Network neutrality is the new common carriage

Christian Sandvig

Christian Sandvig is an Assistant Professor of Speech Communication at the University of Illinois at Urbana-Champaign, Illinois, IL and an Associate Fellow of Socio-Legal Studies at Oxford University, UK.

Abstract

Purpose – *This article considers internet system development with reference to what is currently termed the ''network neutrality'' debate; its aim is to develop improved ways of reasoning about the role of the public interest in networked communications infrastructures.*

Design/methodology/approach – *To assess the degree to which a general non-discrimination rule would be possible or useful, this article this article reviews documented examples of differential service by internet service providers that already occur. It then compares these practices to older debates about common carriage.*

Findings – *Most of the debate about network neutrality focuses on a few kinds of content discrimination, while there are many more varieties at work. While the focus of the debate has been legal, the problem is often technological. Many kinds of discrimination are now at work, often secretly.*

Practical implications – *Rather than one grand, neutral rule for a neutral internet, there is a need for a normative framework that can provide a larger picture of the role of this infrastructure in society, and therefore a way to reason about whether a particular kind of discrimination is normatively good or bad. There is also a need for more public disclosure of actions taken internally by internet providers.*

Originality/value – *This paper provides a set of examples that expand the scope of the network neutrality debate, adding nuance and complexity. It also calls into question the novelty of the issue and suggests that it is unlikely that a single rule (or a small set of general rules) will resolve this dispute.*

Keywords *Telecommunications, Public interest, Networking, Discrimination*

Paper type *General review*

Paper presented at ''Making public-service telecommunications: past and present challenges to networked information infrastructures'', Center for Advanced Study, University of Illinois at Urbana-Champaign, 14-15 April 2006. The author would like to thank Matthew Allen, Dan Schiller, and the participants in the Public Service Telecommunications Conference for their comments on an earlier version of this manuscript. This material is based on work supported by the National Science Foundation under Grant No. 0308269. A portion of this research was kindly supported by a fellowship from the Center for Advanced Study of the University of Illinois at Urbana-Champaign.

Some internet users are worried. For many of them, the internet symbolizes a previously unprecedented capability for communication. Even better, communication services and content on the internet are often free. All kinds of things can be found, seen, heard, and played at any time. This seems to be a self-evident advance from the old media and telecommunications worlds of scheduled, limited offerings coupled with – even worse! – paying, pricing, per-minute charges, pay-per-view, and premium subscription channels. By early 2006, the perception had grown that this free and bountiful internet was threatened by powerful telephone and cable companies, and that this may or may not have something to do with metaphors about railroads and roads. In a *New York Times* editorial on 20 February titled, ''Tollbooths on the internet highway'', the authors framed the issue as internet providers potentially favoring ''giants'' against the ''little guy''. The editorial exhorted the reader that ''Americans feel strongly about an open and free internet. [This] is an issue where the public interest can and should trump the special interests.''

This article considers internet system development policy with reference to what is currently termed the ''network neutrality'' debate; its aim is to develop improved ways of reasoning about the role of the public interest in networked communications infrastructures. Critically explicating the concept of network neutrality as received, I try to develop a more valid assessment of the significance of tollbooths and discriminatory practices on the internet.

This article finds that on the discriminatory, biased, tollbooth-ridden internet that already exists in 2006, the issue is not neutrality. Instead, it is who discriminates for what purpose, and whether this discrimination is hidden or visible. To reason meaningfully about the present and future of the internet, we need not neutrality, but a normative vision of what public duties the internet is meant to serve.

The looming pay-per-view internet

The fears expressed by internet users that the internet could become like a pay-per-view cable system developed over several years. In the scholarly literature, the most influential early analysis of the issue came in 2000 (Bar *et al.*, 2000). To take one memorable example from this study, Bar *et al.* found that in the 1998 annual report of cable television provider AT&T/@Home, the corporation outlined a strategy to leverage its monopoly control of local cable television franchises into control over internet content. AT&T/@Home had forged exclusive partnerships with internet content providers in a number of non-competing content areas. In exchange for these secret revenue-sharing arrangements, AT&T/@Home provided faster access to these preferred internet services, a practice it referred to in 1999 using a verb from television: it was ''programming the internet'' (Bar *et al.*, p. 512)[1].

From the perspective of the user, this is a chilling idea. An AT&T/@Home cable modem subscriber could try internet gaming using a Sega Dreamcast and a competing platform. The Sega Dreamcast internet gaming experience would be more responsive, but the user would never know that the reason for this was not the product's general superiority, but a private agreement between SegaSoft and their monopoly cable provider. This foreshadowed a rocky and uneven internet landscape, where different web sites and internet services might be available on very different terms, foreshadowed by earlier research as ''islands of high interoperability'' accessible only to some users, for some purposes (Bar *et al.*, 1995, p. 44).

