KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

CDT RECOMMENDATIONS FOR EU NET NEUTRALITY POLICY

May 2013

This paper offers CDT's view concerning EU-level policy on net neutrality. Below, CDT:

- Explains that what is really at stake here is the ability of innovators and competitors to challenge today's Internet giants and bring Internet-focused growth to new companies and locations;
- Outlines why it is important to establish basic expectations concerning net neutrality now, rather than waiting until non-neutral practices have become more established and widespread; and
- Suggests key elements for a Commission Recommendation in this area, focused on creating a strong norm and expectation that Internet access services (as distinct from "specialized" or "managed" services) will be delivered on a fundamentally neutral basis.

I. What's Really at Stake

A non-neutral Internet would cement the position of today's Internet giants and undermine the ability of future upstarts in Europe or elsewhere to mount any serious challenge.

The Internet's open and neutral nature facilitates free expression, access to information, and consumer choice. These are all core principles that law and policy should aim to promote. At a practical level, however, it is probably in the area of competition and innovation that a shift away from net neutrality would be felt most immediately and directly.

New competitors and innovative upstarts benefit tremendously from the Internet's low barriers to entry. Once a company pays for its own Internet connection, it instantly gets access to the whole global network – a virtually infinite addressable market. Small providers of content, applications and services can compete directly for end users on a neutral technical playing field, regardless of identity of the users' ISPs.

By contrast, if the Internet were to move in a direction where each ISP may determine whether and how fast its subscribers can access particular content and services, upstarts would face a very different environment. The size of their addressable market would become much less certain. Every new service would have to worry about how its traffic will be treated by various ISPs. And inevitably, some application providers would seek to gain competitive advantage by striking deals with ISPs for favorable treatment. As deals with ISPs became commonplace, anyone who did not strike such deals might face significant competitive disadvantages.

The end result would be much higher barriers to entry. Being an effective online competitor would entail the complex task of negotiating deals with numerous ISPs. Many of those deals could require payment to the ISP, on an ISP-by-ISP basis.

Even for established and already profitable Internet giants, negotiating with and perhaps paying individual ISPs would be burdensome and costly. But if it were to become a competitive necessity to work out arrangements for (for example) prioritized carriage or special exemptions from bandwidth caps or usage-based pricing, at least the large players would have considerable resources and business clout to deploy in negotiations.

For would-be challengers, however, the added burden could prove much more serious, creating a significant barrier to entry and competition. They would either have to shoulder the new costs, or simply accept that their services will start out at a significant competitive disadvantage to their more established rivals.

Thus, a principal effect of a non-neutral Internet would be to cement the position of today's Internet giants. A less neutral Internet means that future upstarts and innovators across Europe would face increased barriers to any effort to chip away at the position of the established providers of Internet-based services. That would directly undercut the effort to develop a more robust, cutting-edge information technology sector in Europe. And it would undermine It would undermine the ability of EU Internet users to enjoy the fruits of a highly competitive and innovative marketplace in online applications and services.

II. Why Policymakers Should Establish Basic Expectations Now, Rather than Waiting

Transparency requirements are important, but not sufficient.

Transparency requirements can provide an important check on ISP traffic management practices. But they are not sufficient to ensure that the Internet remains open and nondiscriminatory. A recent survey by Consumer Focus in the U.K. found that consumers struggle to understand disclosures about traffic management.[1] And even with clear disclosures, consumers have no way to assess the practical impact of traffic management; if a particular website or application performs poorly, for example, a consumer cannot tell if the cause is ISP traffic management or some other problem (flaws in the consumer's computer, the website or application itself, etc).

Perhaps most important, transparency's usefulness as a safeguard depends on consumers' ability and willingness to switch ISPs. But switching ISPs, while possible, is too big a hassle for consumers to do lightly or frequently. For most consumers, traffic management would have to cause a direct and significant impact on a heavily used application or service before it would be a reason to seriously consider switching carriers. Practices that impair applications consumers have not yet come to embrace aren't likely to prompt those consumers to switch.

[1] *See* Consumer Focus, *Lost on the broadband super highway – Consumer understanding of information on traffic management*, 5 Dec. 2012, http://www.consumerfocus.org.uk/publications/lost-on-the-broadband-super-highway-consumer-understanding-of-information-on-traffic-management.

