N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

# Network Transparency: Seeing the Neutral Network

*Adam Candeub & Daniel John McCartney*


Spring 2010 VOL. 8, NO. 2

Northwestern Journal of Technology and Intellectual Property
Volume 8, Number 2 (Spring 2010)

# Network Transparency: Seeing the Neutral Network

**By Adam Candeub & Daniel John McCartney***

## I. INTRODUCTION

¶1 Federal Internet policy is emerging from the net neutrality debate with a clear commitment to vague principles. What began as disputes over configuring routers grew into a dizzying scramble to defend the Internet as we know it – and it turned out, nobody knows it quite the same way. Still, the discourse over net neutrality has been productive. From its initial ambiguity, it blossomed into a rich literature on innovation policy and the future of communications in our democracy. It inspired deep thinking on the core dynamics that make the Internet worth defending.

¶2 While the politics remain unsettled, Congress charged the new Federal Communications Commission (FCC) to help develop a national broadband plan. The FCC is currently engaged in rulemaking to formalize its Internet policy. This rulemaking process begins with the FCC's four principles which ensure that users can transmit or receive content, run applications and use devices of their choice. More broadly, they entitle users to competition among network and service providers. The FCC is also adding two new principles: non-discrimination and transparency. Together, these six principles guide the FCC's program to preserve the Internet's openness and give the vague principles a richer form.

¶3 Chairman Genachowski articulated these goals in a speech at the Brookings Institution on Sept. 21, 2009.[1] In announcing the rulemaking, he explained that openness is the source of the Internet's power: "distributed innovation and ubiquitous entrepreneurship."[2] This power, he emphasized, is not just commercial, but also reveals itself as "an unprecedented platform for speech, democratic engagement, and a culture that prizes creative new ways of approaching old problems."[3] Yet, with all of these blessings, a network does not build itself; it must attract investors.

¶4 The Chairman's speech captured the core lessons from the net neutrality debate: the need for incentives to build networks and the need to ensure the decentralized structure and culture of the Internet. To these ends, the FCC now turns to the work of implementing the principles.

¶5 In this paper, we focus primarily on the newly added principle of "transparency." The Chairman asserted that "providers of broadband Internet access must be transparent

* We thank Joachim Täg and other commenters at the 2008 Telecommunications Policy Research Conference held at George Mason University School of Law.

[1] Julius Genachowski, Chairman, The Brookings Inst., Prepared Remarks for Preserving a Free and Open Internet: A Platform for Innovation, Opportunity, and Prosperity (Sept. 21, 2009), *available at* http://openinternet.gov/read-speech.html.

[2] *Id*.

[3] *Id*.

about their network management practices."[4] Transparency demands a technical and specific disclosure, and we propose such a disclosure regime.

¶6 In the past, it was evident how basic technical features of Internet interconnection and protocols produced confusion. This technical unreality is endemic to all debates about Internet governance. Thus, it was unclear how and who could determine what content was alike.[5] For networks blocking spam or malware, it was unclear if this qualified as "reasonable traffic management." For discriminatory peering and transit agreements among Internet Service Providers (ISPs) and backbones, it went unanswered whether this was a net neutrality concern. These questions are particularly nagging because of the secrecy surrounding the relevant data. The Chairman in his speech acknowledged some of these problems. With the forthcoming rulemaking, we will have the chance to achieve true transparency. Now, we can discover how the networks are managing our traffic internally and externally through their peering and transit agreements. With this network transparency, we will be able to truly evaluate the network's neutrality.

¶7 The policy justifications for disclosure are similarly strong. Internet policy cannot be made in an informational vacuum. Disclosure can serve the dual purposes of informing any potential policy and curbing anticompetitive behavior with minimal regulatory cost to either the government or firms. Calls for disclosure, however, have been ad hoc, with various Internet controversies like Comcast-BitTorrent prompting specific disclosures.[6] New "transparent" rulemaking gives hope for a more systemic effort. Of equal importance, transparency provides an opportunity to elaborate a specific purpose for a disclosure regime.

¶8 However, identifying Internet disclosure's nature, purpose, and goals is not as straightforward because traditional rationales come up short. First, the economic justification for disclosure—which allows for better consumer choice—seems inapplicable to the Internet because of the lack of competition among providers. Consumers lack choice, informed or otherwise.

¶9 Second, historically, the basis for telecommunication disclosure has been regulatory. This rationale is uncertain given the FCC's unsettled standard. The FCC is now unable to make any non-controversial rulings—a point the Comcast-BitTorrent Order discussed in Part 2 makes clear. While the emerging "openness" rulemaking gives hope for a clearer standard, the standard remains elusive for now.

¶10 Third, the typically "static" form of disclosure, like cost data for ratemaking, seems to be an inappropriate form for the Internet. Unlike traditional telephone networks, where routes and carriers are largely fixed, identifiable, and relatively few, Internet traffic travels through an unknown number of carriers on largely unspecified routes. We do not know how our packets will get where they are going until they have already arrived.

---

[4] *Id*.

[5] *See* Kevin D. Werbach, Only Connect (Feb. 20, 2007), *available at* http://ssrn.com/abstract=964991.

[6] *See, e.g.*, Philip J. Weiser, *The Next Frontier for Network Neutrality*, 60 ADMIN. L. REV. 273, 295-97 (2008). Interestingly, the FCC in the recent Comcast-BitTorrent Order states that it will decline to institute rule-making because it feared "unduly tying our hands should the known facts change." Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, 23 F.C.C.R. 13028, ¶ 30 (2008) [hereinafter *BitTorrent Order*]. At the same time, however, the FCC declined to impose any systemic disclosure requirements to cure its acknowledged ignorance. The FCC curses the darkness but has no interest in lighting a candle.

Furthermore, Internet packets are not uniform like voice on the telephone network. Telephone quality could be estimated with a few rough numbers; however, the quality of an Internet connection is a probabilistic function (mathematically sketched out below) that is not meaningfully captured by a handful of metrics.

¶11 Last, markets face a collective action hurdle to providing useful information about Internet access quality because the "quality" of a consumer's Internet experience depends not merely on his or her relationship with the ISP, but with the ISP's interconnection relationship to other networks. No one ISP has the ability or incentive to provide information about other networks so as to provide a more complete picture of Internet quality.

¶12 We argue that mandated disclosure should create "network transparency." We look to network engineering to propose a dynamic disclosure regime that enables consumers to react and even circumvent anticompetitive network managements. Rather than reproduce a static, regulatory disclosure, we encourage a "bottom-up," flexible type of network disclosure which reacts quickly to changes in network technology and provides the specialized, even individualized, revelations that traditional regulatory disclosure cannot. Such disclosures should produce better-informed consumers and, perhaps more important, provide a sort of net-roots antitrust enforcement. Moreover, these disclosures would legitimize and empower third parties to take part in the project of Internet governance.[7]

¶13 To achieve this end, we would require public disclosure of (i) each network's QoS policy with reference to some industry standard (like the widely used DiffServ architecture), (ii) all peering and transit agreements, as well as (iii) the implementation of these interconnection agreements by mandating a network's registration in the Internet Routing Register (IRR) or equivalent public registration.