On this kind of internet, the logic explaining which addresses would be easy to reach and which would be difficult could never be uncovered by the user, as internet ''programming'' would be governed by secret agreements. Even worse, given the limited availability of broadband access and the high cost of switching between different kinds of service providers[2], even if the user found out, she might have no other option for obtaining broadband internet access. This example was a contribution to a policy debate termed ''open access'', a movement to require cable television franchisees to allow other internet Service Providers to use their facilities (for a review, see Farrell and Weiser, 2003).

The tendencies toward an uneven internet are not limited to this example, or to local cable monopolies. While @Home is now bankrupt, what little evidence is available suggests that agreements like @Home's pact with SegaSoft are common, even among carriers that do not have a monopoly. In Australia as of this writing, Telstra's BigPond has the largest share of the internet service provision market and it has entered into a number of content agreements, most notably with the Australian Football League (Hearn, 2006). Some internet content is exclusive to BigPond, and when BigPond users visit internet content covered by a BigPond agreement it does not count against their monthly download limit (Flynn, 2006).

In short, all internet providers try to legally and technically control their user's traffic in some way, if only to prohibit illegal content. Although the object and means of discrimination varies, discrimination is pervasive. Providers limit the use of encrypted virtual private networks (VPNs) commonly used by businesses, the operation of servers to provide information, and high-bandwidth applications like videoconferencing and peer-to-peer file sharing. Providers prohibit resale or sharing with third parties, e.g. via open Wi-Fi wireless internet connections. (For a complete survey of prohibitions in Terms of Service agreements, see Braman and Roberts, 2003.) The motives for these interventions are varied. Some are clearly intended to save the provider money by conserving capacity or to make the provider money by enabling price discrimination, and these efforts may be insensitive to the actual content involved. But other attempts to control traffic are explicitly related to content censorship.

To cite a few more examples that have received wide attention, governments such as China and Cuba block dissident and religious material (e.g. see Zittrain and Edelman, 2003; Kalathil and Boas, 2003). Public schools in the USA are compelled by law to block sexually explicit material (Hunter, 2000). Many service providers try to detect e-mail about topics likely to be unsolicited and differentiate or block it (Beke, 1998). Canadian internet provider Telus blocked subscriber access to its employee union web site during a labor dispute (OpenNet Initiative, 2005).

In order to remedy the situation of service providers censoring and manipulating internet use to suit private, capricious, or sinister ends, Wu (2003) proposed a short list of ''network neutrality'' rules that would prohibit carriers from discriminating between user traffic on certain grounds. Specifically, Wu posited that capacity-based discrimination should be allowed, while content-based discrimination should be disallowed. Your service provider could cap the amount of traffic that you send, but not tell you to send one kind of traffic instead of another. This ''network neutrality'' differs from earlier ''open access'' proposals because open access rules would have tried to address the same discrimination problems via modifying the conditions applied only to local cable monopolies. Wu (2003) terms this a structural solution, and he instead advocates for a more general rule to apply across all broadband carriers (2003) or even all telecommunication systems (Wu, 2005).

Such a rule seemed even more necessary after two significant events in 2005. First, the US Supreme Court ruled in the case of *FCC* v. *Brand X*, where a San Diego internet provider (Brand X) was petitioning for open access to a cable television network. The Supreme Court ruled against open access, foreclosing the chance for open access rules to redress internet discrimination in the near term (see Aronowitz, 2005). In addition, a DSL provider, Madison River Communications, was fined $15,000 by the FCC enforcement bureau for blocking their customers from using the voice-over-internet-protocol (VoIP) service Vonage[3]. This action rested on grounds of consumer protection, and was later cemented by a policy statement indicating the FCC's willingness to intervene in such matters in the future (for a review, see Dinkes, 2005, pp. 862-864)[4].

Most analyses have expressed distaste at this case-by-case, ex post approach. All authors agree that there are some legitimate reasons to discriminate in order to protect the network. How can the FCC be trusted to know when an action by an internet provider is a ''good'' intervention or a ''bad'' one? In this context, network neutrality has been posed as the quest for a general rule, or the failure to find one (e.g. Yoo, 2004, pp. 66-67).

The widespread interest in such a rule has led to the recent introduction of a bill by Sen. Wyden, the *New York Times* editorial that introduced this paper, and other popular media attention (see also Surowiecki, 2006). A number of high-level panels and national symposia are grappling with the issue, new bumper stickers are now circulating[5], there is a national ''Freedom to connect'' conference, and a wide range of institutions are weighing in (e.g. the USC Annenberg Center, 2006).

In their case for neutrality, Wu and others have usefully traced some of the long legal history of non-discrimination rules, comparing internet discrimination to price discrimination and racial discrimination. In telecommunications specifically, Wu has compared discrimination between internet applications such as bans on the attachment of servers to a broadband connection to earlier regulation about customer premises equipment attached to the public switched telephone network (recalling FCC's 1968 Carterfone decision). It may be that useful comparisons go back even farther, and this will eventually bring us back to the railroad. First, let us pause and consider the current state of neutrality and discrimination on the internet.