As a practical matter, therefore, transparency requirements may make it untenable for ISPs to engage in particularly egregious practices, such as blocking popular and well-established websites or applications. But for practices where the discrimination is more subtle, and for new and emerging websites and applications, the protections of transparency are likely much more limited.

Relying on "market forces" is not sufficient.

Market competition among ISPs is unlikely to fully address the "terminating monopoly" problem. Once a consumer has selected an ISP, other online companies and Internet users can reach that consumer *only* via the facilities of that ISP. From the perspective of an upstart trying to roll out new online content, applications, or services, the theoretical ability of consumers to change ISPs occasionally is nearly irrelevant. At any point in time, each ISP has an effective monopoly over the ability to reach its subscriber base – and upstarts trying to break through with a new online application have little realistic chance of convincing significant numbers of consumers to switch ISPs just to try their new product.

Market forces could address this "terminating monopoly" problem only if the marketplace pressure for neutrality and openness were so strong that ISPs all feel compelled to avoid discriminatory practices across-the-board. But BEREC's recent investigation indicates that application-specific practices, while not the norm in Europe, are certainly not uncommon: "BEREC found across Europe a wide array of traffic management practices resulting in restrictions." In particular, BEREC reported that 49 operators of fixed networks and 41 operators of mobile networks restrict peer-to-peer traffic, affecting at least 21 percent of fixed broadband users and 36 percent of mobile broadband users. At least 21 percent of mobile broadband users face restrictions on VOIP usage (and potentially significantly more, since the data was unclear with respect to an additional 18 percent of users). The number of users subjected to these restrictions, while a minority of the overall populace, is nonetheless huge: at least 30 million fixed and 63 million mobile users face technically enforced peer-to-peer restrictions, while at least 33 million mobile users face VOIP restrictions. BEREC reported instances of other, less common restrictions (for example, blocking or throttling specific applications or giving preferential treatment to specific types of over-the-top traffic) occur as well.[2]

Furthermore, BEREC has observed that "the investigation revealed a great diversity of experiences among national markets." For example, in nearly one-quarter of the national markets, the majority of the market share is held by ISPs that restrict peer-to-peer traffic for all users.[3]

---

[2] BEREC, *A view of traffic management and other practices resulting in restrictions to the open Internet in Europe,* BoR (12) 30, 29 May 2012, http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf ("BEREC traffic management report"), at 5, 8, 21, 23.

[3] BEREC, *Summary of BEREC positions on net neutrality,* BoR (12) 146, 3 Dec. 2012, http://berec.europa.eu/files/document_register_store/2012/12/BoR_(12)_146_Summary_of_BEREC_positions_on_net_neutrality2.pdf ("BEREC net neutrality summary") at 2; BEREC traffic management report, BoR (12) 30, at 26-27.

The conclusion to be drawn is that market forces may do a good job of limiting non-neutral ISP behavior in some locations and markets – but the effect is not universal. In some places, and for some types of services, market forces are no guarantee. Policy safeguards are needed to protect the Internet's neutral character in those areas where market forces alone may fall short. The fact that market forces may be sufficient sometimes, or perhaps even a majority of the time, is no reason to reject the adoption of safeguards for those cases when they are not.

A "wait-and-see" approach is risky and unrealistic.

Nobody can say for sure whether and to what extent harmful net neutrality problems will arise in the future. BEREC notes that "rapidly evolving practices make it credible – though not certain – that problems will arise more frequently in the future."[4] But failing to take policy precautions, and instead waiting to see if problems become more serious or widespread, would be risky and impractical.

First, a "wait-and-see" approach carries the risk that a number of innovators, competitors, and consumers may suffer substantial and preventable harms. Even if those harms eventually spur policymakers to act, damage will already have been done in those particular cases. (As discussed above, European consumers subject to application-specific restrictions number in the tens of millions today.)

Second, a "wait-and-see" approach fails to provide marketplace certainty. Without any clear safeguards against discrimination by ISPs, Internet-based upstarts face greater risks and may find it more difficult to attract financing. Policymakers and the public may never know what beneficial innovations or competitors failed to launch due to the uncertain environment.

Finally, it is impractical and unrealistic to think that policymakers can easily unravel a web of discriminatory deals and traffic management practices after they have become more firmly established. Once business plans have been implemented, investments have been made, and network equipment has been installed, changing course becomes much more difficult politically and logistically. For this reason, BEREC's conclusion that "application specific restrictions . . . are not widespread in Europe, except for some specific practices, mainly on mobile networks"[5] is actually a reason to establish clear guidelines now, rather than a reason to wait. Acting now, when non-neutral practices are the exception rather than the norm, would effectively just codify the status quo, with minimal little risk of disruption.