¶14 The *immediate* goal of our proposed disclosure is neither to improve consumer choice nor to achieve a more effective regulatory oversight. Instead, by tracking the incentives that function in open source software collaborations, our proposed disclosure would be aimed at high-level network users, what we term with no doubt flattering vainglory, the "Internet vanguard."[8] Our disclosure is aimed at those with pecuniary, personal, and reputational interests in tracking, reacting to, and defending open networks. The goal is to strengthen the balance between network managers' tendency to centralize and users' tendency to innovate freely at the periphery.

## II. THE CHALLENGE OF INTERNET DISCLOSURE

¶15 In this section, we explore the justification for disclosure. Policy researchers need this disclosure of network management practices and interconnection agreements to understand how the Internet market works. Yet, it remains unclear *what* must be disclosed to improve consumer welfare and increase the amount of usable information for market decisions (as opposed to satisfying policy researchers' curiosity).

---

[7] *See* A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 803-05 (2003).

[8] Note to reader: we find this locution accurate, but somewhat ridiculous, and ask for any suggestions for different terms.

¶16 As alluded to above, unlike the telephone network's quality of service, Internet quality cannot be reduced into a few simple, easily understood metrics. This also raises the question of whether the audience will be able to comprehend the disclosure. The typical goal of disclosure—producing better-informed consumers or better-informed bureaucrats—seems inapt given that consumers right now have so little choice as to ISP. Improved information seems unlikely to improve efficiency in those highly concentrated markets. Further, the current status of regulatory oversight is unsettled. We do hope the forthcoming rulemaking will provide a clear standard to distinguish, in a non-arbitrary way, good discrimination from bad. For now, the standard remains hazy.[9]

¶17 In short, it is unclear (i) what should be disclosed, (ii) to whom it should be disclosed, and (iii) what it should achieve. The following examines each of these questions in turn.

### *A. Disclosure's Content*

¶18 Effective disclosure must actually aid consumers (or market intermediaries) in assessing the value of the product. But, determining this quality or value of Internet access presents difficult, even intractable, questions.

¶19 First, the scattered infrastructure means that owners each have their own discrimination policies and only know the identity of their set of adjacent peers. While one network can produce the information that it knows about—its local traffic policies and the peers to whom it connects—this information is not enough. In order to fix the value of access, even the most technically competent analyst needs to know more; she needs to know about the adjacent networks.

¶20 Second, even though one could estimate an ISP's value using a recursive function, as the sum of the value of their peers, reduced by the aggregate traffic discrimination among those peers, the ISP cannot be expected to disclose the traffic policies of all its peers, the policies of all their peers' peers, etc. This would amount to a single ISP disclosing the network policies of the entire accessible Internet. It is not clear that any one ISP would have the ability, let alone the incentive, to acquire the information to do so.

¶21 Third, even this complete recursive function would not accurately define an ISP's service value. Consumer value depends upon the types of traffic, scaled by the treatment each class receives from the networks on which it travels. This value does not lend itself to *ex ante* measurement. The road analogy is helpful here: what is the value to a property owner of having ready access to the road system? This would be a function of the classes of car traffic they would have, scaled by the speed or tolls that each class would face on all roads. This kind of inquiry requires great speculation, with costly uncertainty.[10]

---

[9] *BitTorrent Order*, *supra* note 6. Comcast has appealed the Order and an opinion is expected shortly. *See* Petition for Review, Comcast v. Federal Commc'ns Comm'n, No. 08-1291 (D.C. Cir. Aug. 29, 2009) [hereinafter *Petition for Review*].

[10] For an attempt to fix a value for this uncertainty, see Mark Gaynor & Scott Bradner, *Statistical Framework to Value Network Neutrality*, 17 MEDIA L. & POL'Y 24, 40 (2007) ("[W]hen market uncertainty is large it decreases the total value of a non-neutral network by 50 percent because the transport provider has picked such an average bundle of services that half of the potential users don't value it as high as its price.").

¶22 To demonstrate this uncertainty, it may help to draw out symbolically the value *V* of access to a single user *u*. This requires summing the Session values of all classes (or types) of traffic *C,* for all destinations (or sources) of that traffic *D*, that *u* would contact. The *Session* value to *u* of access to that destination *d* using just that class of traffic *c*, is a complicated function of (1) the destination *d*, (2) the class *c*, and (3) the treatment the traffic receives from each network between *u* and the *d*:

$$V_u \approx \sum_{c \in C_u} \left( \sum_{d \in D_u(c)} \left[ Session_u\left(d, c, \{T_n(c) \mid n \in N(u,d)\}\right)\right] \right)$$

| | |
|---|---|
| $V_u$ | the value of access to a single user *u* |
| $C_u$ | the set of all classes (or types) of *u*'s traffic |
| $D_u(c)$ | the set of all destinations (or sources) of *u*'s traffic of type *c* |
| $Session_u(d, c, treatment)$ | the value to *u* of *c* traffic receiving *treatment* when transmitted between *u* and *d* |
| $T_n(c)$ | the treatment network *n* gives to the traffic of class *c* |
| $N(u,d)$ | the set of networks along the path between *u* and *d* |

¶23 And this complicated formula is woefully reductive.[11] The *Session* function is complex and opaque. Even if we knew the class of traffic, the destination, the networks

[11] Some have made wildly speculative attempts to flesh out the utility function sketched above. For example, Hermalin and Katz put forth a model to try to capture "a household's utility from connecting to the [ISP] platform and consuming the available applications." Benjamin E. Hermalin & Michael L. Katz, *The Economics of Product-Line Restrictions with an Application to the Network Neutrality Debate*, U.C. BERKELY: COMPETITION POL'Y CTR. at 5 (July 28, 2006), *available at* http://repositories.cdlib.org/iber/cpc/CPC06-059 (last visited Apr. 15, 2010).

Such economic models by necessity make simplifying assumptions in hopes of revealing some underlying phenomenon. We do not weigh in on whether a model should be judged by the reality of its assumptions or instead by its predictive power. But we can still examine assumptions of their model to see what exactly the model aims to predict and what it deems safe to suppress.

Their model assumes that "there is diminishing marginal utility from consuming the content of any specific provider." This is suspect in fact and troubling in its predictive usefulness. Social networks are clear examples of communities where people seem to reap *increasing* "utility" as they "consume" more of the "product." And if we assume that they have diminishing returns, the model will suppress the value of human relationships by suggesting they become ever *less* important as they are lived.

There are a number of other troubling explicit and implicit assumptions in their model. But for now we focus on the most sweeping: the model assumes "[t]here is a unit mass of households with identical preferences." Without any qualifications, this is clearly not accurate (people like different things online); but, more damning, it suppresses the very defining characteristic of the long-tail of the Internet. If we want an economic model of a user's utility from accessing Internet, it will have to capture this world of niches.

Here the demanding challenge for economists is preserving their disciplinary assumption of exogenous uniform preferences, while adequately explaining the felt reality of heterogeneity that defines the Internet. *See generally* George J. Stigler & Gary S. Becker, *De Gustibus Non Est Disputandum*, 67 AM. ECON. REV. 76, 89-90 (1977) ("Our hypothesis is trivial, for it merely asserts that we should apply standard economic logic as extensively as possible. But the self-same hypothesis is also a demanding challenge, for it urges us not to abandon opaque and complicated problems with the easy suggestion that the further explanation will perhaps someday be produced by one of our sister behavioral sciences."). We do not aim to discourage

along the way, and the treatment each gives to the traffic, we still must wonder about the infinite possible communications that may be contained within that traffic. Are they reading Wikipedia, or editing it? Are they watching videos of riots in Tibet, or of a dog on a skateboard?[12] Also, how does the user's perceived value change, when a network along the way treats the traffic a little differently?