The misplaced focus of the network neutrality debate

Network neutrality proponents like Wu (2003) discuss the uneven or ''tiered'' internet as something that comes to exist by almost purely legal means. In this narrative, internet providers use Terms of Service agreements and Acceptable Use Policies (AUP) to prohibit content that they do not like. In 2003, Wu predicts technological interventions in traffic discrimination as largely in the future. However, recall the Bar *et al.* example from 1998 –

while this discussion of open access did deal with AUP restrictions, AT&T/@Home was also technologically controlling traffic by speeding some over others in a way that would be undetectable if pride had not forced it into the annual report to shareholders. This was not a contract with the subscriber or a legal rule, it was a quiet manipulation of network resources.

In the literature and the press, the popular network neutrality debate has focused on the restrictive provisions inserted into subscriber agreements by large carriers. Empirical work has cataloged and compared the restrictions imposed by different providers, but this emphasis is misplaced. Many of these provisions have no legal force and are simply outrageous, presented legalistically as a scare tactic rather than an enforceable contract. For instance, the Verizon Online terms of service agreement forces the subscriber to agree to not use the service to criticize Verizon[6]. While there have been efforts (such as the US Uniform Computer Information Transactions Act) that would legitimate some of these agreements, they are not legitimate now. It is strange, then, that the debate has centered on counting these legal feints. While they may be ugly, the ugliest are likely to be unenforced or unenforceable. This stands in contrast to the longer literature on internet censorship, which has gone to great pains to empirically measure damage, rather than rely on legal or policy statements by potential censors (see Zittrain and Edelman, 2003).

Technological manipulation of traffic – as opposed to legal – is not in the future and is not speculative. A wide variety of software packages and tools now exist to assist internet providers in inspecting the content of internet traffic and controlling it, including Packeteer, L7-filter, Packet Details Markup Language (PDML), netscreen-IDP, and NetScout. These are not prospective or experimental – some are robust software packages that are in wide use. If the readers of this article use the internet, it is likely that their internet traffic is passing through these systems now. The chief use of this software is to discriminate among internet traffic: what the network neutrality debate purports to be about. Let us briefly review the major technological means by which service providers currently discriminate and manipulate internet traffic. In many discussions, four distinct means are identified: address blocking, port or protocol blocking, content filtering, and prioritization.

Address blocking

Speaking metaphorically, this means of interference is no different from address blocking in a postal system: mail sent to or from subversives and undesirables is not delivered. This method of censoring internet traffic has received the most attention, but it is also very crude and obvious. Still, when people talk about internet freedom, the clearest and most convincing example of a danger has been that a user wants to go to a particular web site, but is prevented from doing so. Systems certainly exist that are actively censoring content in this way. They are a major barrier to the free flow of information on the internet in a number of contexts: most notably computers in authoritarian countries and in US schools and libraries (which are required to use them). This technique has been characterized by using evocative phrases like ''The Great Firewall of China.'' However, blocking by address or domain name requires the complicated and error-prone maintenance of blacklists, and can be circumvented by changing addresses or by disguising the traffic's destination by re-routing it through a third party. The propaganda arm of the US Voice of America (the International Broadcasting Bureau) recently funded the development of software called the Peacefire Circumventor that is able to evade censorship by the Great Firewall of China. (It is also reportedly popular in US schools and libraries[7]) Because this form of discrimination has been extensively written about elsewhere, the remainder of this paper will focus instead on traffic manipulations that are less obvious.

Protocol or port blocking

While this technique might seem technically complex, metaphorically it is nothing more than controlling mail in the postal service based on its packaging. Many postal customers immediately discard direct mail advertising because of its package, but of course mailers with an interest in avoiding this filter have devised ways to alter their packaging.

This technique was at issue in *FCC* v. *Madison River*. It identifies internet applications by using a system of convenient numbers that the internet's protocols use to deliver data to the correct applications on a computer connected to the network. In order to ensure that your request for a web page is delivered to your web browser and not to your e-mail client or printer driver, different kinds of traffic have historically been assigned different numbers, called ''ports.'' Port 25 or 143 for e-mail, port 80 for worldwide web pages, formerly 1214 for Napster, and so forth. Madison River scanned internet traffic and dropped traffic with the port number used by voice-over-internet-protocol (VoIP) provider Vonage. While this seems straightforward, this technique is also relatively crude because these port numbers need not be a reliable indication of the application that is actually using that port. If you are sending a bomb or a thick pile of cash through the mail, you have an interest in ensuring that your packaging does not let everyone know what is inside. Because some internet viruses are associated with specific port numbers, port blocking is very widespread among service providers. It used to be a technique employed to block peer-to-peer file sharing services, but these services have simply become more sophisticated in their use of port numbers, instituting quasi-random port number hopping. As with address blocking, one reason that port or protocol blocking is an brutish solution is that the affected parties know that they have been censored and can take action to remedy the situation (e.g. in Vonage's case, by petitioning the FCC).

