Internet Points of Control

I. Introduction

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

If the overlapping categories of pornography and intellectual property have been drivers of public Internet use and therefore growth, they have also therefore created the most powerful pressures to make the Net and the people using it more "regulable." Originally designed by academics for the quick, cheap, and perfect copying and sharing of data – without inquiry or worry about its nature, or that of the people on either end of a given transfer – the Net's architecture has prominently stymied efforts of control by those who believe they are harmed by its less innocuous uses. If one were to randomly pluck 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.

These attempts to impose control have met with mixed success, and a vigorous debate about the extent to which the comparatively anarchic status quo will prevail continues. I wish to add to that debate – in which I incline to the view that control will trump anarchy – by examining a recent experiment in control launched by the U.S. commonwealth of Pennsylvania as it tries to restrict the flow of illegal pornography available to its denizens. This experiment, grounded in a state law by which any

---

2 See DICK THORNBURGH & HERBERT S. LIN (EDS.)., YOUTH, PORNOGRAPHY, AND THE INTERNET 72-73 (2002) ("Compared to the totality of the content on the public World Wide Web, adult oriented sites account for a relatively small fraction (about 1.5 percent). However, these 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.")
4 See, e.g., RAYMOND S. R. KU, MICHELE A. FARBER & ARTHUR J. COCKFIELD, CYBERSPACE LAW (2002) (over 70% of the cases involved pilfering or prurient material), PETER B. MAGGS, JOHN T. SOMA & JAMES A. SPROWL, 2002 SUPPLEMENT TO INTERNET AND COMPUTER LAW (2002) (over 60% of the cases involved pilfering or prurient material), or MARK A. LEMLEY, PETER S. MENELL, ROBERT P. MERGES & PAMELA SAMUELS, SOFTWARE AND INTERNET LAW (2000) (80% of the cases in the Internet law portion of the book involved pilfering or prurient material).
internet service provider can be required to block access by Pennsylvanians to a given Internet destination under threat of criminal liability, is a novel approach, heretofore untried by both anti-pornography’s champions and their counterparts: publishers seeking to limit intellectual property piracy.

The experiment is notable because it requires such an audacious departure from the Internet’s techno-political foundations, enlisting 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. Internet service providers can serve as Net 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 Net, 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 in turn by the technical tools developed by Internet service providers conscripted to accommodate it – could cause a sea change in the Net’s regulability. Such a change would allow Internet usage to be brought 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 persuasively frame their objections to it – and make some case that those objections are truly fatal to the adoption of the general strategy of client-side ISP filtering. By sorting the Net’s brief but intense history of content control struggles into a framework of points of technical intervention along a canonical Net data path, I will explain why the Pennsylvania approach is such a significant departure from prior attempts at regulation, and then explore its desirability should it become commonplace across a range of regulatory purposes. I conclude that the current implementation will prove unwieldy, but that 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 as a technical matter and as a matter of fairness to those censored.

II. 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 Net. 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](image)

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”), most frequently when the computer is attached through a dial-up modem connection. A packet of data is passed from the computer whose user created it, with a label indicating that computer’s IP address, to the computer’s internet service provider. Typically each computer has only one ISP, whose function is to initiate the packet’s journey from the computer to its destination, and pass back in return any packets labeled for that computer’s IP address. The packet’s destination is also identified by its particular IP address.

Most internet service providers themselves have internet service providers – 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

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 and Unix environments.
Such multiple hops are usually necessary because Internet data moves in typically 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 in rather staggered fashion moved 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 the receiving ISP appears to have the computer at the packet’s indicated destination as one of its customers (or customer’s customers). 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 a 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 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, or if they are, 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. Each 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 Net – 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 has requested and is to receive 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 usually neither computer users nor software
developers need concern themselves with the details of Internet routing. However, efforts 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, 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 a matter of both engineering and policy.

Within the U.S. legal framework, once the data in question is properly thought of as “contraband,” i.e. at least in some instances its possession or transmission could be legally actionable, one must still show that an entity targeted for legal action to prevent the data’s transfer or use is indeed thought properly asked to do something about that data. Along with this hurdle for legal responsibility are also varying barriers to practical enforcement of any legal requirement. For those seeking to block illicit content, the challenge is to apply pressure to an entity within the chain of data transfer whose selection maximizes the chances of both legal responsibility and successful enforcement of that responsibility.

II.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 access to 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 to – or be compelled to – and the source of a communication is almost always most clearly and directly legally responsible for it, at least compared to those further along the transmission chain.