In short, setting some clear ground rules in advance, based on the nondiscriminatory model that is the majority practice today, would be far more efficient and effective than trying to reverse established "facts on the ground" at some future date. If the

[4] BEREC net neutrality summary, BoR (12) 146, at 10.

[5] BEREC, *Overview of BEREC's approach to net neutrality,* BoR (12) 140, 27 Nov. 2012, http://berec.europa.eu/files/document_register_store/2012/12/BoR_(12)_140_Overview+of+BEREC+approach+to+NN_2012.11.27.pdf ("BEREC net neutrality overview") at 2.

Commission wants to preserve core elements of the neutral Internet, it is better and more fair to everyone concerned to establish that expectation up front.

III. Key Elements for a Commission Recommendation

It is essential for the Commission to avoid issuing a weak or incomplete Recommendation that could be perceived as signaling growing tolerance for discriminatory practices by ISPs and a general retreat from core neutrality principles.

Active political attention on the issue of net neutrality may be a significant reason why application-specific discrimination has not become more widespread. With the Commission engaged in an active an ongoing policy inquiry over the past several years, many ISPs were likely well aware that any decision to adopt discriminatory practices could draw considerable negative attention and could provoke a policy backlash. The example of the Netherlands provides a smaller scale illustration of the risk: When telco KPN announced that it would start charging extra for using VoIP and a text messaging application, it caused a political storm that resulted in passage of the Netherlands' 2012 statute protecting net neutrality.

If the Commission is perceived as backing away from net neutrality, however, ISPs may conclude that the policy ground has shifted and the risks of non-neutral behavior are receding. Weak or equivocal guidance on net neutrality could be perceived as signaling increased tolerance for non-neutral behavior, effectively giving ISPs the "green light" to experiment with discriminatory practices. The likely result would be a gradual moves by ISPs to favor some traffic over others and a gradual erosion of the Internet's open character.

A Recommendation should clarify the crucial distinction between Internet access services and specialized services.

Numerous reports and analyses have emphasized the crucial distinction between nondiscriminatory, "best-efforts" Internet access service and other communications services that are "specialized" or "managed." The idea is that network operators may want to offer additional services that reflect different business models or technical architectures from the open and innovation-friendly Internet – but such services must create additional options to ordinary Internet access. As Ofcom has put it, the policy goal should be to "ensure that managed services continue to co-exist with 'best efforts' access to the open Internet."[6]

A Commission Recommendation should clearly articulate this distinction. In particular:

- The Commission could provide guidance on how the two services are different. ARCEP recently offered a useful description: "An Internet access service allows customers to send and receive data to and from the entire Internet" and "provides access to an array of applications," whereas "[u]nlike Internet access services,

[6] Ofcom, *Ofcom's approach to net neutrality*, 24 Nov. 2011, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf, at 27.

specialized services (or managed services) provide access to . . . a small selection of content or applications with a controlled quality."[7] Concrete examples might include a movie delivery service offering dedicated capacity for speedy online transmission of selected movies, or a quality-controlled video conferencing link between a company's branch offices.

Following this concept, the Commission could explain that specialized services must be truly specialized in the sense of serving a specific and limited purpose. A service that provides a general-purpose ability to send and receive data communications across the entire Internet should not be eligible for treatment as a specialized service.

- To avoid efforts to blur this important distinction, the Commission should make clear that specialized services may not be marketed as "Internet access" or anything confusingly similar. Nor should a service be treated as a "specialized service" if it is intended, marketed, or widely used as a substitute for Internet access service.

- The Commission should direct Member States to monitor specialized services closely for any sign that they are negatively affecting the provision of ordinary Internet access. As BEREC has suggested, "[s]pecialized services should be monitored for their potential to degrade [Internet access service], should they grow at the expense of (rather than alongside) the best effort Internet."[8] This is a risk to which Member States need to remain alert. (And where Member States find that regular Internet access has in fact been impaired, the Commission could encourage them to consider Universal Service Directive Article 22(3), empowering national regulators to set minimum quality of service standards, as a possible remedy.)

A Recommendation should establish the clear expectation that Internet access services must be provided in a neutral manner, without discrimination based on the content, applications, or services subscribers choose to access.

