Grove, Nico; Agic, Damir; Sedlmeir, Joachim

Conference Paper

Network neutrality and consumer discrimination: Comparing ISP's GTCs and DPI application

23rd European Regional Conference of the International Telecommunications Society (ITS), Vienna, Austria, 1st-4th July, 2012

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Grove, Nico; Agic, Damir; Sedlmeir, Joachim (2012) : Network neutrality and consumer discrimination: Comparing ISP's GTCs and DPI application, 23rd European Regional Conference of the International Telecommunications Society (ITS), Vienna, Austria, 1st-4th July, 2012, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/60403

Network Neutrality and Consumer Discrimination: Comparing ISP's GTCs and DPI Application

Nico Grove[1], Damir Agic[2], Joachim Sedlmeir[3]

ABSTRACT

Network neutrality and alleged discriminatory practices on the part of ISPs regarding the transmission of Internet data packets has been the subject of notable scholarly discussion and appears to be a widespread phenomenon. However, it is noteworthy that actual consumer discrimination has only been proven in a small number of individual case studies. Hence, we aim to provide solid evidence for discriminatory behaviour of ISPS in our in-depth study. This lack of overwhelming evidence is not, as we assume, the result of an absence of discriminatory behaviour - on the contrary it may be whittled down to a number of grounds: the absence of studies comparing services offered by ISPs, the existence of high switching costs between operators accruing to consumers, and a lack of awareness on the part of consumer of the putative discriminatory measures, given the information asymmetry between ISP and consumers, where the consumer is not in a position, being able to distinguish between an impaired quality of service and potential discrimination behaviour by the ISP.

The paper at hand examines ISPs' traffic management measures and determines whether such practices breach the ISP's contract with the consumer. Relying on an examination of services provided by European ISPs (France, Germany and Italy) we can conclude that data traffic is subject to "discriminatory management". Our investigative model is based on M-Lab data (Glasnost Test) and related processing algorithms provided by "The Network is Aware" project. In order to corroborate our findings that ISPs are breaching their own contractual service agreements, the results regarding discriminatory measures are compared with the contractual General Terms and Conditions (GTC) as agreed between the ISPs and consumers.

Results of the study conducted provide evidence that major ISPs in the countries examined deployed DPI (Deep Packet Inspection) mechanisms for the given time period in order to discriminate P2P BitTorrent applications. Many ISPs that have admitted to blocking and restricting particular services and applications claim they did so only during the hours of peak load, when their networks are congested. By contrast, we conclude that this behaviour occurs continuously, irrespective of the time of the day, and that therefore ISPs were guilty of violating their own GTCs in some cases.

[1] Assistant Professor at the Infrastructure Economics & Management, Bauhaus-University Weimar

[2] PhD Researcher at the Infrastructure Economics & Management, Bauhaus-University Weimar

[3] PhD Researcher at the Institute for Information, Organization and Management, Ludwig-Maximilians- University Munich

For policy makers, this provides evidence for potential regulatory interventions in order to counteract discriminatory restrictions on consumer data traffic and the need for higher transparency for end consumer Internet services. Furthermore, the study proves that solely relying on inter-provider competition to self-regulate does not work out, as it fails to impede discrimination due to a lack of transparency (information asymmetry) and high switching costs.

KEYWORDS: Network neutrality, regulation, General Terms and Conditions, telecommunications, user discrimination.

JEL Codes: D22, D63, G13, I38, K23, L86

This research is partially funded by a google research grant.

1. INTRODUCTION

The issue of network neutrality has gained high attention in the past several years becoming a global phenomenon. Initially, it was deemed solely a matter for network operators and content producers. However, the alleged discrimination in data transmission has led to heated debates on "network neutrality" being placed on the international political agenda. The fundamental idea behind network neutrality is that Internet Service Providers (ISP)[1] are obliged – by national regulatory authorities – to treat all data in a similar fashion i.e. to transfer all data packages across the internet equally, according to the manner in which it is received. However, the Internet as an open platform and the generator of innovative ideas, value creation and promoter of freedom of speech might have been adversely affected by the above mentioned network operators - not adhering to principles of open internet - responsible for the provision of internet access to end-users[2]. Hence, the proponents of network neutrality have emphasised a range of potential detriment to consumers, thus arguing for additional regulatory intervention.