Filtering based on content

Rather than examining the information about the content, a more invasive technique is to monitor the content itself, reconstructing packet streams and opening them like a zealous postmaster might have opened letters in the nineteenth century. Some stand-alone web filtering software packages use this technique. These can incur a performance overhead and can be defeated by encryption by the user. If filtering is meant to work without human intervention, a computer must be able to accurately recognize the content and characterize it as forbidden, which can be a serious problem for the would-be censor. For instance, the popular peer-to-peer file sharing software Azureus now contains a feature called ''traffic obfuscation'' that uses strong cryptography to make it more difficult to recognize its own traffic.

Prioritization and shaping

Far more important and less often considered are circumstances that are often termed ''traffic shaping'' or ''conditioning''. Complaints about possible internet ''tiering'' are complaints about prioritization. In this scenario, port numbers, addresses (see above), or other means (such as pattern recognition of an application's data signature) are used to separate some traffic from others for different treatment. It is this form of discrimination that has not been thoroughly examined, and it is in some ways the most problematic. In traffic shaping, it is not clear that anyone would know they had been discriminated against if the discrimination was simply a change in throughput. It is this kind of discrimination that was practiced by AT&T/@Home in the late 1990s, via co-location. Traffic shaping today is widespread, and has many positive uses. For instance, because voice traffic is sensitive to the delays that are often present on internet protocol networks (termed latency), network engineers currently often try to segregate voice traffic on IP networks to insure service quality for campus and corporate VoIP phone service.

Application bias via internet redlining

There are many examples in communication history of governments finding ingenious ways to censor communication without needing to delve into its content. In Singapore, subversive television programs were controlled by restricting the use of satellite dishes to financial institutions. This is a form of censorship that uses class or occupation to stand in for tedious identification of programs that are perceived harmful. Other countries have pursued this strategy by providing uncensored internet only in tourist hotels – a form of blocking by address. This line of thinking is alive and well on the internet in a more subtle way, employing the fourth form of traffic manipulation: prioritization and shaping.

A hallmark of many network neutrality proposals has been the endorsement of ''application neutrality'' – rules that do not discriminate against a particular use or software program (application). Considering one case in detail will demonstrate that the notion of application neutrality is false and disintegrates when examined too carefully.

Wu's application-neutral rules proposed in 2003 would allow service providers to discriminate against traffic if it was required to ''prevent broadband users from interfering with other broadband or internet users' use of their internet connections'' (Wu, 2003, p. 170). One example of acceptable censorship that is posed is ''neutral limits on bandwidth usage'' (Wu, 2003, p. 170). This seems fair: asking those who use more to pay more, or limiting the amount of capacity provided (called ''capping'') to the size of your budget seem to have nothing to do with censorship or discriminating between one use and another. However, given that internet applications are wildly disparate in bandwidth and latency requirements, how would neutral limits on bandwidth usage really function? Luckily, the answer is known because these caps are widely used to manage traffic and backhaul expense.

While internet traffic discrimination often evokes the Government of Cuba, the villain in the next vignette – if there is one – is the University of California, Berkeley. In 2002, as peer-to-peer networking continued to gain in popularity among college students, Berkeley began to exceed the maximum amount of network bandwidth that it had budgeted (Network Advisory Committee, 2002). As Berkeley's internet connection became saturated and performance degraded, network engineers urgently needed to address the problem. First, they asked the Vice Chancellor for $50,000 to buy more bandwidth, then they began to look into traffic shaping that would be entirely consistent with Wu's (2003) application-neutral proposals. As described by a review on the internet 2 peer-to-peer working group's web site, Berkeley divided the campus into two regions: residence halls and ''ROC'' (rest of campus)[8]. By separating this traffic they were able to set different caps for each. The strategy review (probably jokingly) referred to residence halls as the ''bad neighborhoods'' of the network. It is clear that the growth in peer-to-peer traffic was the problem that needed to be stopped. In some implementations of a bandwidth cap, if traffic were not prioritized, application-neutral bandwidth limits could be far worse than a specific attempt to ban p2p. As the residence halls reach their limit, all internet traffic suffers. The traffic shaping in this case is an attempt to stop one application, but it is consistent with application-neutral rules because the criterion is ostensibly geography (residence halls vs ''ROC''). In a word, this is redlining. This example was easy to unearth because universities routinely publicize their internal reports. Private carriers are certainly also likely to be restricting traffic based on geography, but there is no public scrutiny of the mechanisms employed, which are also technical and arcane.

It is reasonable to want more public scrutiny of these processes from a variety of ideological and theoretical perspectives, and there is precedent: public utility regulation has routinely allowed the investigation of the internal mechanisms that utilities use to provide service. The lack of transparency about an ISP's internal traffic routing, shaping, and differentiation is a problem for deregulatory economists as much as for consumer advocates: the idea that competition will solve all problems obviously presupposes that if an alternative carrier does exist, consumers will be able to understand the benefits of switching. With almost all discrimination done in secret, users will never understand why their traffic is degraded. Specific calls for more transparency in the area of ISP peering and routing predate the network neutrality debate (see Cave and Mason, 2001).