A Recommendation should make clear that for Internet access services, there is a general expectation that ISPs will not discriminate among lawful traffic based on its content, source, destination, ownership, application, or service. This is the core principle that prevents ISPs from "playing favorites" and ensures that the Internet can provide a level playing field for all speakers, competitors, and innovators. Reasonable traffic management is an exception to the nondiscrimination principle, as discussed below. But nondiscrimination should be established up front as the baseline expectation.

The Commission could further clarify as follows:

---

[7] ARCEP, *Report to Parliament and the Government on Net Neutrality (English Version)*, Sept. 2012, http://www.arcep.fr/uploads/tx_gspublication/rapport-parlement-net-neutrality-sept2012-ENG.pdf ("ARCEP Report") at 16.

[8] BEREC net neutrality summary, BoR (12) 146, at 3.

- This basic nondiscrimination principle should bar not only blocking, but any type of discrimination in the way ISPs transmit lawful traffic.

- The principle should not bar, however, ISP policies and actions that focus on the overall volume or usage patterns of particular users' data communications, without regard to what those communications contain. For example, it is not discriminatory to charge extra or even throttle the bandwidth of users who have exceeded a transparently disclosed usage cap.

- Nor should the principle bar ISPs from enabling individual subscribers to designate certain traffic for prioritization, blocking, or other special treatment. Allowing users to make choices about their own Internet traffic does not undermine the open Internet and does not constitute discrimination.

A Recommendation should establish principles for evaluating traffic management practices, based on the criteria suggested by BEREC.

There is widespread recognition that determining which traffic management practices are reasonable and beneficial, and which give ISPs an undue amount of leverage and "gatekeeper" control, is in many ways the crux of the net neutrality debate. Guidance on this question would therefore be particularly useful.

CDT does not believe the Commission should attempt to specify which particular technical practices should be prohibited or allowed. Detailed technical choices are best left to the ISPs, since they are in the best position to understand the technical consequences and tradeoffs associated with different choices. ISPs also need appropriate flexibility to devise new tactics and respond to new threats.

The Commission could and should, however, establish some general principles for evaluating which traffic management tactics are appropriate and which are not. These could be based on the criteria set out by BEREC. BEREC suggests that traffic management should be non-discriminatory between players; efficient and proportional; application agnostic; and provide end-user control where possible.[9] Other analyses have been generally consistent with BEREC's. For example, the European Economic and Social Committee has suggested that traffic management should "comply with the general principles of relevance, proportionality, efficiency, non-discrimination between parties, and transparency."[10] ARCEP has recommended that ISP traffic management mechanisms should "comply with the general principles of relevance, proportionality, efficiency, non-discrimination between parties and transparency."[11]

---

[9] *See* BEREC net neutrality summary, BoR (12) 146, at 6.

[10] *Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: The open Internet and net neutrality in Europe'*, COM(2011) 222 *final* (2012/C 24/31), 26 Oct. 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:024:0139:0145:EN:PDF, at 7.12(iii).

[11] ARCEP Report at 74.

CDT would note that under these principles, traffic management is not automatically considered reasonable any time the ISP has a valid purpose. A big part of the goal of net neutrality policies is to push ISPs to address their valid traffic management goals using mechanisms that minimize any negative impact on the open character of the Internet. Thus, reasonableness cannot turn solely on the ISP's intent.

CDT would put particular emphasis on the idea that wherever possible, traffic management practices should be content- and application-agnostic. This is the most reliable way to ensure that traffic management is applied fairly and evenly, and that the ISP is not selecting which specific content or applications to favor or disfavor. For congestion management in particular, ISPs should use objective, application-agnostic criteria such as volume of bandwidth usage. A key test for reasonableness would be: does this practice have equal impact on all applications with comparable bandwidth usage characteristics? (Of course, this principle would not apply to some instances of security-related traffic management, which may require ISPs to discriminate against known malicious content.)

CDT would also recommend that reasonable traffic management practices should, wherever possible, comply with the common technical standards on which the Internet is based. Application developers rely on and design technology with the expectation that applications built to use and respond to these technical standards will function the same way across the entire Internet. Traffic management tactics that depart from key standards risk increasing instability across the Internet, causing applications and services to behave in unexpected ways and complicating the task facing innovators.

A Recommendation should make clear that neutrality principles are not limited to fixed Internet access services, but apply to mobile Internet access as well.