Early efforts to combat illegal pornography focused on Figure 1’s source of the pornographic content. Operators of online bulletin boards who offered subscriptions for access to obscene photographs were found criminally liable under the standard Federal anti-obscenity laws9 – and answerable for their actions several states away, under the destination state’s standards for obscenity.10

The Communications Decency Act of 1995 made it a crime to, among other things, initiate the transmission of “indecent” material to minors, and its presumed high impact on the behavior of those placing information on the Net was the source of its Constitutional vulnerability.11 The relevant provisions of the CDA were found unconstitutional precisely because they so effectively restrict the material available to children. By encouraging, through threat of criminal liability, self-censorship by speakers on the Internet at the very source of the speech, parents would be deprived of the ability to fine-tune what their children could see on the Net. Also troubling for

10 See U.S. v. Thomas, 74 F.3d 701 (6th Cir. 1996).
Constitutional review were the spillover effects on adults' own access to speech. The worry was that rather than setting up systems to distinguish kids from adults, speakers wishing to avoid 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 proxy for adulthood. Thus, the law’s deleterious effect on the availability of material not Constitutionally proscribable for adults was thought to be constitutionally fatal.\(^\text{12}\)

This 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 lesson that legal duties placed upon the source of Internet content can have powerful effect is more general.\(^\text{13}\) Indeed, other provisions placing legal requirements on those who are the source of pornographic material regardless of 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.\(^\text{14}\) A Web search on a citation to the law’s provision, “18 USC 2257,” yields approximately 75,000 results – the overwhelming majority of which appear to be statements of compliance with the law offered by pornographic web sites.\(^\text{15}\)

Other Federal regulatory efforts focus quite naturally on the source of an Internet communication: the U.S. Food and Drug Administration has long held medical and pharmaceutical web sites responsible for their claims,\(^\text{16}\) as has the Securities and Exchange Commission,\(^\text{17}\) and the Federal Trade Commission.\(^\text{18}\)

Apart from public agencies’ application of statutory and administrative law, aggrieved private parties have also sought redress against the sources of Internet content. Defamation,\(^\text{19}\) trade secret misappropriation,\(^\text{20}\) and other common law torts against them can be found, as can actions for copyright infringement, both civil and criminal.\(^\text{21}\)

---

\(^{13}\) Congress has taken at least one additional (if so far 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) (2002). 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 Ashcroft v. ACLU, 122 S. Ct. 1700 (2002).
\(^{15}\) Search performed on Google using “18 USC 2257.” (Oct. 16, 2002.)
\(^{17}\) See, e.g., S.E.C. v. SG, Ltd., 265 F.3d 42 (1st Cir. 2001).
\(^{21}\) Civil copyright infringement was found in Kelly v. Arriba Soft Corp., 77 F. Supp.2d 1116 (C.D. Cal. 1999); criminal copyright infringement was found in U.S. v. Rothberg, No. 00CR85, 2002 WL 171963 (N.D. Ill. Feb. 4, 2002).
In the latter case, after a narrow interpretation of the scope of the statute providing for 
criminal copyright infringement, Congress hastened to amend the law to provide for 
criminal penalties for those who willfully infringe copyright by distributing such works 
electronically even without financial gain.22

While going after the source of a contested Internet transmission is usually the most 
direct and natural course of action from a legal standpoint, and there is plenty of 
evidence of actual effect on large swaths of behavior, 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, especially before any problem has been 
identified. 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 the 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 coming 
to believe that they have crossed an actionable legal line or that they face imminent 
sanction, thereby changing their behavior prospectively.23 (Consider the relative ease 
with which state sales tax can be collected from a merchant, compared to the 
corresponding 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.24)

Further, the technical ability to link objectionable source materials to a particular 
individual’s identity is often elusive, adding expense and effort to an already-
cumbersome individual prosecution or private lawsuit. At times a user’s internet service 
provider has been enlisted to assist in identifying a user, in early cases by individuals 
seeking to identify the proper defendant of a personal defamation action or by 
companies seeking the identities of employees or others alleged to be transmitting trade 
secrets or defamatory material.25 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 to routinely provide such information.26

