, namely the Court's decision in *Mathews v. Eldridge*, the necessary procedural protections would be determined by balancing the *Mathews* factors: the significance of the private interest that would be affected by the government action; the extent to which additional procedural safeguards would reduce the risk of error; and the public's interest in resolving the matter quickly and efficiently. 424 U.S. 319, 335 (1976).

[113] *See* 18 PA. CONTS. STAT. § 7330 (lacking a time limit provision).

given issue of a newspaper, but all future newspapers emanating from a given printing press, without checking to see if future editions contained the material claimed to provide the justification for the ban.[114]

To be sure, as Section I explains, the source of a data transfer on the Internet is quite often anonymous, especially in the case of possibly illicit material—making notifications difficult and possibly constituting a form of waiver of notification.[115] As part of the growing number of cases surrounding "John Doe", however, subpoenas, source ISPs and OSPs asked to reveal what they know about the identities of their difficult-to-track subscribers have developed voluntary mechanisms to notify such subscribers of these requests.[116] Some jurisdictions have permitted those subscribers to then argue—while their identities remain unknown—for a quashing of the subpoena as the real party in interest.[117]

Prospective viewers of the Internet sites slated for blocking undoubtedly have constitutional interests of their own to advance.[118] Internet users attempting to access sites blocked under the law will not be informed why the sites are unavailable.[119] Given the nature of routing as described in Figure 1, the block could be taking place anywhere along the chain of packet-passing, and current routing protocols offer scant opportunity for an explanation—packets are either routed or not, and an Internet user's software simply reports a failure to connect should the circuit not be completed for any reason.

An apparent system of informal notifications by law enforcement to destination ISPs, resulting in blocked sites without explanation to the Internet users attempting to access them, or even formal notifications to ISPs still not readily made available to the public, is deeply troubling as a policy matter. Given the apparent reluctance of Pennsylvania ISPs to demand formal invocation of the law, much less to litigate a use of it, such a system would seem to give the government significant power to infringe Internet users' First Amendment rights, without the users' knowledge that the government was acting at all. Of course, the law could be amended to provide for public notifica-

---

[114] This is precisely what was found to be unconstitutional in *Near*. 283 U.S. at 721.

[115] *See supra* Section I.

[116] *See generally* Doe v. 2TheMart.com Inc., 140 F. Supp.2d 1088 (W.D.Wash. 2001).

[117] *Id.*

[118] *See, e.g.*, Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Counsel, 425 U.S. 748, 756–72 (1976) (finding that consumer have First Amendment-protected interests in receiving certain commercial information).

[119] *See* 18 Pa. Cons. Stat. § 7330 (2002) (failing to mention any notice to Internet users).

tion of sites blocked. To do so, the government must create a public index to illegal material often only partially blocked, since there might be ISPs beyond the state boundaries not subject to the order.

Alternatively, ISPs themselves could maintain the public lists. ISPs might be the best custodians for the purposes of conveying to the public when a failure to reach an Internet point of presence is due to government intervention. If each state government, as well as the federal government, maintained its own lists, interested Internet users would have to search every jurisdiction with relevant regulations to see if a site has been ordered blocked in the absence of a system to aggregate data across jurisdictions. Either way, many users would have to speculate whether an ISP with whom they are not in direct privity might be affecting their attempts to reach a site—a surmise that would have to be grounded in knowledge of routing tables and the user's ISP's relation to other ISPs within the Matryoshka doll chain or peers within the cloud. For example, users of uunet, a WorldCom subsidiary, would have to know that their packets were going through WorldCom's servers. Users at a particular university might find their packets routed through a WorldCom backbone and thus dropped if in relation to a banned site without realizing that they should be consulting WorldCom's list of blocked sites for the explanation, since they were in fact relying on WorldCom to carry those packets along the chain.