¶24 Despite these difficulties, observe that, of all the unknown variables in this function, the user cannot possibly know the treatment network *n* gives to the traffic of class *c*, $T_n(c)$, or the set of networks along the path between *u* and *d*, $N(u,d)$; they are the infrastructure details known only to the network owners. This keeps the user from performing this utility calculation. Similarly, the network cannot know the value of access to a single user *u*, $V_u$, the set of all classes (or types) of *u*'s traffic, $C_u$, or the set of all destinations (or sources) of *u*'s traffic of type *c*, $D_u(c)$, since they all depend on user preferences, so the network owner cannot make the calculation either. Furthermore, this whole formula ignores the timing of the choices. It tells of a fixed set of choices, which is absurd in the context of a rapidly changing Internet where new network configurations and new networked applications are introduced and removed all the time.

¶25 Even if we just take the *average* value of some class of traffic, the dimensions used to approximate this calculation (class, treatment, direction) are interdependent and resist reduction into simple terms. For example, the value to a consumer of a certain traffic class—say traffic with streaming video characteristics—greatly depends upon the content of the video (or of the traffic flow that appears to the network to be a video stream. Recall, the network can only make statistical inferences about the actual content of traffic). Further, this particular video stream may be encoded in such a way as to combat some prevalent network delays or disruptions, but the same encoding may leave it more vulnerable to other disruptions.

¶26 All of this suggests that networks have little incentive to provide disclosure, and it is unclear that any regulatory mandate could provide perfect, or even useful, disclosure. The strategy we employ gives those necessary bits of information—the raw instrumentalities—to those who have an incentive and capacity to tease meaning out of this raw data, *i.e.* the "Internet vanguard," a group discussed below. They will craft the necessary disclosure, tailored to the needs of a shifting Internet community at-large, that no regulation could possibly foresee.

### *B. Disclosure's Audience*

¶27 Many advocates of Internet disclosure appear to believe that disclosure will allow for efficiency-enhancing consumer behaviors. In other words, consumers will choose ISPs with network management disclosure policies closer to their desired tastes—which would include non-discriminatory networks.[13] There are several problems with this scenario.

---

modeling efforts by economists; rather, we hope they can find a way to creatively explain this seemingly "opaque and complicated problem."

[12] Skateboarding Dog, http://video.google.com/videoplay?docid=-8762816342722081405 (last visited Apr. 15, 2010).

[13] *See, e.g.*, Barbara van Schewick, Oral Testimony at the Federal Communications Commission's Second Public En Banc Hearing on Broadband Network Management Practices at Stanford University,

¶28 The primary problem is that most people do not really have a choice among ISPs.[14] If there really is no choice within the competitive broadband market, information will not be useful to enhance the performance of the market. People will only gain a better understanding of the extent of their ISP's market power and their own consumer impotence.

¶29 Another problem with targeting consumers generally is the technical complexity of the disclosures. The disclosure will be of little use to the typical consumer. Like the disclosure on prescription drugs, which require an advanced degree in pharmacology to understand,[15] technical disclosures of traffic management and peering relations cannot provide guidance to the average consumer.[16]

### *C. Disclosure's Purpose*

¶30 When a producer can provide, convey, or obtain the pertinent information at a lower cost than can the consumer, mandatory disclosure may be appropriate.[17] Such disclosure provides the market, in the cheapest way, the information that will allow consumers to buy things that best match their ideal preferences, resulting in economic efficiency.[18] In theory, by diminishing a firm's ability to exploit consumers' ignorance (by demanding higher prices or by delivering lower quality goods), mandatory disclosure increases market efficiency. Not surprisingly, mandated disclosure exists in situations like food labeling, in which the consumer cannot easily ascertain an important product characteristic,[19] *e.g.*, does my cupcake have trans fats?

¶31 However, mandated Internet disclosure alone does not seem likely to improve consumer surplus or efficiency. This is true primarily because consumers have so few

---

Docket No. 07-52, at 3 (April 17, 2008), http://www.fcc.gov/broadband_network_management/041708/vanschewick-written.pdf. ("[D]isclosed information must provide enough detail to enable customers to make an informed decision and to enable them to adjust their behavior. Comcast's current acceptable use policy falls short of these goals.").

[14] *See* FEDERAL COMMC'NS COMM'N, INDUSTRY ANALYSIS AND TECHNOLOGY DIVISION, WIRELINE COMPETITION BUREAU, HIGH-SPEED SERVICES FOR INTERNET ACCESS: STATUS AS OF JUNE 30, 2006 3 (2007), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-270128A1.pdf .

[15] Or a consumer may forgo a pharmacology degree and simply search the Internet. *See, e.g.*, WebMD–Better Information, Better Health – Drug Index, http://www.webmd.com/drugs/index-drugs.aspx (last visited Apr. 15, 2010) ("Search for prescription and over-the-counter medications by brand or generic name, or by condition."). Medical advice online is controversial in part because of the gravity of the subject and the rent-protecting behavior of medical professionals. This sourcing of experts to digest the disclosures into a widely useful form mirrors part of the mechanism we envision in our disclosure proposal, albeit in a much different field.

[16] The technical terms of network management policy will be incomprehensible to consumers who sign up on the phone for Internet access. *Cf.* Douglas A. Hass, *The Never-Was-Neutral Net and Why Informed End Users Can End the Net Neutrality Debates*, 22 BERKELEY TECH. L.J. 1565, 1630-31 (2007) (describing how disclosing traffic control policies directly to consumers, similar to the Fair Credit Act, "would help consumers more easily compare different service offerings"). Also the ISP's peering relationships are not meaningful without reference to the topography of the rest of the Internet; an ISP cannot be expected to know this topography let alone to disclose it to the consumer over the phone. Instead, there must be a bridge to close the gap between users who are positioned to signal their preferences and the meaning of the technical information that an ISP discloses.

[17] RICHARD POSNER, ECONOMIC ANALYSIS OF LAW § 4.6, at 111 (6th ed. 2003).

[18] *Id*. ("A monopolist (or cartel) may have a greater incentive than a firm in a competitive industry to misrepresent the qualities of its product.").

[19] *Id*. at 113.

choices in their broadband providers. It does not help to learn about the deficiencies of your provider if you cannot switch to another. Further, disclosure must be easily understood by consumers in order to aid their choices. As the above discussion shows, no such metrics currently exist.

¶32 Historically, a telecommunications disclosure has not served to inform consumers; it has served to inform regulators, primarily for rate-making functions. For instance, for almost a century, long-distance companies submitted cost information to substantiate their tariffs. The FCC knew what to do with this disclosure because rate-of-return or price cap regulation reflected coherent regulatory goals with an established implementation. Regulators had their own goals: set prices that give adequate returns to producers and would emerge in the absence of market power.

¶33 In contrast, it is not quite clear what the FCC would do with proposed network disclosure because there is no accepted standard as to what constitutes legitimate Internet discrimination. The FCC has a chance in the forthcoming rulemaking to establish such a standard, but the BitTorrent order should stand as a warning to the new FCC about how *not* to regulate with clarity.