---

22 See the No Electronic Theft Act (<http://www.usdoj.gov/criminal/cybercrime/17-18red.htm>), reversing the state 
23 See Steve Silberman, Caught in the Kid Porn Crusade, WIRED, October 2002, available online 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, August 20, 2002, available online at <http://www.news.com.com/2100-
1023-954591.html>.
24 Austan Goolsbee & Jonathan Zittrain, Evaluating the Costs and Benefits of Taxing Internet Commerce, 52 
NATIONAL TAX JOURNAL 413 (1999).
Kaplan, Companies Fight Anonymous Critics with Lawsuits, NEW YORK TIMES, March 12, 1999, available online at 
26 See, e.g., In re Subpoena Duces Tecum to America Online, Inc., 2000 WL 1210372 (Va. Cir. Ct. 2000). The 
fights over ISP assistance in uncovering and divulging the identities of users alleged – but not proven – to have
have also adopted this approach. Currently the Recording Industry Association of America and Verizon, in its role as an ISP, are litigating whether the RIAA can enforce a subpoena upon it demanding identification of a Verizon user alleged to be illicitly sharing copyrighted material through Verizon using a peer-to-peer service. Thanks to specific Federal legislation on the subject, the publishers appear to have the strongest case among various types of complainants; 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.

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 – or even assist in eavesdropping on packets of data from the source that might assist in an investigation or prosecution.

Apart from the added effort of identifying a person behind a communication’s source, some would-be defendants even once identified may simply be physically remote from the complaining jurisdiction, and thus able to ignore an adverse judgment, or may interpose legal arguments based on jurisdiction, choice of law, or comity concerns. Reciprocal barriers seem to exist in at least some circumstances, with a U.S. federal court indicating an aversion, for First Amendment reasons, to enforcing damages flowing from a French court’s finding of transmission by a U.S. company into France of material that is illicit there.

Finally, from the point of view of some private actors considering focusing efforts at data interdiction at the source, it may be best 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, especially when the pecuniary award in the suit 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

---

27 See <http://www.riaa.com/News_Story.cfm?id=547>; Motion to Enforce July 24, 2002 Subpoena Issued By This Court to Verizon Internet Services, Inc. and Memorandum in Support Thereof, No. 1:02MS00323 (D.D.C. 2002), available online at <http://www.riaa.com/pdf/RIAAMotionToEnforce.pdf>.


Church of Scientology’s actions to squelch online critics through claims – perhaps valid – of copyright infringement.30

II.B. Asserting control upon the source ISP

Seeking to solicit or force cooperation in blocking data transmissions at the next stage in Figure 1’s data transfer – by interceding with the internet service provider 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 here a generally more difficult legal position, if a slightly easier enforcement prospect should the legal position be vindicated.

To explain, one must distinguish between Internet service providers and online service providers. As ISPs, firms simply serve as a link between a particular client entity (e.g. an individual customer or a smaller, “downstream” ISP) and the Internet at large. But Internet service providers often do more than simply pass along packets as illustrated in Figure 1; they, along with other entities, also can act as “online service providers,” hosting content – and thus be thought of as the source of it in network terms – placed there by others, quite often their customers. In the United States, legal attempts to place responsibility upon OSP’s for others’ content have met with mixed results, often demarcated along substantive doctrinal lines, with responsibilities varying depending on whether the nature of the objectionable content hosted is pornographic, illicit material under common law (such as defamatory material), or infringing of copyright.

Illegal pornography is, unsurprisingly, nearly uniformly against the “acceptable use policies” of domestic OSP’s such as Yahoo! Geocities and Angelfire that maintain general purpose bulletin boards, chat rooms, and home page hosting services,31 and once alerted to its claimed existence such OSP’s usually act expeditiously to remove it.32 While the law may provide for responsibility for an intermediary’s continued hosting of obscene content,33 so far there has been no documented attempt by government authorities within the United States to hold such OSP’s responsible for illegal pornography placed on their servers by third parties in the absence of the OSP specifically encouraging, participating in, or being clearly aware of the activity; for

31 Yahoo! GeoCities’ Terms of Service are available online at <http://docs.yahoo.com/info/terms/geoterm.html>; the Lycos (Angelfire) Terms and Conditions are posted at <http://info.lycos.com/legal/legal.asp>.
33 There’s at least some prospect that bookstores could be held responsible for carrying obscene books. Under Roth v. U.S., 354 U.S. 476 (1957), obscenity is not protected speech. 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. The Court determined that states could prohibit these activities. Paris Adult Theatre I v. Slaton, 413 U.S. 49 (1973), reiterated this notion, and even specifically mentioned adult bookstores (413 U.S. at 58 fn 7) and suggested that, if a bookstore carried obscene materials, access to the bookstore could be restricted or even wholly denied.
example, a recent investigation of illegal child pornography circulating within Yahoo! Groups appears to have made no claim against Yahoo! itself.\textsuperscript{34} 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 case was abandoned after a nominal conviction.\textsuperscript{35} For the purpose of limiting illegal pornography, the most useful function accomplished by the existence of a source OSP distinct from the source (or destination) 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 defendant and Ohio minor that took place through a Virginia ISP/OSP.\textsuperscript{36}