Beyond traffic shaping, once you begin looking, it is even easier than this to find decisions made throughout an internet provider's network that obviously have a large effect on use and can be changed in order to manipulate or censor use, although from some perspectives they may appear to be ''application neutral''. For example, some users get a permanent (static) internet protocol (IP) address from their ISP and some do not. It is much easier to provide some kinds of information with a static IP address (such as your own web server). While rules against operating your own web server have come up regularly in the network neutrality debate, the conditions on the network that make running a web server difficult have not been addressed. Another example in this vein is the asymmetry of broadband connections via

DSL, which are designed to privilege downloading. It could be said that this is not ''application-specific'' because these design decisions may not map on to a particular software package or implementation (like Vonage), but this simply begs the question of what is defined as an application. Producing information rather than receiving it is an important function of these systems, and with a normative framework for communication, it is clearer that freedom to produce is a requirement for the network to serve the needs of a participatory democracy.

Manipulating the centripetal versus the centrifugal forces of the internet

If geographic redlining is a way to meet application-neutral rules but censor applications, a reverse sort of problem was found in a recent multi-year study of 62 private, municipal, and amateur groups attempting to become internet service providers (conducted by the author). These fledgling internet entrepreneurs were champions of network neutrality, yet they hoped to break application-neutral rules for a good cause. The same behavior by an established provider, however, would for them remain cause for alarm.

In interviews, participant observation, and archival research with these groups, ample empirical evidence suggested that network neutrality rules were very much desired. In fact, the entrepreneurial impulse which led small, formerly uninvolved groups of people to enter the internet service provider market was almost always motivated by dissatisfaction with the current offerings (or lack of offerings) from larger providers (see Sandvig, 2003). People who want to provide their own internet service do so because of the constraints on applications, symmetric bandwidth, and geographic reach of existing networks. Any rule that forced large providers to treat customers equally (as many network neutrality rules do) would be hailed by almost all of these providers as a victory and a step forward. Yet, in their own behaviors while organizing internet provision, they regularly hoped to institute traffic discrimination that would break at least some of these same rules. For example, while a proto-ISP might be upset that the local carrier does not allow them to host their own web server (typically via port monitoring), if they go to the trouble of building their own internet service, they often dream of installing hardware and protocol modifications that favor the same services that they were previously denied – even though this would presumably be at the expense of equality, and of other services. Their goals seem noble: community-based grassroots organizations typically wish to favor locally-originated internet content, for example – the same hopes proffered by the earlier ''Community Networking'' movement of a decade earlier (Schuler, 1996). Additionally, some hope to encourage (rather than discourage) peer-to-peer applications. Yet, this contradicts some of the same rules for network neutrality that they favor and leaves the value of application neutrality (at least) in doubt.

Compared to the rhetoric surrounding ''big cable'' censorship in the network neutrality debates, these proposed small interventions by entrepreneurial, municipal and community wireless projects seem minor, but they are worth highlighting because in some sense their existence reinforces the notion that there can be ''good'' discrimination and ''bad'' discrimination (an old idea). As mentioned above, one of the chief kinds of discrimination that local broadband groups are interested in involves modifications to routing to ensure that locally-originated traffic receives priority. At the minimum, many providers make it a design goal for their network to reduce latency for local users to access local content – typically this can be accomplished by providing a network path that does not require local traffic to be routed and interconnected at data centers operated by large carriers in distant metropolitan areas. In the current network neutrality debate this sort of example would probably not be recognized as relevant: it could be classified as the normal operation of network engineering. Yet, an argument might be made that this form of content discrimination is not simply an attempt to improve a network's efficiency. Without agreeing with this logic, one can point out that in the early days of the internet, one of the exciting promises of the network was the ''death of distance''. By this view, the fact that a local user could access an international source of information as easily as the local newspaper was a feature, not a problem of inefficient routing[9]. By bringing this sort of traffic discrimination into the frame, it is clearer that all kinds of programs are underway to speed or to slow different sorts of information on the internet without any public scrutiny or even the concept that public scrutiny might be

desirable. This again highlights the value of transparency in network operations, so that these campaigns can at least be detected and discussed.

Network neutrality is the new common carriage

Howard Waltzman, telecommunications counsel to the US congressional committee that planned to revise the Telecommunications Act, was quoted in 2006 complaining that ''network neutrality'' proposals for the internet would turn ''broadband pipes into railroads''. This is a surprisingly common complaint about internet law and policy – authors of all backgrounds like to justify proposals about the internet's specificity by brandishing examples from communication infrastructures whose glory days have passed. ''Today's computer-based, all-digital networks'', some have argued, ''are as far from a railroad-like architecture as smoke signals are from satellite communications'' (Neuman *et al.*, 1997, p. 65).

The periods at the end of these quoted sentences are almost exclamation marks. While the strident claims of ''different!'' will continue to be useful for authors advancing new policy proposals, the debates surrounding the most advanced digital communication systems would benefit from a few claims of ''same!'' From the perspective of public policy, it is the most useful approach to compare but not especially contrast the internet with historical infrastructures like the railroad. Dazzled by technological jargon and new capabilities, debates about advanced communication systems tend to proceed as though all of the modern policy problems encountered are new. Though the internet may be new, these public issues are not.