The Commission should specify that net neutrality principles should not depend on whether Internet service is delivered by fixed or mobile means. Providers of mobile Internet access should not be exempt.

First, BEREC's survey of current practices concluded that discriminatory practices, such as blocking of VoIP, are more prevalent today on mobile networks.[12] It would be strange indeed for net neutrality principles to fail to apply to the very setting where the problems appear most common.

More generally, as network capacities and device capabilities increase, people are increasingly using mobile Internet access in much the same ways as their fixed connections. In a converging world where mobile wireless connectivity is expected to make Internet access increasingly ubiquitous, failing to address mobile would leave a gaping hole in any policy meant to promote openness and nondiscrimination on the Internet. The move towards mobile access need not and should not come at the expense of the Internet's openness.

[12] BEREC net neutrality summary, BoR (12) 146, at 2.

Mobile carriers may face some special technical challenges, relating to such factors as spectrum limitations and radio interference. Given these technical realities, what constitutes reasonable traffic management on a mobile data network may differ from the norm on fixed connections. But there is no reason to think that mobile ISPs need to discriminate among traffic based on content-related factors such as its source, ownership, application, or service. Core neutrality principles can and should apply.

A Recommendation should specify that neutrality principles apply specifically and exclusively to the provision of Internet access services, and not to over-the-top or other services.

The idea of net neutrality is to preserve the Internet as a neutral and non-discriminatory transmission medium. It reflects the simple premise that *carriers providing connections to the network* should not limit choices or play favorites. Thus, net neutrality applies specifically and exclusively to providers of Internet access service – and not to the almost limitless array of content, services, and applications that may be accessed over the Internet.

Trying to extend the concept net neutrality to over-the-top services or computer software or hardware would invite dangerous overbreadth and quickly raise a host of problems. A core purpose of net neutrality is to permit innovation and choice at the Internet's endpoints. This produces a smorgasbord of services and applications, many of which are not non-discriminatory in any sense of the term; rather, they reflect the particular preferences or idiosyncratic tastes of their creators and users. Extending neutrality requirements to over-the-top services and applications would undercut the very choice and innovation that an open Internet is intended to facilitate.

To be sure, some over-the-top services may come to present legitimate questions regarding market power or anticompetitive conduct. Where that happens, competition or consumer protection laws may apply. But net neutrality policy cannot provide an all-purpose safeguard across the entire Internet ecosystem; to be effective, it needs to be tailored to the specific risk for which it was designed. A Commission Recommendation could make this clear.

The Commission could emphasize that Member States will have flexibility regarding what mechanisms to use to safeguard the Internet's neutral character – so long as they establish neutral treatment of content, applications, and services as a clear norm and expectation for the provision of Internet access service.

The Commission could specify that Member States will have flexibility to determine how to implement net neutrality principles at the national level. As an illustration of different approaches, the Netherlands and Slovenia have already chosen to adopt legislation, while Norway established nonbinding guidelines to be followed up by annual stakeholder meetings to assess their status. Other mechanisms may be possible, so long as they successfully establish the clear norm and expectation that Internet access services (as distinct from specialized services) will be delivered on a fundamentally neutral basis. The guiding principles, however, should be set forth by the Commission in order to

ensure a reasonable level of harmonization and consistency in the way Internet access operates across the EU..

At the same time, in issuing a Recommendation at this time, the Commission should make clear that it would be prepared to put forward legislation on net neutrality in the future if the measures and policies of some Member States fail in practice to protect the ability of their citizens to "access and distribute information or run applications and services of their choice."[13] Likewise, the Commission should indicate that it would pursue further action if its Recommendation on net neutrality fails to achieve generally consistent policy outcomes across the Single Market. The availability of open and neutral Internet access, on which users and not ISPs select which content and applications to use, should not depend upon the particular EU Member State from which an Internet user seeks access.

About the Center for Democracy & Technology

The Center for Democracy & Technology is a non-profit public interest organization working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, CDT seeks to enhance free expression and privacy in communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

For more information, please contact:

Jens-Henrik Jeppesen, Representative and Director for European Affairs, jjeppesen@cdt.org
David Sohn, General Counsel, dsohn@cdt.org
Andrew McDiarmid, Senior Policy Analyst, amcdiarmid@cdt.org

[13] Framework Directive, 2002/21/EC, Art. 8.4(g).