For common law claims, some close cases under state defamation law in the early 1990's\textsuperscript{37} – some favorable to OSP's, others less so – sparked a movement by OSP's for Congress to create a pocket of immunity. It did so in section 230(c) of the Communications Decency Act of 1995. 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," and 230(e) 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."\textsuperscript{38} This has been construed broadly for state common law claims, effectively cutting off any redress by those alleging harm thanks to an OSP's continued hosting of defamatory or other content actionable under common law, and the provisions were not challenged and therefore not struck down in the earlier litigation over the separate pornography-related aspects of the law.\textsuperscript{39}

For intellectual property, the doctrine is murkier: there is a patchwork of cases generally eschewing claims of direct copyright infringement for OSP intermediaries who host allegedly infringing material provided by others,\textsuperscript{40} at least so long as the OSP did not

\textsuperscript{36} See State v. Maxwell, 95 Ohio St.3d 254, 767 N.E.2d 242 (Ohio 2002).
\textsuperscript{38} 47 U.S.C. §230(c), (e) (2002).
appear to have a hand in selecting or otherwise more carefully processing the work.\footnote{See Playboy Enterprises, Inc. 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, and Playboy Enterprises, Inc. v. Webworld, 991 F.Supp. 543 (N.D. Tex. 1997), \textit{aff'd}, 168 F.3d 486 (5th Cir. 1999), in which the OSP acted more as a simple commercial portal, retrieving copyright images from elsewhere on the Internet and selling them to its own subscribers.} Part of the Digital Millennium Copyright Act of 1998, 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 OSP’s act expeditiously to remove allegedly infringing content once notified in a particular structured fashion,\footnote{17 U.S.C. §512(c) (2002).} and 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.\footnote{See 17 U.S.C. §512(g) (2002).}

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 U.S. copyright infringement claims,\footnote{See 17 U.S.C. §512(a) (2002).} and at least as immune as OSP’s within the other doctrinal areas.\footnote{E.g., in a defamation setting, see Lunney v. Prodigy Services Co., 94 N.Y.2d 242 (1999).} To find otherwise spawns an \textit{ad disasterum} argument by which ISPs would find themselves in the position of, say, telephone companies asked to take responsibility for the illegal content of calls traversing their networks – possibly out of business, facing an impossible (and itself possibly lawbreaking)\footnote{See the Electronic Communications Privacy Act, 18 U.S.C. §2511 (2002).} task of monitoring subscribers’ communications.

For the purposes of limiting the unauthorized distribution of intellectual property, the DMCA’s statutory immunity for ISPs is carefully structured to block only those actions for damages.\footnote{See 17 U.S.C. §512(j) (2002).} Another section of the act provides for a process by which a court, under certain conditions, can grant injunctive relief: 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; in the case of 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.\footnote{See 17 U.S.C. §512(a) (2002).}

It may be this prospect of injunctive relief that has led to a practice by publishers of asking ISPs to monitor and police activity taking place on their networks. For example, the Motion Picture Association of America sent a letter to Harvard University complaining of allegedly infringing material hosted by someone on the Harvard network. Harvard, in turn, discovered that the material in question was hosted by an
undergraduate on his own computer attached to the Harvard dormitory network. 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. Notices by publishers to ISPs seeking action by the ISPs against individual users have become routinized, 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. 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 at all. 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 from student dormitories, effectively dampening the university’s contribution to worldwide file sharing/piracy.

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 what is sought is simply a revelation of subscriber identity, the result pushes the problem back to the source, and for overseas ISPs, 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.


50 See <http://www.netpd.com>. Net PD provides “protection services to copyright owners whose material is being pirated through the internet.” Net PD employs patented search technology to locate infringing material online, and “search 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.” Automated removal of infringing material is also possible: “at the clients 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.”

51 See, e.g., Letter from Howard E. King, Attorney, on behalf of Metallica and Dr. Dre to Neil L. Rudenstine, President, Harvard University (September 6, 2000) (available online at <http://www.itcom.umd.umich.edu/mp3/mp3ltr.html>). Similar letters were sent to Columbia, University of Virginia, Stanford, Boston University, Georgia Institute of Technology, MIT, Princeton, the University of Michigan, the University of California at Berkeley and UCLA, and approximately 15 other large universities.