C. *Objections Arising from Overblocking*

Refusing to carry packets is a crude instrument of Internet discipline. ISPs and operators of backbone routers within the cloud have developed the means to selectively ignore packets labeled as to or from a specific IP address as a form of "Internet death penalty," principally reserved to prevent denial-of-service attacks or large-scale spam in progress.[120] Such attacks can consist of a stream of packets from a given set of sources targeted to overwhelm a particular destination, and can cause congestion along the chain of ISPs carrying those packets, particularly those close to the destination. Tools developed by ISPs to implement the Internet death penalty against hackers and spammers enable those ISPs to then hew to a Pennsylvania court order asking for the same treatment of sources of allegedly obscene material.

---

[120] *See* On-Line Hacker Jargon File: Version 4.3.3, *Internet Death Penalty* (Sept. 20, 2002), *available at* http://jargon.watson-net.com/lexicon.asp?L=O.

Internet routing and numbering characteristics described earlier, however, make blocking on a broad scale difficult for an ISP, and suggest persistent overblocking in many circumstances.[121] First, broad scale blocking is difficult because each router along the chain of a transmission maintains a table of possible destinations, just as neighbors passing mail from one house to the next need to recall which houses are westward and which are eastward. To be able to document simply that "all Los Angeles addresses are westward" compresses the handling of many individually addressed letters into one easy rule of thumb. Indeed, one might know that all letters bearing ZIP codes beginning with nine should be passed to the west. Routers behave similarly, and pausing to consider a special rule or exception for a single destination increases the router's work. China, however, appears to have overcome this limit as it embeds thousands of exceptions in otherwise standard routing tables serving its Internet users,[122] suggesting that WorldCom and others could come to do so as well.

Second, and technically more vexing, IP addresses may be reassigned from time to time, or even moment to moment. Pennsylvania's order to WorldCom demanded blocking for distinct "uniform resource locators," one level of abstraction higher than IP addresses.[123] Should the site found at http://www.blockedsite.com/blockedsite move to a new or additional IP address while retaining its URL—a feature explicitly intended for domain names and the URLs in which they are often found—an ISP's routing tables would continue blocking a now irrelevant IP address, and possibly the new digital denizen there, as IP addresses, like telephone numbers, are recycled. At the same time, the routing tables would permit packets to pass to and from the illicit site's URL at its new IP destination. WorldCom adverted to this problem in response to Pennsylvania's attorney general, indicating that it would continue to check the sites to be blocked to see if they retained their URL's but directed them to new IP ad-

---

[121] *See supra* Section I.

[122] *See* Jonathan Zittrain & Benjamin Edelman, *Empirical Analysis of Internet Filtering in China* (Nov. 2002), *available at* http://cyber.law.harvard.edu/filtering/china/; *see also* CHASE & MULVENON, *supra* note 91, at xii; Jonathan Zittrain & Benjamin Edelman, *Real-Time Testing of Internet Filtering in China, available at* http://cyber.law.harvard.edu/filtering/china/test/ (last visited Apr. 23, 2003).

[123] Sept. 17, 2002 Order of Court of Common Pleas of Montgomery County, Pennsylvania, In the Matter of the Application of D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania for an Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography, (July 2002) (No. Misc. 689) (on file with author).

dresses. Blocking individual URLs, rather than IP addresses, is not impossible, but the tools to reliably do so on a large scale appear to exist only among countries devoting particular energy to countrywide filtering, such as Saudi Arabia, and in a recent and sporadic complement to its IP filtering, China.[124]

Retaining blocking at the IP level also means that a site hosting multiple, unrelated users' work, such as http://www.blockedsite.com/illegalmaterials and http://www.blockedsite.com/innocuousmaterials, could find all its users blocked by various destinations' ISPs since all users' work can be found at the same IP address. The Pennsylvania/WorldCom case included a demand to block material made available by a user of one such overseas host, Spain's OSP terra.es.[125] The attorney general's cover letter to WorldCom accompanying the court's order acknowledged this all-or-nothing dilemma, suggesting that WorldCom could escape it by persuading terra.es to remove the offending page.[126] WorldCom did just that,[127] but had terra.es not complied, Pennsylvania citizens would have been denied access to substantial amounts of speech they possess a constitutional right to see, viz. the content created by terra.es users unrelated to the allegedly obscene content created by a single terra.es user. Denying access would create the very dynamic that so troubled the U.S. Supreme Court as it struck down most provisions of the Communications Decency Act.[128]

There is another form of overblocking to consider. Even if a site containing offending content can be solely targeted, all Internet activity to and from that source is blocked. A computer might serve as both a source of Internet Web content and as a surfing tool for its individual user; blocking by the destination ISP renders that computer a pariah with respect to the destination ISP's customers and peers for all purposes.