¶34 In the BitTorrent order, the FCC ruled Comcast's deep-packet inspection and packet injection techniques violated, in a *prima facie* way, the FCC's two Internet principles of allowing consumers to run any application they wish and maximizing consumer control.[20] To reach this conclusion, the FCC found that Comcast "blocked," or at least "delayed" traffic in a discriminatory fashion.[21] Recognizing that traffic management may justify blockage or delay, the FCC created a test to determine the acceptability of an ISP's management—whether the blocking or delaying methods are "carefully tailored to its interest in easing network congestion" and/or constitute "reasonable network management."[22]

¶35 This test, borrowing strangely from constitutional strict scrutiny analysis, fails to provide meaningful guidance to network operators. Under traditional First Amendment strict scrutiny analysis, a court upholding a government speech restriction must find that it (i) furthers a compelling state interest and (ii) constitutes a "narrowly tailored" means of doing so.[23] For instance, the Supreme Court, in upholding the Federal Election Campaign Act's restriction on federal campaign contributions, found that such restrictions were "marginal," but the state's interest in prohibiting vote buying was compelling.[24]

¶36 The problem the FCC faces in adopting this test for traffic shaping is that *all* network management and policies can limit consumers' ability to run applications or minimize their control. The FCC assumes that an ISP has a menu of options to achieve a given degree of network usage and that it can pick the least restrictive or "narrowly tailored" option. Such a rule is unrealistic—it needs greater specificity. The FCC gives no metric or conceptual rule to guide a network in managing a congested network. The only rule it announced is a one-off prohibition on egregious practices by Comcast,

[20] *BitTorrent Order*, *supra* note 6, ¶ 44.
[21] *Id.* ¶ 45.
[22] *Id*. ¶¶ 44-48.
[23] JERRY KANG, COMMUNICATIONS LAW & POLICY 225 (3d ed. 2009).
[24] Buckley v. Valeo, 424 U.S. 1, 20-22 (1976).

aggravated by misleading public statements.[25] The forthcoming rulemaking must give more meaningful guidance to network operators, or else the rules will fail at their purpose.

## III. WHAT IS CURRENTLY DISCLOSED

¶37 We do not need to mandate disclosure of what is already disclosed. Those with pecuniary, personal, and reputational interests already attempt to track network management techniques. A varied group of academics, professional programmers and engineers, hobbyists, and others, the aforementioned "Internet vanguard" already have developed ways to estimate what the network is doing. A skilled hacker[26] can poke and prod at the network in an effort to estimate some of the data that we suggest disclosing.

¶38 In this section, we explore these limits. We review (i) efforts to detect a network's (like an ISP's) traffic management practices to control and shape traffic *within* its network and (ii) efforts to determine the interconnection relationships between networks. If these estimates were revealing enough, our disclosure proposal would be redundant, yet, as discussed, the techniques are limited and underscore the need for a regulatory response.

### *A. Uncovering Internal Traffic Management*

¶39 Dan Kaminsky frequently gives speeches entitled "Black Ops of TCP/IP."[27] Kaminsky, a network security researcher—otherwise known as a hacker with a business card—discusses his latest efforts to do "bad" things to TCP/IP. In his 2006 and 2007 talks, he described two ways for a consumer to detect network neutrality. He clarified the network neutrality problem using the language of Internet exceptionalism: rather than defending network neutrality, the focus should be on detecting and defending against "provider hostility."[28]

¶40 While his techniques are clever, providing some blurry-eyed detection of "provider hostility," they are severely limited. The 2006 technique relies on error-prone inferences made worse by conflating factors.[29] The 2007 technique has to make use of unrelated

---

[25] *BitTorrent Order*, *supra* note 6; s*ee Petition for Review*, *supra* note 9.

[26] The term "hacker" in this context refers to the tinkering sort. *See* Gary Scott Malkin & Tracy LaQuey Parker, *Internet Users' Glossary*, http://www.apps.ietf.org/rfc/rfc1392.html (defining "hacker" as "[a] person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular").

[27] *See generally* DoxPara Research, http://www.doxpara.com (last visited July 29, 2009) (listing previous *Black Ops* presentations along the right-hand side).

[28] Dan Kaminsky, Remarks at Def Con 15: Black Ops 2007: Design Reviewing The Web, at 32:06, http://video.google.com/videoplay?docid=3470502418262982787 [hereinafter *Black Ops of TCP-IP 2007*] (explaining that "[i]t's not about defending network neutrality; network neutrality is the fricken status quo" instead "[w]hat's actually suggested is 'provider hostility'"). He describes one kind of provider hostility, the "Times Square Effect:" like the altered ads in a movie depicting Times Square in New York City, the ISP alters a webpage to display its own advertisements. An ISP, he explains, may alter search results to insert a link atop the results, or to replace web contents with its own. *Id.*

[29] In his 2006 talk, he introduced a method for detecting when an ISP is treating some traffic differently than others. His method simulates traffic patterns and checks whether one receives better (web surfing) or worse (P2P file sharing) treatment from the network. *See* Dan Kaminsky, Remarks at the www.ToorCon.org Information Security Conference: Black Ops Of TCP-IP 2006, at 3:42, http://video.google.com/videoplay?docid=2235822817954898588 (last visited Apr. 15, 2010). This

security bugs, is deeply inefficient, and still cannot detect many forms of traffic management.[30]

¶41 The Electronic Frontier Foundation recently made the first release of its "Switzerland" software.[31] Instead of squeezing through a security bug (as did Kaminsky's 2007 method), Switzerland lets users explicitly coordinate with a trusted third party to validate traffic. It detects any drop, forgery, or modification between any two computers, when both are running the software. It also tracks a variety of meta-data about the quality of the connection, in hopes of someday detecting more subtle interference.[32]

¶42 This software is still in its infancy, but it already allows consumers to detect the most blatant practices by ISPs, like forging packets.[33] Despite this accomplishment, Switzerland is unable to reliably detect more subtle (and common) techniques of ISPs—unless and until a broad community forms to coordinate its use by aggregating and analyzing the meta-data. Even then, the policies can only be roughly inferred. Like Kaminsky's first detection tool, Switzerland must make an error-prone inference in the face of conflating factors (like unintended network performance fluctuations). Switzerland also cannot be certain which network between the two connected computers is actually causing the discrimination.

### *B. Inferring External Interconnection*

¶43 Moving away from efforts to detect the network's internal traffic management, we look now at efforts to infer how the networks are externally interconnected. The topology of the Internet remains the focus of many network researchers, yet the data required for this research is scarce and not widely available.[34] Furthermore, there are many conceptual "maps" of the Internet. We are interested specifically in how separately administered networks are interconnected.

¶44 One way to map the Internet is by tracing the way data is routed between IP addresses—IP topology. Most computers come with a "traceroute" program that gives a

---

method is highly error-prone. The user must guess at the classes of traffic being mistreated, then must fool the ISP by simulating it realistically. Also, measuring the relative treatment that the ISP is giving each class of traffic introduces large margins of error because of conflating factors (like unintentional network performance fluctuations). Finally, as Kaminsky mentioned in his talk the following year, the tool has the effect of flooding the network. *Black Ops of TCP/IP 2007*, *supra* note 28, at 31:45 ("Right, like I want to be the guy who tests the network by breaking it."). This shows the delicate position of a principled Internet exceptionalist: he wants to win the war without destroying the countryside.