II.C. Asserting control at the destination

The “destination” end of Figure 1 has witnessed intensive attempts at intercepting 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 disjunct between who owns the destination computer and who uses it, and the computer owner desires that the user avoid certain Internet destinations, as parents might wish for children. Personal computer filtering software exists to allow a computer owner to control or at least monitor some aspects the computer’s use, and some is even built directly into Internet web browsers.\(^{54}\) Most filtering efforts are devoted to identifying and screening out pornographic material, illegal or not, though the taxonomy of sites filtered can be quite extensive.\(^{55}\)

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,\(^{56}\) or decisions by such public entities themselves to implement screening for their students and patrons.\(^{57}\) These efforts have met with stiff First Amendment challenges, still unresolved, grounded largely in their inaccurate categorization and therefore overbroad blocking of Web sites.\(^{58}\)

Many corporate environments have voluntarily adopted filtering software for pornography,\(^ {59}\) in part perhaps because of fears of liability for suborning a hostile work environment.\(^ {60}\) The Software & Information Industry Association encourages corporate workers to report on the use of unlicensed copies of software within companies for the
purposes of bringing infringement suits and accompanying demands for settlements, and 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.

To be sure, such filtering only works when the owner of the computer can be convinced or compelled to install it; in the common case of the user himself or herself owning the computer, this is not easy. 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, but successful implementation remains months if not years away, and perhaps will not take place in the absence of controversial (and possibly Constitutionally suspect) Federal legislation designed to compel hardware and software makers to come to terms with content producers on the standards for such systems – and to make the resulting standards mandatory.

To be sure, possession of illicit pornography or copyrighted material can be actionable in its own right, but the threat of liability may have attenuated effects on individuals as consumers, just as it has its limits with individuals as sources of such content, and apart from any deterrent effect prosecutions would have to laboriously proceed one user at a time to make progress on the problem. The publishers have had little stomach to mount copyright infringement actions against mere possessors of copied material without further evidence of a desire and capacity to traffic in it, and government prosecutors targeting possession of illegal pornography appear to pick their individual prosecutions carefully – focusing on people in positions of special trust or responsibility – to conserve resources.

II.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 legal responsibility for content carried by Internet service providers from the network at large to their own customers are rare, and legal authority to do so traditionally nearly nonexistent. Source ISPs at least 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 are simply “off ramps” for others’ data solicited by the destination ISPs’
customers and thus much more remote from faraway activities engaged in, and/or hosted by, others.

Destination ISP’s are functionally equivalent to source ISP’s with respect to providing identifying information about their own subscribers to those who might have a legal claim against them – 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 as much as viewing the source as “exporting” it – but there is 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 that, perhaps because, should the law be accommodating, exercising control through the destination ISP is comparatively appealing from an enforcement point of view. Destination ISPs are by their nature local – if the worry is about the online material to which residents of a U.S. state or, for Federal law purposes, all those within the United States, have access, then ISPs serving those people will have equipment and assets within the reach of the interested jurisdiction. The ISPs are firms that will seek to conform their activities to fit legal requirements and incentives, and while there are many ISPs, the vast majority of those in the United States with Internet access obtain that access from a small handful of providers.\(^{65}\) 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 for the difficulties of reaching a faraway sender and drop box pair; in a world in which there are only a handful of international couriers entering one’s jurisdiction, stopping such identifiable packages after they’ve left the drop box but before they’ve reached their respective destinations might prove even more effective, even if the sender’s packages might fan out across multiple delivering firms from its initial single point of entry into the flow of carriage.

This certainly 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, and while they 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

---

\(^{65}\) 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 online at <http://www.nwfusion.com/newsletters/isp/2001/00846039.html>. According to India Infoline Sector Report on Internet Service Providers, June 25, 2002, AOL is the largest retail ISP, with over 22mil subscribers and 40% of that market segment. AOL’s share is more than the next 20 ISP’s shares combined. 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. Online at <http://www.indiainfoline.com/sect/itsp/ch05.html>.
places into the personal computers of Internet users within those countries, and they are maintained regularly by those countries.66

III. Filtering objectionable content using destinations’ ISPs: The Pennsylvania Maneuver

The first sustained U.S. effort at content control through destination ISP’s is now under way. The commonwealth of Pennsylvania has, in essence, sought to replicate the Chinese filtering scheme within its borders, while 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.67