To the extent the lack of subtlety in blocking is unavoidable, perhaps it could be permissible. Of more importance is a sense of just how much tinkering would have to occur to provide for a nuanced

---

[124] *See* Zittrain & Edelman, *supra* note 91.

[125] Notice Under 18 Pa. Const. Stat. § 7330, In the Matter of the Application of D. Michael Fisher, Court of Common Pleas of Montgomery County, Pa. Criminal Division (July 2002) (No. Misc. 689) (on file with author).

[126] Letter from D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania, to Craig Silliman, Attorney, WorldCom Network and Facilities Legal Team (Sept. 17, 2002) (on file with author).

[127] Letter from Craig Silliman, *supra* note 99.

[128] *See supra* Section I.A.

system of content control. Courts, perhaps rightly, might expect such tinkering to take place when suitable opportunities are presented. For example, the online filesharing service Napster was ordered to undertake changes to its technical architecture to block unauthorized copyrighted material from being indexed for its users, while allowing innocuous material to pass.[129] The Napster example represents a baby-splitting compromise of the sort that the Supreme Court was not squarely asked to consider when it ruled on the status of VCRs as instruments of contributory copyright infringement.[130] Rather, the Court balanced the devices' legitimate uses against illegitimate ones and imagined that the devices would be either wholly banned or wholly allowed, without being asked to contemplate ordering manufacturers to attempt to rework the devices to proscribe illegitimate uses.[131] If ISPs are capable of learning to filter more exactingly, the *ad disasterum* arguments that so powerfully bar impulses to ask ISPs to control or monitor their networks vanish.

III. Implications of Asserting Control at the Destination ISP

Pennsylvania's approach is one in a series of laws designed to force destination ISPs to assist in Internet content control. On October 10, 2002, the New Jersey State Assembly took up a bill nearly identical to Pennsylvania's.[132] On October 21, 2002, a Canadian member of Parliament reintroduced a proposed Internet Child Pornography Prevention Act, incorporating Pennsylvania's approach with the additional prospect of requiring destination ISPs to monitor for obscene content.[133]

Pornography is not the only content at issue. A German court has held that approximately sixty destination ISPs in the state of North-Rhine Westphalia can be lawfully asked to block German customer

---

[129] A&M Records v. Napster, Inc., 2000 WL 1009483, at *8 (N.D. Cal. July 26, 2000).

[130] Universal City Studios, Inc. v. Sony Corp. of Am., 480 F. Supp. 429, 469 (D.C. Cal. 1979). Without dwelling on possible approaches to reengineer the VCR to better restrict infringing uses while permitting noninfringing ones, the Court may well have considered playback-only VCR's differently from those with both recording and playback capabilities.

[131] *Id.* at 468–69.

[132] Assembly No. 2863, 210th Leg. (N.J. 2002), *available at* http://www.njleg.state.nj.us/2002/Bills/A3000/12863_I1.PDF (no longer available) (not yet enacted into law, the bill is available online).

[133] Internet Child Pornography Act, R.S.C., ch. C-234 (2002) (Can.), *available at* http://www.parl.gc.ca/37/2/parlbus/chambus/house/bills/private/C-234/C-234_1/372010bE.html.

access there to two U.S.-hosted Web sites determined by the German government to contain banned Nazi propaganda.[134]