[30] The 2007 technique is a kind of benign exploit that makes use of an unrelated security bug. Roughly speaking, his technique involves use of a trusted third-party to verify the contents of ongoing connections, to detect when an ISP tries to make this sort of alteration. *See Black Ops of TCP/IP 2007*, *supra* note 28, at 31:20. He explains that this technique is very messy (since it relies on bugs in another protocol) and that it is not a long-term solution. He predicts that complete network encryption, while costly and inefficient, may be inevitable; the ad-supported model of many websites will demand it.

[31] Electronic Frontier Foundation, *Switzerland Network Testing Tool*, http://www.eff.org/testyourisp/switzerland (last visited Apr. 15, 2010).

[32] Peter Eckersley, Switzerland Design (May 2008), http://switzerland.svn.sourceforge.net/viewvc/switzerland/trunk/doc/design.pdf.

[33] This forging of packets is what Comcast was caught doing, so Switzerland can now detect that technique.

[34] *See* Dmitri Krioukov et al., *The Workshop on Internet Topology (WIT) Report*, ACM SIGCOMM COMPUTER COMM. REV. at 69 (Jan. 2007).

user the path of IP addresses along the way to a specified destination. The traceroute software attempts to plot out the sequence of intermediate hosts between the source and destination. It sends a series of packets addressed to the destination so that the network will send them along the path to the destination. The trick is that the packets are crafted to *not* make it all the way to the destination and to reveal the IP address of the last hop that they managed to reach. By crafting each packet to go one hop further than the last, the traceroute tool receives the sequence of IP addresses between the source and destination.[35]

¶45 The Cooperative Association for Internet Data Analysis (CAIDA) developed a tool named "skitter" to collect this traceroute data from 25 strategically placed locations around the Internet.[36] At each of these 25 places, they perform traces to as many addresses on the Internet as they can (they keep a list of destination IP addresses; the goal is to hit every nook and cranny of the net).

¶46 However, when a traceroute reveals the sequence of IP addresses, it does not quite reveal how any networks are interconnected. Instead, we have the interconnections between IP addresses—we have the IP topology—and some of these IP addresses may reside within the same network. To get network topology (the set of interconnections between separately administered *networks*) each IP address must be translated into the network on which it resides. This translation requires a mapping between IP addresses and the network that administers that address. It's like knowing the cities when you want a map of countries—you must be able to match city (IP) to country (network).

¶47 To understand how networks are identified, we must explore inter-network protocols (that is, protocols that handle routing between not just two devices but between two separately administered networks). One problem that Internet protocols are designed to address is the coordination of separately administered networks as a single utility.[37] When a computer sends out a packet destined for a particular IP address, how does a router know where to send it next? This routing problem is solved in two parts: internally (using "interior gateway protocols") and externally (using "exterior gateway protocols").

¶48 Interior gateway protocols (IGPs) handle routing traffic within a set of routers that are commonly controlled.[38] A network administrator has complete control over these

---

[35] Each IP packet has a "time to live" value (TTL) which indicates the number of hops the packet should "survive"—after that many hops, the packet should be dropped by the network. This works by having each hop decrement the TTL by 1. When the packet is dropped, the last hop it reached sends a packet to the original sender indicating that the packet did not reach its destination. This notice (from the intermediate host along the path between source and destination) includes the address of the intermediate host. So the traceroute tool crafts each packet to go just one-hop further than the last (i.e. has a TTL of 1 more than the last), recording the address of the intermediate hosts along the way.

[36] *See* Priya Mahadevan et al., *The Internet AS-Level Topology: Three Data Sources and One Definitive Metric*, ACM SIGCOMM COMPUTER COMM. REV. at 17-18 (Jan. 2006) (describing how CAIDA's "skitter" collects traceroute data).

[37] David D. Clark, *The Design Philosophy of the DARPA Internet Protocols*, ACM SIGCOMM COMPUTER COMM. REV. at 106 (Aug. 1988) (describing "some of the early reasoning which shaped the Internet protocols" to explain "why the protocol is as it is").

[38] Two prominent examples of IGPs are IS-IS and OSPF. *See generally* Richard P. Colella, Ross Callon, Ella P. Gardner & Yakov Rekhter, *Guidelines for OSI NSAP Allocation in the Internet*, at 8-12, http://www.apps.ietf.org/rfc/rfc1629.html (last visited Apr. 15, 2010) (describing IS-IS); John Moy, *OSPF Version 2*, at 6-7, http://www.apps.ietf.org/rfc/rfc2328.html (last visited Apr. 15, 2010) (describing OSPF as an IGP which "means that it distributes routing information between routers belonging to a single Autonomous System").

routes since the traffic is only traversing his own network. These internal routes are not important for this interconnection discussion.[39]

¶49 Exterior gateway protocols (EGPs) handle routing traffic among separately administered networks.[40] On the public Internet, a separately administered network is called an "autonomous system" (AS), and each AS is assigned an identifying number (called an ASN).[41] The "Border Gateway Protocol" (BGP) is the EGP used on the public Internet to exchange routing information among these ASes.[42] So when an AS arranges to interconnect with another AS, they use BGP to exchange routing information (the path to get to some IP address).

¶50 The BGP session between two ASes is important because it implements their interconnection agreement. When an AS arranges to interconnect with another AS, they will have to decide what traffic they will carry from each other. These interconnection agreements come in many flavors.[43]

¶51 To implement the agreement each AS must configure their externally facing BGP router. They will specify which routes it will accept or share in the BGP session with their neighbor. It also specifies which IP addresses are within their AS. In this way, the BGP session between pairs of neighboring ASes technically defines their interconnection.

¶52 Network researchers have two ways to get information about the various BGP sessions ongoing between ASes on the public Internet. The first way is to set up their own AS and interconnect with networks on the Internet which provide a view of the global Internet routing system from that perspective. This kind of perspective of the Internet's routing system is revealed by some networks using "Looking Glass" software

---

[39] Note that while the internal routes are not important here, the internal traffic management *is* important but is not part of this external interconnection discussion.

[40] We refer here to the general category of EGPs, not to the old "EGP" (itself an instance of an EGP) that BGP (another, more modern EGP) builds upon. *See* Yakov Rekhter, Tony Li & Susan Hares, *A Border Gateway Protocol 4 (BGP-4)*, at 7, http://www.apps.ietf.org/rfc/rfc4271.html (last visited Apr. 15, 2010) ("[BGP] is built on experience gained with EGP").

[41] The number space for ASNs is scarce. Currently, the ASN numbering system is transitioning from the original 2-byte sized ASN (with a maximum of around 65,000 ASNs) to a 4-byte sized ASN (raising the count to around 4-billion). Still, these numbers must be assigned. The Internet Corporation for Assigned Names and Numbers (ICANN) develops the broad policy for issuing AS numbers. The Internet Assigned Numbers Authority (IANA) then implements this policy by allocating blocks of ASNs to Regional Internet Registries (RIRs). A qualifying network can then register for an ASN from their RIR. *See* ICANN, *Global Policy for Allocation of ASN Blocks to Regional Internet Registries* (July 31, 2008), http://www.icann.org/en/general/global-policy-asn-blocks-31jul08-en.htm (last visited Apr. 15, 2010) (describing how the IANA must allocate ASN blocks to RIRs who in turn assign these ASNs to organizations); *see also* ARIN, ARIN NUMBER RESOURCE POLICY MANUAL § 5 (Aug. 5, 2008), http://www.arin.net/policy/nrpm.html (last visited Apr. 15, 2010) (describing one RIR's policy for assigning ASNs to organizations); *ASO - RIR Links*, http://aso.icann.org/Internet-community/regional-Internet-registries-rirs/ (last visited Apr. 15, 2010) (listing by ICANN of all RIRs and their associated regions); John Hawkinson & Tony Bates, *Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*, http://www.apps.ietf.org/rfc/rfc1930.html (last visited Apr. 15, 2010) (describing scenarios when a network should, or should not, try to acquire an ASN).