The law is careful to state that the destination ISP is not under any obligation to monitor the flow of data through its routers for child pornography,68 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 – misdemeanors for the first two offenses, felonies for subsequent ones.69

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.70 Worldcom refused to block the sites on the basis of those informal notices.71 As a result, pursuant to the statute, the

68 See 18 Pa. C.S. §7330(b) (2002).
69 See 18 Pa. C.S. §7330(c) (2002).
71 Id.
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.\footnote{See September 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, (No. Misc 689, Jul 02).}

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 there violated the OSP’s terms of service.\footnote{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 (September 23, 2002).} Two sites not blocked at the source were then blocked by Worldcom.\footnote{Id.}

Were a Constitutional challenge brought to the Pennsylvania statute, it might well be struck down. Some of its potential infirmities may inform a more general discussion of the Constitutional prospects for other forms of control of destination ISP’s 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.

III.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 implemented for all Worldcom subscribers, regardless of location.\footnote{Id.} 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.\footnote{See American Libraries Association v. Pataki, 969 F.Supp. 160 (S.D.N.Y. 1997).}

The law in question was a New York state sibling to the federal Communications Decency Act, and without reaching the First Amendment questions later resolved against the CDA by the 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.”\footnote{Id. at 184.} 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 the Pennsylvania law seeks to limit its reach only to the activities of ISP’s 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 the Pennsylvania jurisdiction.
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. 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. 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.

III.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. However, the categorization of material as obscene is itself fraught with First Amendment implications. The Pennsylvania law contemplates a judge’s finding that there is “probable cause” that the material to be blocked is child pornography, but the finding is made ex parte, with the most logical real party in interest – the source of the material – not notified that the material is slated for state-mandated interception. Were the government to order 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 – and the newspaper publisher could likely object further on due process grounds were it not alerted to the order and given a chance to object.
Further, a blocking of a given destination under the Pennsylvania law has no particular time limit. This, then, is as if the government banned not only a 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.\(^{85}\)

To be sure, as section II.A. explains, the source of a data transfer on the Net is quite often anonymous, especially in the case of possibly illicit material – making notifications difficult, and perhaps constituting a form of waiver of notification. However, as part of the growing number of cases surrounding “John Doe” subpoenas, source ISP’s and OSP’s being 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, and 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.\(^{86}\)

Those wishing to view the Internet sites slated for blocking no doubt have Constitutional interests of their own to advance.\(^{87}\) Internet users attempting to access sites blocked under the law will not be informed why the sites are unavailable. 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 ISP’s, resulting in blocked sites without explanation to the Internet users attempting to access them, or even formal notifications to ISP’s still not readily made available to the public, is deeply troubling.

Of course, the law could be amended to provide for public notification of sites blocked – so long as the government was prepared to create a public index to illegal material often

in Carroll v. President and Com’rs of Princess Anne, 393 U.S. 175 (1968) the Court stated that “[t]he value of a judicial proceeding . . . is substantially diluted where the process is ex parte, because the Court does not have available the fundamental instrument for judicial judgment: an adversary proceeding in which both parties may participate. … Judgment as to whether the facts justify the use of the drastic power of injunction necessarily turns on subtle and controversial considerations and upon a delicate assessment of the particular situation in light of legal standards which are inescapably imprecise. In the absence of evidence and argument offered by both sides and of their participation in the formulation of value judgments, there is insufficient assurance of the balanced analysis and careful conclusions which are essential in the area of First Amendment adjudication.”

Also, under procedural due process law, namely the Court’s decision in Mathews v. Eldridge, 424 U.S. 319 (1976), 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).

\(^{85}\) This is precisely what was found to be unconstitutional in Near v. Minnesota, 283 U.S. 697 (1931).


\(^{87}\) See, e.g., Virginia State Board of Pharmacy v. Virginia Citizens Consumer Counsel, 425 U.S. 748 (1976) (consumers were found to have First Amendment-protected interests in receiving certain commercial information).
only partially blocked, since there might be ISP’s beyond the state boundaries not subject to the order.

ISP’s themselves could be asked to maintain the public lists, and might be the best custodians for the purposes of conveying to the public when a failure to reach an Internet point of presence might be due to government intervention. If the governments themselves maintained the 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 as to whether an ISP with whom they are not in direct privity still might be affecting their attempts to reach a site – a surmise that would have to in many cases be grounded in knowledge of routing tables and the user’s ISP’s relation to other ISP’s within the Matryoshka doll chain or peers within the cloud. For example, a user of uunet, a Worldcom subsidiary, would have to know that her packets were all 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.