Given that there is a continuous flow of emerging innovations in applications and services, there is a great need to ensure faster and more precise data transmission. Bearing this in mind, facilities-based operators are faced with a trade-off between the increasing demand for infrastructure investments and the rising costs of its provision. Hence, opponents of network neutrality argue that network operators should be allowed to introduce different pricing schemes in order to recoup investments made in the networks. Otherwise, they argue, governmental intervention i.e. the presence of price regulation might diminish incentives to invest into additional capacity and innovation.

Technical progress enables new mechanisms for traffic management, as for instance, Deep Packet Inspections (DPI), Quality of Service (QoS), or Packet Shaping. Therewith, ISPs are able to prioritize between different data flows, supporting applications that are time-sensitive (e.g. Voice over Internet Protocol – VoIP), or those that require high-bandwidth (e.g. video) or even a higher level of security (e.g. e-commerce). On the other hand, using these new technologies, the operators are able to charge different prices for different types of information transported via their networks, differentiate between QoS for different applications (two-lane model), or even block or discriminate certain applications and content from their networks, hence, putting the principles of network neutrality under severe pressure.

While there have been some prominent cases of network neutrality violations in USA, there exists thus far no (significant) evidence that operators in Europe are engaging in unfair discrimination in a way that harms consumers or competition.[3] In light of this, the aim of this paper is to investigate whether certain ISPs are using new technology – here the focus lies on DPIs - in a consumer harmful manner, thus prioritizing, discriminating and blocking particular services and applications. The paper at hand also determines whether such practices breach the ISP's contract with the consumer. In order to answer this question, a cross-provider analysis is applied. In addition, the paper provides comprehensive results for Italian, French and German ISPs, examining data for the period January 2009 – January 2012. To gain relevant information and data sets necessary to conduct this analysis, Measurement Lab (M-Lab), an open, distributed server platform that was launched by Google in 2009, is utilised. For the processing of the data, an approach developed by "The Network is Aware" project is used.[4] The Glasnost Test has been developed to detect blocking or throttling of BitTorrent and other peer to peer (P2P)[5] applications.[6] For the purpose of the specific analysis, the tool *Glasnost* and the processing of corresponding data provided by M-Lab is used primarily. Thereby, a data-set of major variables of internet performance is established to evaluate possible significant differences in the internet performance among the end-users considering different ISPs and services. The output will, hence, give major insights into the interplay between the end-users´ internet performance and specific access providers and shed light on the various practices ISPs apply to data traffic processed via their networks. Furthermore, in order to underline our findings that ISPs are breaching their own contractual service obligations, the results regarding discriminatory measures are compared with the contractual General Terms and Conditions (GTC) as agreed between the ISPs and their clients.

The paper is structured as follows. The introduction was given in section 1. Section 2 provides a brief introduction into the field of network neutrality before focusing on the potential discriminatory practices network operators might engage in. Furthermore, this section provides insights into various forms of network discrimination which affect both end-users and application and content providers (both are paying fees for having internet access). Section 3 introduces the methodological framework used to

measure consumer discrimination amongst ISPs. In order to answer the question whether certain ISPs are utilising new technologies in a consumer harmful manner, thereby (unfairly) prioritising, discriminating and blocking particular services and applications (in this case BitTorrent), a cross-provider analysis is applied. The results are then compared with the GTCs as agreed between the consumers and the ISPs at consideration. Using this framework, the most common discriminatory practices are then analysed in the context of the European (German, French and Italian) access providers with a special emphasis on contractual obligations of the ISPs towards their customers as stipulated in the GTCs. Finally section 4 contains conclusions and comments on further research.

We would like to express our deepest appreciation to "The Network is Aware" research team at Syracuse University School of Information Studies and Delft University of Technology led by Professor Milton Mueller for providing us with relevant data and methodological assistance.

2. THEORETICAL FRAMEWORK

This section gives an overview of the theoretical framework of topics of network neutrality and network discrimination upon which this analytical framework is based. For the sake of brevity, the paper refers to fundamentals according to Grove/Agic, 2012 and will not discuss in detail the concept network neutrality and the recent developments in the broadband market.[7] The primary focus of this section is on the main cases of discrimination of the openness of the internet considering the conditions under which a network provider might have an incentive to discriminate against a specific application or content.

2.1 What is Network Neutrality?

Before continuing with the main consideration in this section, namely defining network discrimination and exploring technical and economical motivations for discrimination as well as interspersing this with some practical examples, the fundamentals of network neutrality are introduced briefly.