One place to observe evidence for this statement is in the late MIT political scientist Ithiel de Sola Pool's 300-page analysis proposing that non-discrimination rules should apply to new communication technologies. This award-winning book, *Technologies of Freedom* (1983), is 23 years old at this writing and out of print. In it, de Sola Pool forcefully and in great detail explained that principles similar to network neutrality should apply to television and derivative electronic media in the USA – an idea that has not been adopted. Remarkably, most of his conclusions are identical to many of the principles now advocated under the banner of network neutrality. In his ''policies for freedom'' (de Sola Pool, 1983, pp. 246–249), de Sola Pool argued that:

1. all media conduits should be treated equally;
2. rules should be blind as to the use or content of the communication;
3. monopoly conduit franchises should not be allowed to leverage their power into control of content;
4. true non-discrimination implies enforcing interconnection guarantees;
5. non-discrimination enforcement depends on carriers disclosing information about their operations;
6. enforcement must be *ex poste* to be successful;
7. regulation should impose as light a burden as possible;
8. intellectual property protections like copyright must be reworked in order to make them less restrictive in electronic media.

de Sola Pool's analysis of 23 years ago captures word-for-word many of the points made in the network neutrality debates today. They match material from public policy documents like the USC Annenberg statement almost word-for-word. The material from the 2000s is more likely to be framed as ''innovation policy'' than competition policy and the newer proposals emphasize competition among application providers or third-parties, while de Sola Pool more simply wrote about easing new entry for small carriers and the use of ''novel technologies.'' The fact that de Sola Pool was able to reproduce these conclusions while analyzing what were arguably different technologies in a different context is worth a comment.

de Sola Pool sought to advance a neo-liberal agenda of increased competition by warning against the menace of government intervention. In this, his agenda appears consistent with network neutrality critics like Yoo. However, the policy proposals he suggests are identical to those advanced by network neutrality advocates like Wu. One reason for this is that the regulatory context is so different now that de Sola Pool's proposals sounded like ''hands off!'' 23 years ago, and yet these same proposals are now the tools of interventionists, and sound like ''hands on!'' A second explanation is that the idea of a short list of rules to manage the long list of bargains, negotiations, tiers, filters, censors, and traffic shapers was misguided both then and today. Absent an elaborated normative justification, a rule like #5 that suggests carriers must ''disclose information about their operations'' is not specific enough to do any good.

de Sola Pool took pains to strongly frame his arguments in terms of the requirements for a free and democratic society. His first principle, omitted in this review until now, is that the First Amendment applies to all technologies, and that ideally anyone must be able to publish or speak at will. As de Sola Pool's concern was the licensing of television broadcasters, his worries about the infringement of civil liberties by censorship in new media technologies were framed largely in terms of government censorship and the First Amendment[10].

de Sola Pool drives the comparisons and justifications for non-discrimination far back beyond Carterfone into the distant past. He reviews railroad regulation, remarks on canals and roads, and extensively considers cable television, postal services, and broadcasting. The phrase that includes nondiscrimination rules in these contexts is ''common carriage''. Common carriage is a common law legal concept that may date to the Roman empire (for a review, see Noam, 1994). In brief, a common carrier is a private party offering transport or communication services who is subject to special public duties in return for legal benefits. The chief obligation of the common carrier is nondiscrimination – it must undertake to carry all people indiscriminately[11]. (This is of course the center of the network neutrality debate.) Common carriers include railroads, taxis, airplanes, and telephones.

In exchange for this burden of non-discrimination, common carriers have received a number of benefits: chiefly, liability protection. As common carriers can have no interest in the content that they carry, they are not liable for transporting stolen property – you cannot sue the phone company for copyright infringement if a telephone is used to read aloud a copyrighted work. Carriers may also not be liable for any other illegal content: offensive messages, indecent messages, or death threats. In addition, common carriers are allowed to use public rights of way to provide their services and may receive other benefits[12].

The parallel between common carrier regulation and the network neutrality is a fairly obvious one. ''One might think of the notion of [network] neutrality as the 21st Century version of common carriage,'' said Vint Cerf (Cook, 2006, p. 92), the computer scientist commonly referred to as ''father of the internet'', now Vice President at Google. However, he went on, ''I hesitate to draw the comparison if only because of the complex way in which [the] 'common carriage' concept and rules have evolved.'' (Cook, 2006, p. 92). The complexity alluded to here may be what regulatory insiders refer to as ''the baggage of title II'' – referring to title II of the Communications Act of 1934. de Sola Pool also admitted the practical difficulties with the formal, absolute non-discrimination rule that is equated with common carriage and network equality in much discussion. While he calls for non-discrimination in a dramatic fashion at the end of the book, earlier he admits that the US has never applied an absolute non-discrimination rule, and it is unlikely to. He notes that the political will and economic rationale for non-discrimination rules derive from the limited options in a monopoly or concentrated communication system, but that the US has in fact often imposed ''very restrictive policies'' opposite to the freedom of speech (Cook, 2006, p. 82) even under conditions of monopoly or oligopoly, when the lack of any alternative system would presumably make ''network freedom'' that much more important. There are a number of conclusions to be drawn from these comparisons: one of import is that network neutrality is an old problem that has often been addressed in ways particular to the historical, political, and technological context of the time.