[42] *See* Rekhter, Li & Hares, *supra* note 40, at 4 (specifying the BGP standard).

[43] One way to categorize these agreements is as either "peering" or "transit." While the distinction is not always clear, peering generally refers to a more balanced exchange (carrying each others traffic as "peers") whereas transit involves one AS paying another to carry traffic (carrying the traffic as "provider"). It is sometimes conceptually helpful to make a strong distinction between these two sorts of arrangements, but from a technical perspective, the amount of money changing hands is not important. What *is* important is the way traffic is actually routed. This implementation is reflected in the reachable addresses announced by an AS to his BGP neighbors.

which lets the public issue (usually limited) sets of commands to display the Internet's routing system from that network's perspective.[44] The University of Oregon's "Route Views" project aggregates BGP data from a number of different locations (perspectives) around the world to provide a more complete view.[45]

¶53 Another source for BGP session data is the Internet Routing Registry (IRR).[46] This is a place where an AS can voluntarily register their BGP configuration.[47] If the AS registers their BGP configuration in the IRR, they can then set up their BGP routers to be automatically configured. Some backbone providers require this registration of their customers,[48] but others do not; and providers are free to input misleading data. This can make the IRR data inaccurate.[49]

¶54 We have now seen three ways to infer the interconnection relationships between networks, and each gives a view along a different dimension: (1) using traceroute to get IP address paths and then mapping these to ASNs (a "data" view); (2) the "Route Views" method of setting up an AS and recording routing tables (a "control" view); and (3) the voluntary IRR where networks register themselves (a "management" view).[50] None of these methods provides enough reliable or useful data.[51] Unless and until there is an overhaul of the inter-network routing architecture such that the routing is exposed to the end-user,[52] our disclosure proposal aims to improve the quality of data produced by these existing methods so that they become more useful.

---

[44] *See generally* Welcome, http://www.bgp4.net (last visited Apr. 15, 2010) (listing various "looking glass" resources).

[45] Advanced Network Technology Center, University of Oregon, *University of Oregon Route Views Project*, http://www.routeviews.org/ (last visited Apr. 15, 2010).

[46] Internet Router Registry, *Overview of the IRR,* http://www.irr.net/docs/overview.html (last visited Apr. 15, 2010) ("The Internet Routing Registry (IRR) is a distributed routing database development effort.").

[47] Within the IRR, these routing policies are described using the Routing Policy Specification Language (RPSL). *See* David Meyer et al., *Using RPSL in Practice* (Aug. 1999), http://www.apps.ietf.org/rfc/rfc2650.html (last visited Apr. 15, 2010) (explaining in practice how to specify, register, and analyze routing policies using RPSL).

[48] *Id*. at 2 ("CW, ANS and CA*Net customers are generally required to register their policies in their provider's registry. Others may register policies either at the RIPE or RADB registry, as preferred.").

[49] *See* Mahadevan et al., *supra* note 36, at 19 (discussing both intentional and unintentional inaccuracies in the IRR).

[50] *Id.* at 25 ("It remains an open question which data source most closely matches actual Internet AS topology, given that each graph approximates a different view of the Internet looking at the *data* (skitter), *control* (BGP), and *management* (WHOIS) planes.") (emphasis added). Note that the "WHOIS" tool is used to access the IRR.

[51] "In its current state, Internet topology research is not an informed discipline since available data is not only scarce, but also severely limited by technical, legal, and social constraints on its collection and distribution." *See* Krioukov et al., *supra* note 34.

[52] One particularly interesting proposal—"A New Inter-Domain Routing Architecture" (NIRA)—to overhaul the interconnection architecture was proposed in 2004. Xiaowei Yang et al., *NIRA: A New Inter-Domain Routing Architecture*, 15 IEEE/ACM TRANSACTIONS ON NETWORKING at 775 (Aug. 2007) (describing a new architecture "that gives a user the ability to choose the sequence of providers his packets take"). NIRA lets end users control the path their packets travel. This puts the end-user in the position to transact more directly with the backbone providers. This not only aligns the industry structure along user's preferences, but it also makes end-to-end QOS more feasible. If something like NIRA is adopted it would remove the conceptual distinction we make between *internal* traffic management and *external* interconnection—the traffic management becomes part of the end-user's interconnection selection. For more on NIRA, Xiaowei Yang's dissertation goes into even greater detail. *See* Xiaowei Yang, NIRA: A New Internet Routing Architecture (2004) (unpublished Ph.D. dissertation, Massachusetts Institute of Technology) (on file with Computer Science & Artificial Intelligence Lab, Massachusetts Institute of

## IV. NETWORK TRANSPARENCY: A PROPOSAL

¶55 Networks should be forced to disclose their internal traffic management and their external interconnection relationships. We begin with an overview of this proposal, and later describe each part in more rigorous detail. In describing these disclosure requirements, we must beware of the dangers of specificity: it risks fixing the state-of-the-art and thereby ossifying network engineering practices, forcing it into a rigid mold.

¶56 We propose a disclosure aimed at the more scattered audience that we term the "Internet vanguard." The Internet vanguard are those with the technical competence and the inspiration—whatever its source—to use the disclosure. This is a varied group with shifting and often conflicting interests including hobbyists, academics, application developers and infrastructure owners. We seek to expose network practices so the knowledge will serve as another arrow in the quiver of the Internet vanguard. The hope is to blunt any negative impacts of non-neutral networks without outright prohibiting them.[53]

¶57 The first set of disclosures reveals the network's internal traffic management, its "QOS policy." This shows all that happens to a user's traffic *inside* the network. This requires disclosing the combinations of techniques and algorithms that are used to classify traffic and to actually implement a "QOS policy."[54]

¶58 The second disclosure reveals the ISP's interconnections. After (or before) surviving the ISP's internal traffic treatment, this disclosure looks *outside* to show where traffic travels. There are at least two ways to require this. For reasons we discuss below, accurate and timely participation in the IRR seems the most cost-effective way to reveal the interconnections.

### *A. Internal QOS*

¶59 The fear of ossifying network engineering is especially felt in describing the QOS disclosure requirement. The form of disclosure required must be open ended to allow flexibility in implementing these mechanisms. The hard part is balancing disclosure uniformity, on the one hand, against design flexibility on the other. We want to craft the internal disclosure requirement with enough reference to a standard (like the widely used "DiffServ architecture" we discuss *infra*) without stifling design flexibility. Complete

---

Technology).