Further, in a short-lived case that would have proved an interesting test of the DMCA's provisions on injunctions,[135] thirteen record companies filed a lawsuit in August 2002 to force five major domestic ISPs, in their role as destination ISPs and backbone providers within the Internet cloud,[136] to block their customers' Web access to www.listen4ever.com, an allegedly unauthorized China-based source of the plaintiff companies' copyrighted music.[137] The record companies' complaint echoes many of the limitations previously described for each of the alternatives to intervention at the destination ISP phase of data transit: the identities of the actual operators of the listen4ever site are unknown;[138] the source ISP is itself in China, a location allegedly selected precisely to place it beyond the reach of U.S. copyright law;[139] and the source ISP has ignored cease and desist letters.[140] Furthermore, Internet users within the United States ("destinations" in Figure 1) could easily find the site, navigate its English language prompts, and search for and download the copyrighted music.[141] Days after filing the suit, the plaintiffs withdrew their claims,[142] perhaps because the listen4ever site had apparently vanished.

Unlike the scope of Pennsylvania's law, the Federal provisions under which the record companies sought the injunction appear to limit compelled blocking to sites hosted outside the United States.[143] Furthermore, in weighing a request made pursuant to the copyright statute, the court is to consider, among other things, the burden such an injunction would place upon the defendant ISPs, whether less

---

[134] *See Germany: The Idea of Internet Providers Blocking Illegal Content is Questionable*, 8 SAFER INTERNET, Nov. 2001, at 3, *available at* http://www.saferinternet.org/news/safer8.htm; *see also* Heise Online, *Haftung für rechtswidrige Inhalte fraglich*, Oct. 15, 2001, *available at* http://www.heise.de/newsticker/data/hod-15.10.01-000/ (for a description in German of the first German court's decision in this case); Vigilant.tv, *Heise: Duesseldorf Arranges Immediate Blockage of Nazi Websites*, Sept. 13, 2002, *available at* http://vigilant.tv/article/2162 (describing second German court's reiteration of the blocking order).

[135] 17 U.S.C. § 512(j) (2000).

[136] *See supra* Figure 1.

[137] *See generally* Complaint, Arista Records, Inc. et al. v. AT&T Broadband Corp. et al., No. 02 CV 6554 (S.D.N.Y. Aug. 2002) (on file with author).

[138] *Id.* ¶ 39.

[139] *Id.* ¶ 40.

[140] *Id.* ¶ 43.

[141] *Id.*

[142] Notice of Voluntary Dismissal, Arista Records, Inc. et al. v. AT&T Broadband Corp. et al.. (KMW) (S.D.N.Y. Aug. 21, 2002) (No. 02 CV 6554) (on file with author).

[143] 17 U.S.C. § 512(j)(1)(B) (2000).

burdensome but equally effective means of dealing with the problem exist, and the extent to which the requested blocking might interfere with access to noninfringing material at other online locations.[144] Thus the copyright-protecting mechanisms for enlisting ISP assistance in blocking sources of illicit data set a higher threshold than is evident in the Pennsylvania counterpart provisions against child pornography for imposition of a blocking order. The additional showing required in the copyright setting is fact-based, and those facts are evolving as more and more pressures are placed upon backbone providers and destination ISPs to discriminate in their carriage of data. As ISPs augment their tools to hew to requirements like Pennsylvania's, the technical burden on them to block sites under the DMCA's injunction provision will naturally drop, and the effectiveness of the block—at least for the overseas sites which are the most nettlesome to the complainants and specifically provided for in the Act—is far greater than contemplated intervention at other points in the chain.

In tandem with blocking technology refinements, adjustments to the legal principles for mandated blocking by destination ISPs and backbone providers can make such interventions less constitutionally suspect. For example, the law might provide for procedures to attempt to give notice to and an opportunity to object to the real party in interest, i.e. the source of the alleged illicit material. Legislators might also contemplate procedures for reviewing blocked sites at regular intervals to see if blocking is still merited under the original standard of the injunction. Legislators could also provide for a technically sophisticated list of blocked sites, so that the affected public can know why—and on whose authority—it is prevented from reaching a given source of information on the Internet.

If the legal provisions are refined as much as possible to account for the sort of objections previously described and technical adjustments are made to minimize the technical burden to ISPs asked to block particular sources of data from their customers, what problems remain?