Conclusion: a map for the uneven terrain of the biased internet?

The points made in this essay so far can be recapped briefly. The internet is not neutral now. Most of the debate about the internet focuses on a few kinds of content discrimination, while there are many more varieties at work. While the focus of the network neutrality debate has been legal, the problem of content discrimination is often technological. Many forms of discrimination are already at work – often secretly – and it is not at all clear that all of these forms of discrimination are a bad idea. Today's network neutrality debates seem new, but they echo common carriage debates that are a century old. Examining writing proposing non-discrimination rules from the history of common carriage shows that these rules were not absolute.

The effort spent in this essay so far has brought us here only for the purpose of pointing out that when a polity considers enacting law about what content can be favored over others, it is essential to have some normative concept of what communication is supposed to do. This concept is absent in the current debates, which are framed in terms of protecting a non-existent neutral internet and in terms of enhancing competition.

Even the most recent congressional testimony about network neutrality rules given by proponents is written as though the internet were neutral, and congress should act to ''preserve'' the ''level playing field''. Of course these arguments are framed strategically, and new regulation is unpalatable in a deregulatory climate. Still, how long is it useful to continue to believe the fiction that the internet is neutral now? Any call for ''legislation that protects the environment for internet innovation and competition that the original internet produced'' (Lessig *et al.*, 2006, p. 11) holds up a fictional internet. As a few of the earlier examples given here have shown, content discrimination is widespread in the internet, and it is too widespread to go away. Rather than frame the problem as one of writing a neutral competition rule for a neutral internet, the more useful approach would be to grant the varied terrain to today's uneven network and instead work to craft a normative justification for communication systems that serve the public. This would provide the judge, regulator, and critic alike an analytical tool that can be used to determine which acts of discrimination are good and which are not. In short, the present uneven terrain of the discriminatory internet invites us to revisit our principles, and history suggests that we will not be able to serve our principles well with a simple rule.

Notes

1. ''Secret'', in that their existence is disclosed to shareholders and not consumers, and the exact terms of the agreements are disclosed to no one.
2. Such as switching between cable modem service and DSL. Bar *et al.* estimated switching costs could be over $500 in 2000 (p. 503).
3. See also the Madison River Consent Decree, File No. EB-05-IH-0110, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A1.pdf
4. Also see FCC policy statement 05-151A1 http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A1.pdf
5. ''Fat pipe, always on. Get out of the way! – Tim Bray''
6. This example was pointed out on the mailing list CYBERTELECOM-L: ''You may NOT use the Service as follows:... (j) to damage the name or reputation of Verizon.'' www.verizon.net/policies/vzcom/tos_popup.asp
7. see www.peacefire.org/
8. See the anonymous document, ''Campus Bandwidth Management'' at http://p2p.internet2.edu/documents/CBM-Matrix.pdf
9. Some might see this example as frivolous because it is so ''obviously'' (or ''objectively'') true that reducing the number of links required for transport between two nodes on a network is a good idea, and efficient. But this example is offered here exactly in order to highlight that cases of ''good'' discrimination between traffic are based on judgments about what the network ought to do, and relate to what criteria (efficiency, or what kind of efficiency) are legitimate.

10. However, as his inquiry was grounded in the free exchange of information as a societal goal, his arguments remain relevant in the context of private censorship by carriers like internet providers.

11. Other duties have been imposed on common carriers at different times. For example, monopoly common carriers have had higher standards of service imposed on them.

12. For instance, common carriers may be granted powers of eminent domain.

References

Aronowitz, S. (2005), ''*Brand X internet Services* v. *FCC*: the case of the missing policy argument'', *Berkeley Technology Law Journal*, Vol. 20 No. 1, pp. 887-905.

Bar, F., Borrus, M. and Steinberg, R. (1995), ''Islands in the bit-stream: mapping the NII interoperability debate'', Berkeley Roundtable on the International Economy Working Paper # 79, BRIE, Berkeley, CA. available at: www-rcf.usc.edu/ ~ fbar/Publications/islands-in-the-bitstream.pdf

Bar, F., Cohen, S., Cowhey, P., DeLong, B., Kleeman, M. and Zysman, J. (2000), ''Access and innovation policy for the third-generation internet'', *Telecommunications Policy*, Vol. 24 Nos 6/7, pp. 489-518.

Beke, T. (1998), ''Fending off automated mass electronic mail: or, how to distinguish yourself from a computer'', *First Monday*, Vol. 3 No. 2, available at: www.firstmonday.org/issues/issue3_2/beke/

Braman, S. and Roberts, S. (2003), ''Advantage ISP: terms of service as media law'', *New Media & Society*, Vol. 5 No. 3, pp. 422-48.