[53] *See generally* JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008). The P4P effort attacks the problem from a similar approach (exposing infrastructure to application). *See* P4P, http://openp4p.net. But P4P targets the narrow realm of P2P file sharing and focuses mostly on performance increases (P2P applications perform better when they know what kind of network they are running on: they can pick nearby peers). This only indirectly addresses NN concerns since it aims only at reducing network load from P2P traffic (the decreased load would theoretically diminish the incentive to discriminate). It does not address the broader structural concerns about human communications or about content development and control. Also, the P4P solution (ISPs sharing their topology to P2P applications) rests precariously on the accuracy of the ISP's disclosure. Without some teeth to force ISPs to accurately disclose, this leaves the applications vulnerable to ISPs' incentives to misrepresent in order to minimize their costs (to the detriment of application performance). Still, the P4P project is—in theory—a creative and interesting attempt to cooperate; hopefully it can resolve these issues.

[54] We explore this terminology below.

flexibility, however, undermines the usefulness of the disclosure; the less uniform the disclosure, the more complex and difficult it is to develop useful tools.

¶60 QOS architecture is important because it outlines the form of this disclosure requirement. Before introducing the components of QOS architecture, it is important to carefully explain what "architecture" means in the network engineering context. When we talk about architecture, the term is not merely a creative way to say design and construction. Instead, it means a "kind of abstract thinking about resources and relationships" that results in "a set of high-level design principles that guide the technological design" of the implementation.[55] In this way, architecture does not mechanically instruct the technical design, rather it provides a way "to ensure that the resulting technical design will be consistent and coherent—the pieces will fit together smoothly—and that the design will satisfy the requirements" of the architecture.[56] With such a flexible framework, our disclosure requirement strikes a balance between useful uniformity and network design freedom.

¶61 There are two primary QOS architectures: integrated services ("Intserv") and differentiated services ("Diffserv"). Intserv lets each application reserve a portion along each node of the network.[57] In contrast, Diffserv classifies the traffic and then treats it according to the class's previously-selected policy.[58]

¶62 We focus on Diffserv because, as a result of overcoming the scalability issues of Intserv, it is more widely deployed in private and public networks.[59] The Diffserv QOS architecture describes a system where each router has a set of classes each corresponding to a treatment. A set of Diffserv routers that together implement a QOS policy are called a Diffserv "domain." At each router, a packet is classified and then treated accordingly. Our disclosure requirement compels disclosure of the composite treatment across the domain.

---

[55] ROBERT BRADEN ET AL., DEVELOPING A NEXT-GENERATION INTERNET ARCHITECTURE 3-4 (2000), *available at* http://www.isi.edu/newarch/DOCUMENTS/WhitePaper.pdf.

[56] *Id*. In network engineering, the architecture is to the implementation much the way the principle is to the rule in law. The implementation flows from the architecture, and changes to the implementation must still fit within the general principles of the architecture.

[57] Robert Braden et al., Integrated Services in the Internet Architecture: An Overview, June 1994, http://www.apps.ietf.org/rfc/rfc1633.html (last visited Apr. 15 2010) (discussing the IntServ architecture).

[58] Steven Blake et al., An Architecture for Differentiated *Services*, Dec. 1998, http://www.apps.ietf.org/rfc/rfc2475.html (last visited Apr. 15 2010) (discussing the DiffServ architecture).

[59] Intserv is unworkable (and thus unused) on the public Internet because it is expensive at large scale and it requires end-to-end coordination. JOHN EVANS & CLARENCE FILSFILS, DEPLOYING IP AND MPLS QOS FOR MULTISERVICE NETWORKS: THEORY AND PRACTICE 149-50 (2007) [hereinafter DEPLOYING QOS]. The Intserv QOS architecture describes a system for each application to reserve network resources. An application running on a user's computer wants a certain QOS from the network (that is, the application wants its traffic to be given a certain treatment by the network). The request (including the class of quality required) is forwarded on to each subsequent node in the network along the path to the destination, with each node confirming the request if it can. In this way, the path is guaranteed to provide the quality required. The problem is a router has to keep track of all ongoing traffic to avoid confirming too many requests. This has to be done in each router on the network. In this way, Intserv is both expensive to deploy in a large network and further complicated by the diversity of owners of the routers on the public Internet. A Diffserv domain scales better than Intserv because it does all the classifying of traffic at the edges of the network, and only keeps track of each class, rather than tracking each flow of traffic. *Id*.

1. Classification or "Trust"

¶63 Before treating the traffic, a Diffserv domain must classify each packet into one of a limited number of classes. The selected class is important because it dictates how the traffic will be treated. The classification is done as near as possible to the edge of the network (near the source of the traffic), to simplify the network design.[60] Subsequent hops along the way need only respond to the class as marked on the packet, rather than keep track of each connection.

¶64 There are generally two ways to classify and mark traffic. "Source marking" is when the end-system (the computer that generates the traffic) marks its own traffic as belonging to some class.[61] "Ingress marking" is when a node (a router) close to the source device uses a classification technique to mark the traffic.[62]

¶65 The choice between marking at the source or upon ingress brings us another vocabulary gem: "trust." When the Diffserv domain will rely on the classifying marks made by a device, the device is "trusted."[63] This trust may be limited; some kinds of classification mechanisms (sometimes called "color-aware") perform their own complex classification and only incorporate the incoming marking as one input to a new classification.

¶66 This "trust" has not been as misused as some other network engineering terms. But, it is easy to see how it might be: "My ISP does not trust me to say how important my traffic is!" While this trust is fairly close to its literal meaning, it is important to understand exactly what it means: it describes the reliability of the pre-existing traffic classifications. If a network disclosure indicates that the network does not "trust" its users, this should be understood in its precise technical meaning.

2. Routing or "Fairness"

¶67 After classifying the traffic (or trusting the pre-existing marking) the router then schedules their departure. This scheduling is where the QOS policy will be translated into algorithms to actually control the traffic. When a router's scheduling algorithms faithfully implement a QOS policy, it is considered "fair."

¶68 This "fairness" is particularly vulnerable to misunderstanding; when interpreting a network's disclosure, we must keep in mind its precise meaning. It is generally used simply as a metric when evaluating how well a scheduler achieves a desired bandwidth allocation.[64] This sense of "fairness" has more to do with conforming to rules than it with being equitable or even-handed. While there has been some effort to alter the focus of the technical research community, the focus has remained on flow-rate fairness, and each flow *of a given class* should be treated equally.[65]

---

[60] *Id.* at 99 ("as close to the traffic source as possible in order to simplify the network design").

[61] *Id.* ("Packet marking may be applied at the source end-system itself; if the end-system is considered to be *trusted* then this marking may be relied upon throughout") (emphasis added).

[62] *Id.* at 100 (describing how a trusted device close to the end-systems will perform implicit or complex classification when the end-systems are "not capable of" or "cannot be trusted to" mark their own traffic).

[63] *Id.* at 99.

[64] *Id.* at 118 ("how closely the scheduler achieves the intended bandwidth allocation"); *id.* at 123 (repeated).

[65] Bob Briscoe, *Flow Rate Fairness: Dismantling a Religion*, ACM SIGCOMM COMPUTER COMM. REV. at 65 (April 2007) (arguing that current research on "fairness" continues to fail because it focuses on the

¶69 This flow-fairness is surprising in two ways. First, "fairness," so-defined, takes the classification policy as given. To an outsider, saying that something is fair because it conforms with rules just begs the question: what rules? This sense of fairness is very much *not* a proxy for any broader equitable sense of the term because the classifying criteria and their associated treatment—the rules—are not evaluated for their normative desirability. The second related surprise is "fairness" does not look at whose computer is generating the flow. If one user's application generates 10,000 flows of a certain class, while a second user generates only 1, each of the 10,001 flows are seen as formally equal in the eyes of this "fairness." This highlights a difference of perspective.