III.C. Objections arising from overblocking

Refusing to carry packets is a crude instrument of Internet discipline. Internet service providers 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. 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 ISP’s 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.

However, characteristics described in section II make blocking on a broad scale difficult for an ISP, and suggest persistent overblocking in many circumstances.

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 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 9 should be passed to the west. Routers behave similarly, and pausing to consider a special rule or exception for a single destination increases the work the

router needs to do. China has appeared to overcome this limit as it embeds thousands of exceptions in what otherwise are likely to be standard (and thus manageable) routing tables serving its Internet users,\textsuperscript{89} suggesting that Worldcom and others could come to do so as well.

Second and more vexing as a technical matter, IP addresses might be reassigned from time to time, or even moment to moment. The Pennsylvania order to Worldcom demanded blocking for distinct “uniform resource locators,” one level of abstraction higher than IP addresses.\textsuperscript{90} Should the site found, say, at \url{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), while permitting packets to pass to and from the illicit site’s URL at its new IP destination. Worldcom adverted to this problem in response to the Pennsylvania 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 addresses. Blocking individual URL’s, rather than IP addresses, is, as with all such technical challenges, 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 addition to its IP filtering, China.\textsuperscript{91}

Retaining blocking at the IP level also means that a site hosting multiple (and unrelated) users’ work, such as \url{http://www.blockedsite.com/sourcexillegalmaterials} and \url{http://www.blockedsite.com/sourceyinnocuousmaterials}, 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. The attorney general’s cover letter 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.\textsuperscript{92} Worldcom did just that,\textsuperscript{93} 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, creating


\textsuperscript{91} See Jonathan Zittrain and Benjamin Edelman, Documentation of Internet Filtering Worldwide, available online at <http://cyber.law.harvard.edu/filtering>.

\textsuperscript{92} Letter from D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania, to Craig Silliman, Attorney, WorldCom Network and Facilities Legal Team (September 17, 2002).

\textsuperscript{93} 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 (September 23, 2002).
the very dynamic that so troubled the Court as it struck down most provisions of the Communications Decency Act.94

There is yet another form of overblocking to consider: even when and if a site containing offending content can be solely targeted, all material to and from the source in question is blocked. Indeed, 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 these lacks of subtlety in blocking are unavoidable, perhaps they could be found permissible. Of more import is a sense of just how much tinkering would have to occur to provide for a nuanced system of content control. Courts, perhaps rightly, might expect such tinkering to take place when it can. For example, the online filesharing service Napster was ordered to undertake changes to its technical architecture so as to block unauthorized copyrighted material from being indexed for its users, while allowing innocuous material to pass,95 a baby-splitting compromise of the sort that the Supreme Court never considered when it ruled on the status of VCRs as instruments of contributory copyright infringement.96 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. If ISP’s are capable of learning to filter more exactly, the ad disasterum arguments that so powerfully bar impulses to ask ISP’s to control or monitor their networks vanish.

IV. Implications of asserting control at the destination ISP

The Pennsylvania approach is plausibly a continuation of a series of laws designed to force destination ISP’s to assist in Internet content control. On October 10, 2002, the New Jersey state assembly took up a bill nearly identical to Pennsylvania’s.97 On October 21, 2002, a Canadian member of parliament reintroduced a proposed Internet Child Pornography Prevention Act, incorporating the Pennsylvania approach with the additional prospect of requiring monitoring for obscene content by destination ISP’s.98

Pornography is not the only content at issue. A German court has held that approximately 80 destination ISP’s in the state of North-Rhine Westphalia can be

---

94 See section II. B., supra.
96 Universal City Studios, Inc. v. Sony Corp. of America, 480 F.Supp. 429 (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.
97 Assembly No. 2863, 210th Leg. (N.J. 2002).
lawfully asked to block customer access there to two U.S.-hosted Web sites determined by the German government to contain banned Nazi propaganda.99

Further, in a short-lived case that would have proved an interesting test of the U.S. Digital Millennium Copyright Act’s provisions on injunctions,100 thirteen record companies filed a lawsuit in August 2002 to force five major U.S. ISP’s, in their role as destination ISP’s and backbone providers within the Internet cloud,101 to block their customers’ Web access to <www.listen4ever.com>, which was alleged to be an unauthorized China-based source of those companies’ copyrighted music.102 The record companies’ complaint echoes many of the limitations described in section II 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;103 the source ISP is itself in China, allegedly selected precisely to place it beyond the reach of U.S. copyright law;104 the source ISP has ignored cease and desist letters;105 Internet users within the U.S. (“destinations” in Figure 1) can all too easily find the site, navigate its English language prompts, and search for and download the music at issue.106 Days later the plaintiffs withdrew their claims, perhaps because the listen4ever site at issue had apparently vanished.107