Cave, M. and Mason, R. (2001), ''The economics of the internet: infrastructure and regulation'', *Oxford Review of Economic Policy*, Vol. 17 No. 2, pp. 188-201.

Cook, G. (Ed.) (2006), ''Symposium discussion, Part II: uses for devices of multiple capabilities cannot always be predicted or channeled'', *The Cook Report on internet Protocol*, Vol. 14 Nos 10/11, pp. 71-117.

de Sola Pool, I. (1983), *Technologies of Freedom*, Harvard University Press, Boston, MA.

Dinkes, J.S. (2005), ''Rethinking the revolution: competitive telephony in a voice over internet protocol era'', *Ohio State Law Journal*, Vol. 66 No. 4, pp. 833-73.

Farrell, J. and Weiser, P.J. (2003), ''Modularity, vertical integration, and open access policies: towards a convergence of antitrust and regulation in the internet age'', *Harvard Journal of Law & Technology*, Vol. 17 No. 1, pp. 83-134, available at: http://jolt.law.harvard.edu/articles/pdf/v17/17HarvJLTech085.pdf

Flynn, D. (2006), ''Hit the fast lane'', *The Age, Tech: Connectivity*, available at: www.theage.com.au/news/wireless–broadband/hit-the-fast-lane/2006/06/28/1151174266136.html (accessed 1 July).

Hearn, L. (2006), ''BigPond chasing AFL web rights'', *The Sydney Morning Herald BizTech*, available at: www.smh.com.au/news/biztech/bigpond-chasing-afl-web-rights/2006/06/28/1151174258981.html (accessed 29 June).

Hunter, C. (2000), ''Social impacts: internet filter effectiveness – testing over- and under-inclusive blocking decisions of four popular web filters'', *Social Science Computer Review*, Vol. 18 No. 2, pp. 214-22.

Kalathil, S. and Boas, T.C. (2003), *Open Networks, Closed Regimes: The Impact of the internet on Authoritarian Rule*, Carnegie Endowment for International Peace, Washington DC.

Lessig, L., Wendell, C. and Carlsmith, E.M. (2006), ''Testimony of Lawrence Lessig, C. Wendell, and Edith M. Carlsmith in Hearing on 'Network Neutrality''', US Senate Committee on Commerce, Science, and Transportation, Washington, DC. Available at: http://commerce.senate.gov/pdf/lessig-020706.pdf

Network Advisory Committee (2002), ''Commodity network bandwidth: problems and recommendations'', University of California, Berkeley, CA, September, available at: http://nac.berkeley.edu/bandwidth/

Neuman, W.R., McKnight, L. and Solomon, R.J. (1997), *The Godian Knot: Political Gridlock on the Information Highway*, MIT Press, Cambridge, MA.

Noam, E. (1994), ''Beyond liberalization II: the impending doom of common carriage'', *Telecommunications Policy*, Vol. 18 No. 6, pp. 435-52.

OpenNet Initiative (2005), ''Telus blocks consumer access to Labour Union web site and filters an additional 766 unrelated sites'', *OpenNet Initiative Bulletin*, No. 10, available at: www.opennetinitiative.net/bulletins/010/

Sandvig, C. (2003), ''An initial assessment of cooperative action in wi-fi networking'', *Telecommunications Policy*, Vol. 28 Nos 7/8, pp. 579-602.

Schuler, D. (1996), *New Community Networks: Wired for Change*, Addison-Wesley, New York, NY.

Surowiecki, J. (2006), ''Net losses'', *The New Yorker*, 20 March, available at: www.newyorker.com/talk/content/articles/060320ta_talk_surowiecki

USC Annenberg Center (2006), ''The Annenberg Center Principles for Network Neutrality'', Available at: www.annenberg.edu/news/news.php?id = 13

Wu, T. (2003), ''Network neutrality, broadband discrimination'', *Journal of Telecommunications and High Technology Law*, Vol. 2 No. 1, pp. 141-79.

Wu, T. (2005), ''One rule for telecommunications regulation'', paper presented to the 32nd Annual Conference on Communication, Information, and internet Policy. Washington, DC, available at: http://web.si.umich.edu/tprc/papers/2005/420/onerule.PDF

Yoo, C. (2004), ''Would mandating broadband network neutrality help or hurt competition? A comment on the end-to-end debate'', *Journal of Telecommunications and High Technology Law*, Vol. 3 No. 1, pp. 23-68.

Zittrain, J. and Edelman, B. (2003), ''Empirical analysis of internet filtering in China'', unpublished manuscript, available at: http://cyber.law.harvard.edu/filtering/china/

Further reading

Fulmer, C.E. (2006), ''When discrimination is good: encouraging broadband internet investment without content neutrality'', *Duke Law & Technology Review*, Vol. 6, available at: www.law.duke.edu/journals/dltr/articles/PDF/2006DLTR0006.pdf

Corresponding author

Christian Sandvig can be contacted at: csandvig@uiuc.edu