A. *Overblocking*

Filtering on the basis of IP addresses remains a crude metric along several dimensions. First, when a given IP address corresponds to a computer hosting content from several distinct and unrelated

---

[144] *Id.* § 512(j)(2).

users—as in the terra.es example from the Pennsylvania court order to WorldCom—blocking that IP address presents an all-or-nothing proposition. Of course, hosts like terra.es would themselves likely adjust for major blocking of their content by destinations that matter to them—by either adopting acceptable use policies in line with local law to avoid receiving the "Internet death penalty," or carving different users' sites into different IP addresses precisely to prevent spillover effects. And, with China and Saudi Arabia leading the way, destination ISPs (if not cloud-residing backbone providers) might learn to filter on the basis of a URL instead of an IP address.

Second, blocking of a given source of data—whether by IP address or by URL—typically blocks all such data between that source and the blocking ISP's client destinations. Technical adjustments might seek to make filtering more granular, but this requires anticipation of the ways in which the source computer is being used, and for what purposes. Again, China leads the field.[145] Beginning in the fall of 2002, China's destination ISPs began to search data packets for particular sensitive keywords.[146] When specific keywords are found, access by the user in China to the source of data in question is cut off for a designated period of time.[147] For example, a search for "Jiang Zemin" on Google from some Chinese computers will result in part of a results page being loaded, followed by a loss of access to Google for a certain period of time.[148]

B. *Violation of End-to-End Principles*

Those who designed the Internet's protocols espouse an engineering rule of thumb—keep the middle of the network simple and implement fancy functions at the endpoints.[149] They also observe that complexity is the bane of scalability.[150] Accordingly, Internet engineers recommend that even such routine features as error checking are best implemented apart from basic Internet Protocol routing. Re-

---

[145] *See* Jonathan Zittrain & Benjamin Edelman, *Replacement of Google with Alternative Search Systems in China,* Sept. 10, 2002, *available at* http://cyber.law.harvard.edu/filtering/china/google-replacements/.

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] J.H. Saltzer et al., End-to-End Arguments in System Design, Second International Conference on Distributed Computing Systems 509–512 (Apr. 1981), *available at* http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.mss.

[150] *Id.*

cently the end-to-end argument has taken on a political dimension; it has been adopted by those arguing against corporate mergers that might diversify the incentives and strategies of network players who previously simply sought to move packets from one point to another as quickly as possible.[151] For example, a company that is both a backbone provider and a source of content on the Internet might begin to privilege the passage of its own data over those of its competitors. Such actions are both undesirable and best avoided by preventing any diffusion of the typical network provider's corporate mission.

The technical aspect of the end-to-end argument suggests a warning against blocking data transmissions at any point in Figure 1 apart from the source and destination endpoints. To implement common blocking—aside, perhaps, from the extreme cases in which network providers ignore certain packets if they are deemed part of a hacking attempt—would risk the reliability of the network itself. Such concerns might be best understood as echoes of the claim that hundreds or thousands of exceptions to default routing tables, which would be required for widespread ISP-level source IP address blocking, could slow everyone's routing to a crawl, and naturally result in inconsistent results depending on what path one's data happened to take across the entirety of Figure 1. Inconsistent results on the basis of network provider variance outside or within the network cloud breaks the illusion of "one click" nearness of every point to every other network point. Further, users wishing to evade blocking will come up with kludges that themselves put further stress on the network; some will use virtual private networks or other proxy to relay data inaccessible from their point of presence through a point that is mutually accessible. While any given workaround might be blocked and problems resulting from the discontinuity between the network functions of IP addressing and the desired use of IP addresses or URLs to implement filtering of objectionable content may eventually be solved, one must still be cautious about the spiral of patches, tweaks, and overlays that cumulatively could severely impair the Internet as it exists now. When "tussles" between network parties are fought out through the network

---

[151] *See, e.g.*, Mark Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era,* 2000 Berkeley Law & Economics Working Papers, *available at* http://www.bepress.com/blewp/default/vol2000/iss2/art8; Written Ex Parte of Professor Mark A. Lemley and Professor Lawrence Lessig, *In re* Application for Consent to the Transfer of Control of Licenses MediaOne Group, Inc. to AT&T Corp., (F.C.C. 1999) (CS No. 99–251), *available at* http://cyber.law.harvard.edu/works/lessig/cable/fcc/fcc.html.