The provisions under which the record companies sought the injunction appear, for ISP’s serving destinations or carrying data within the cloud per Figure 1, to limit compelled blocking to sites hosted outside the United States.108 In weighing the request, the court is to consider, among other things, the burden such an injunction would place upon the defendant ISP’s, whether less 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.109 Thus the copyright-based mechanisms for enlisting ISP assistance in blocking sources of illicit data have several potential safeguards missing from the Pennsylvania counterpart provisions against child pornography. These elements are fact-based, and the facts are evolving as more and more pressures are placed upon backbone providers and destination ISP’s to discriminate in their carriage of data. As ISP’s evolve their tools to

99 See Germany: The idea of Internet providers blocking illegal content is questionable, SAFER INTERNET, November 2001, Number 8 at 3, available online at <http://www.saferinternet.org/news/safer8.htm>, for a description of the first German court’s decision in this case. More detail is available at <http://www.heise.de/newsticker/data/hod-15.10.01-0001> (in German). The second German court’s reiteration of the blocking order is described at <http://zem.squidly.org/weblog/article/2162>.
101 See Figure 1, supra.
103 Id. at para. 39.
104 Id. at para. 40.
105 Id. at para. 43.
106 Id.
107 Notice of Voluntary Dismissal, Arista Records, Inc. et al. v. AT&T Broadband Corp. et al., No. 02 CV 6554 (KMW) (S.D.N.Y. Aug. 21, 2002).
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 most nettlesome to the complainants and specifically provided for in the act – is far greater than likely intervention at other points in the chain.

In tandem with refinements to blocking technology, adjustments to the legal principles for mandated blocking by destination ISP’s and backbone providers can make such interventions less Constitutionally suspect. For example, the law might provide for procedures to attempt notice to and an opportunity to object by the real party in interest, i.e. the source of the alleged illicit material. It 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. And it might 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 getting to 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 described in section III, and technical adjustments are made to minimize the technical burden to ISP’s asked to block particular sources of data from their customers, what problems remain?

IV.A. Overblocking

Filtering on the basis of IP address remains a crude metric along several dimensions. First, when a given IP address corresponds to a computer hosting content from several distinct and unrelated 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 – 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 ISP’s (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 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, here China leads: it appears, beginning in the fall of 2002, to have its destination ISP’s actually searching data packets for particular sensitive keywords; when such keywords are found, access by the user in China to the source of data in question is then cut off for a designated period of time. 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. ¹¹⁰

IV.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.¹¹¹ They observe that complexity is the bane of scalability, and for those 
reasons and others recommend that even such routine features as error checking are 
best implemented apart from basic Internet Protocol routing. Recently 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.¹¹² 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, and 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 
oblocking, 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 addressed as they arise 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 – one might beware a spiral of patches, tweaks, and overlays that cumulatively severely impair the Internet as it exists now. When “tussles” between network parties are fought out through the network protocols themselves, the efficient functioning of the network is threatened.\footnote{David D. Clark, Karen R. Sollins, John Wroclawski & Robert Braden, \textit{Tussle in Cyberspace: Defining Tomorrow's Internet}, SIGCOMM '02, August 19-23, 2002. Available online at \url{<http://www.acm.org/sigcomm/sigcomm2002/papers/tussle.pdf>}.}

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 themselves 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 level or in a more refined way. Such 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.\footnote{Lawrence Lessig, \textit{Tyranny in the Infrastructure}, WIRED (July 1997), available online at \url{<http://www.wired.com/wired/5.07/cyber_rights_pr.html>}.} To change 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 called for. At the very least, one might wish to take into account end-to-end violation and portability effects in weighing the costs and benefits of mandated filtering for an ostensibly narrow purpose, and conclude that the solution is overall disproportionately burdensome in relation to the acknowledged problems.

IV.C. Proposing a network user’s bargain

The Internet’s threat arises from its distributed 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 criminal – true for certain categories of 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.

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, of 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 points of presence simply disappear with respect to others – at first for some rather than all – portends enormous but subtle control over who can say what on 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.