¶70 From the ISP perspective, it is a problem when "fairness" ignores the identity of source. These network operators must concern themselves with allocating network access among all of their consumers. The "fair" allocation among all consumers, however, is not the concern of each individual consumer. Indeed, this is the fundamental joint-resource problem faced by the ISP.[66]

¶71 This stilted notion of fairness causes added confusion when raised in the wider public debates over "fair" use of bandwidth.[67] It conflates flow-fairness with the notion of "fairness" in the context of the economic free-rider problem that an ISP faces. Free-riding refers to when a person uses an "unfair" amount of a common good, whether by overuse or underpayment. Furthermore, the "fairness" reported by network engineering risks being misunderstood as the ever-controversial "fair share" that I am obligated to do if I benefit from others' cooperative action.[68]

¶72 The technical idea captured by the "fairness" is important—it describes how effectively the QOS policy is implemented. But, since it does not really touch on the human actors and does not evaluate the classifying criteria or QOS policy itself, it should not be understood to make the moral claim that "fair" might normally suggest.

¶73 To effectively implement a QOS policy, network engineers can select from a variety of algorithms to piece together the desired treatment. These algorithms are

---

wrong thing—flows; instead it should focus on the cost of user's actions on each other).

[66] From a strategic standpoint, the rhetoric of "fairness" puts ISPs in a tricky position. They will want to support it if it prompts development of a social norm for customers to be well-behaved. Then their customers have solved the ISP's joint-resource problem. But social norms are not so easily controlled as contractual terms. The prevailing "fairness" norm today may treat high-bandwidth P2P applications as "unfair" (perhaps because of presumed copyright infringement), but tomorrow some new high-bandwidth application might not have the same social stigma. This would force ISPs to instead fight against "fairness."

[67] *E.g.*, Iljitsch van Beijnum, *Growth of P2P Leads IETF to Debate "Fair" Bandwidth Use*, ARS TECHNICA, Dec. 5, 2007, http://arstechnica.com/news.ars/post/20071205-growth-of-p2p-leads-ietf-to-debate-fair-bandwidth-use.html (last visited Apr. 15 2010).

[68] JOHN RAWLS, A THEORY OF JUSTICE: ORIGINAL EDITION 112 (reprinted 1st ed. 2005) ("We are not to gain from the cooperative labors of others without doing our fair share.") (citing H. L. A. Hart, *Are There Any Natural Rights?*, 64 PHIL. REV.185 (1955)); *see also* Russell Hardin, *The Free Rider Problem*, STAN. ENCYCLOPEDIA OF PHIL., *available at* http://plato.stanford.edu/entries/free-rider/. When a journalist describes how P2P applications do not behave "fairly" it implies that they are taking advantage of some unstated generosity in violation of a broader "fair" use of the network. *See e.g.*, Beijnum, *supra* note 67. "Fairness" in this context conceptually glosses over the distinction between a product purchase and a group asset. A customer should not blame their neighbor for defects in a service they purchase. Their neighbor's use might be a but-for cause of their unsatisfactory Internet access, but it is the ISPs responsibility (not their neighbor's) to ensure Internet access. This mindset treats the purchased product as if it were part of a collective group (like corporate network users), but each consumer purchases Internet access from the ISP separately. A customer has no obligations to the other customers to preserve network resources. Consumers are not being "unfair" when they use what they have purchased.

sometimes grouped under labels: queuing, scheduling, shaping, dropping, etc. These labels are not equivalent (e.g. a dropped packet is never sent, whereas a "shaped" packet might be sent eventually), but they are all ways of describing the treatment that packets receive after they are classified. The fairness of a QOS implementation reflects the effectiveness of this arrangement of algorithms to implement the desired policy. But beware when analyzing a network's disclosed QOS policy; this sense of fairness is descriptive and should not be misunderstood as giving normative guidance.

### *B. External Interconnection*

¶74 In the preceding paragraphs, we discussed how to interpret a disclosed QOS policy; the QOS policy is effected within the network. We move now to the border of a network to discuss the disclosure requirement at the boundary of administrative control—the interconnections between separately administered networks.

¶75 As we discussed earlier, AS interconnections form the topology of the public Internet. The three methods we discussed for acquiring this information (traceroute, "Route Views", and the IRR database) reinforce each other, so if our disclosure can improve one, then the effect is amplified across all three.

¶76 We compare two ways to compel disclosure of this interconnection information to take advantage of these methods. The first is to require a network's accurate and timely participation in the distributed IRR database. Some networks already maintain IRR entries. However, as discussed previously, this data is often stale and inaccurate. The second way to compel the disclosure is to require networks to enable real-time (programmatic) access to their "Looking Glass" (LG) portal and to expose it to the public. As discussed previously, many networks already have an LG portal setup, yet they often limit the access and prohibit automated access.[69]

¶77 There are at least three reasons to prefer the first way (accurate and timely participation in IRR) over the second way (LG portal). First, the IRR provides all of the routing data in a single place making it easier to use. A person trying to use the data does not need to locate all the different network LG portals. Second, the IRR database is already set up to be distributed and mirrored, making it more reliable. This ensures that the data can be accessed, without relying on each network to keep their LG portal responsive. Third, maintaining an IRR entry is likely to be less costly for the network than providing an LG portal. A network's LG portal could be overwhelmed by queries whereas the IRR is duplicated and mirrored by third parties to ensure capacity (e.g., a heavy user could even create their own copy). Also, the IRR need only be updated when the network adds a new interconnection. The network will already have to reconfigure their routers to add the new interconnection, so requiring entry in the IRR adds only minimal extra work since the IRR is set up to enable this reconfiguration to be automated by registry updates.

¶78 Any interconnection disclosure will be amplified since all three methods of inferring interconnection reinforce and check each other. Compelling networks to

[69] *E.g.*, Sprint, Sprint Looking Glass, https://www.sprint.net/lg/ (last visited Apr. 15, 2010) ("Sprint's Looking Glass is NOT to be used with ANY automated scripts/applications unless expressly authorized by Sprint.").

maintain accurate entries in the IRR seems the most cost-effective way to reveal the technical details of their interconnections.

¶79 Finally, and perhaps most controversially, we would require the filing of all interconnection agreements of networks providing either Internet access or transmission to the public. The FCC could play a role in collecting and making public these documents. While such publication would undoubtedly hurt the bargaining of certain access providers, it is not clear that there would be any welfare loss. Further, such disclosure would provide a powerful curb against strategic behavior.

## V. CONCLUSION

¶80 The Comcast-BitTorrent Order took only tentative steps to unearth information for Internet policymaking. The forthcoming FCC initiative promises to create a more systematic mechanism for transparency. Our proposal advances this work with a specific and detailed disclosure regime to both deflect anticompetitive abuses on the Internet and reveal the openness of a network. The proposal harnesses the generative Internet to provide a new type of regulatory disclosure—one that is aimed neither directly at consumers nor at regulators—but instead seeks to provide the raw data to those who can aggregate, transform, and interpret the information needed to guide any regulatory policy or consumer choice. To see and know a neutral network, we need this network transparency.