protocols themselves, the efficient functioning of the network is threatened.[152]

Of course, these technical objections are persuasive in inverse correlation to the extent to which would-be regulators feel aggrieved by the Internet's status quo. So, too, perhaps are the political end-to-end arguments, which in their general form can be constructed to inveigh against any form of blockages along the network path that deviate from standard protocols which call for nondiscriminatory routing. But regulators might want to consider the "portability" effects of causing network carriers to develop smarter tools to filter data, whether at the IP address level or in a more refined way. Portability concerns drove at least one objection to a set of filtering standards that could be used to categorize Web sites; even if the filtering on the basis of those standards was intended to take place at an endpoint (typically the destination, through user-installed filters), the fear was that governments could use the framework to mandate country-wide filtering of objectionable content.[153] Changes in the network's functioning to accommodate blockages for pornography or intellectual property deemed truly proscribable could in turn make it substantially easier for authoritarian regimes to enhance their nascent country-wide destination ISP filtering systems. A meta-ideology of network freedom—even understanding that such freedom carries distinct harms within one's first-level ideology—might be necessary. At the very least, one might wish to take into account end-to-end violation and portability effects when weighing the costs and benefits of mandated filtering for an ostensibly narrow purpose and conclude that the solution is overall disproportionately large in relation to the acknowledged problems.

Conclusion: Proposing a Network User's Bargain

The Internet's persistent tensions with many prevailing legal frameworks arises in large part from its distributed peer-to-peer reach: an ability to bring together one individual with another when neither is accustomed to direct regulation of what they choose to say or see. The notion that some content is so harmful as to render its transmission, and even reception, actionable—true for certain categories of

---

[152] David D. Clark et al., *Tussle in Cyberspace: Defining Tomorrow's Internet,* SIGCOMM (2002), *available at* http://www.acm.org/sigcomm/sigcomm2002/papers/tussle.pdf.

[153] Lawrence Lessig, *Tyranny in the Infrastructure,* 5.07 Wired (July 1997), *available at* http://www.wired.com/wired/5.07/cyber_rights_pr.html.

both intellectual property and pornographic material—means that certain clicks on a mouse can subject a user to intense sanctions. Consumers of information in traditional media are alerted to the potential illegality of particular content by its very rarity; if a magazine or CD is available in a retail store its contents are likely legal to possess. The Internet severs much of that signaling, and the ease with which one can execute an Internet search and encounter illegal content puts users in a vulnerable position. Perhaps the implementation of destination ISP-based filtering, if pressed, could be coupled with immunity for users for most categories of that which they *can* get to online in the natural course of surfing.

The most worrisome outcome is one in which filtering creeps into the system in an ad hoc way, without formal evaluation of the standards by which it is taking place or the criteria by which ISPs choose to accede to such filtering when the requests are informal, or an ability to fully evaluate the nature of the sites filtered. To have sources of Internet content simply disappear from the perspective of others—at first for some rather than all—portends enormous but subtle control over who can say what on a formerly free-for-all medium. The Internet's brilliant methodology of data routing—a flexible set of intermediaries functioning in tandem yet with little central coordination—offers multiple opportunities for control that are only now coming into focus for regulators. Such control cannot be accepted, even if initiated for substantively good intentions, without the most exacting of processes to avoid abuse, including a comprehensive framework where sovereigns' actions to block material are thoroughly documented and open to challenge. If carefully implemented and circumscribed, however, government mandated destination-based filtering stands the greatest chance of approximating the legal and practical frameworks by which sovereigns currently sanction illegal content apart from the Internet. Attention to distinct points of control, then, can force cyber-libertarians to dispense with procedural or jurisdictional concerns about regulation and instead either to rely flatly on theories of free speech and action that go beyond even the most liberal governments' current allowances, or to invoke Internet exceptionalism to explain why it should be indeed freer than its analog media counterparts.