The Internet´s original edifice was (and is argued to continue in this vein by e.g. van Schewick, 2010) constructed on the core principles of freedom of opinion and innovation.[8] As a general-purpose technology, the Internet (though it does not create value through its existence only) has enabled and fostered the creation of a phenomenal number of new applications and services, and has given users infinite access to all

kind of data and information.[9] It is no exaggeration to point out that internet-based communication, information retrieval, online entertainment or internet-based collaboration, have become an essential part of our daily life. This trend, known as digitization and convergence, has made the internet a sort of public good that has to be considered by public policymakers.[10]

Even though network neutrality has many facets – and subsequently several definitions of the term are in current use [11] – the fundamental idea behind network neutrality is that Internet Service Providers (ISP) shall be obliged – by national regulatory authorities – to treat all data in a similar fashion i.e. to transfer all data packages across the internet equally, according to order in which it is received.[12] However, the Internet as an open platform and enabler of innovative ideas, value creation and promoter of freedom of speech has been adversely affected by the network operators responsible for the provision of internet access to end-users.[13] Hence, the proponents of network neutrality have emphasized a range of possible detriment to consumers arguing for increased regulatory intervention.[14] At this juncture, it should be stressed that this issue is not only linked to the traditional text and audiovisual content, but also to services such as search engines (such as e.g. Yahoo, Google, and Bing) and VoIP (such as e.g. Skype and Viber).[15] By limiting the users' ability to use the network connection according to their personal preferences, network operators significantly might reduce the usefulness and the value of the Internet for the users connected. Hence, reducing incentives to innovate in the form of new applications and services, according to van Schewick, will inevitably lead to a decrease in Internet´s contribution to economic growth and will also threaten the Internet´s ability to realize its social, political and cultural potentials.[16]

Given that there is a continuous flow of emerging innovations in applications and services, there is a great need to ensure faster and more precise data transmission. Bearing this in mind, facilities-based operators are faced with a trade-off between the increasing demand for infrastructure investments and the rising costs of its provision. Thus, opponents of network neutrality argue that network operators should be allowed to introduce different pricing schemes in order to recoup investments made in their networks. Otherwise, governmental intervention i.e. the presence of price regulation will reduce incentives to invest and innovate.[17]

In respect to enormous technical advances, for instance, with Deep Packet Inspections (DPI), Quality of Service (QoS), or Packet Shaping, ISPs are able to prioritize between different data flows and, hence, charge different prices for different types and quality of information (QoS) carried over their networks (so called two-lane model), or even block or ban certain applications and content from their networks, hence, jeopardizing the principle of network neutrality.[18]

The following section deals with different forms of discrimination network operators are allegedly deploying towards end-users, considering various incentives to discriminate against some applications and also technical instruments which facilitate such discriminatory behavior. At this point it is necessary to stress that not all forms of discrimination are considered user-unfriendly and/or harmful. In order to enable a solid and fair network traffic management whilst treating all packages and data in an application and technology neutral form, network operators are allowed (and even encouraged) to freely engage in application-agnostic ways of managing congestion and, hence, prioritise (if necessary) amongst different packages and data streams. By fairly allocating bandwidth amongst users in application-agnostic ways, network providers might be better off, letting the users determine how to use their "share" of bandwidth.

2.2 Defining Network Discrimination

In the context of net neutrality, it is of crucial importance to understand both technical and economic motivations for discrimination, the various kinds of discrimination and how they actually are applied in practice. Even though network discrimination could constitute (and very often does) a remedy to solve the ever-present problems of data congestion (i.e. by prioritising between packets and discarding low-priority packets first, but only when absolutely necessary), some other incentives lie behind the actual use of discriminatory practices.

Due to the massive increase in internet usage and its infrastructure in all spheres of human activities, the unfettered and open use of the internet could be regarded as a public good.[19] Hence a regulated access by public authorities might be inevitable in order to ensure a non-discriminatory use of the merit good Internet and to guarantee the fundamentals of all social and economic benefits facilitated by an open Internet.[20] However, Next Generation Networks (NGN) offer a great variety of modern instruments (Deep Packet Inspections, Quality of Service or Packet Shaping, just to mention a few) for inspecting and also influencing the quality level and the content of data packages and, thus, for discrimination between them.[21] Both fixed and mobile providers have claimed that increased internet traffic has resulted in "ballooning" costs for networks.[22] In order to manage the ever-growing amounts of data transmitted over their networks and to preserve sound network traffic, ISPs see those tools as necessary. Nevertheless, to deploy this new potential in a non-discriminatory manner – for managing data traffic and preventing possible congestion only - transparent information regarding the handling of services and content is required.[23] On the other hand, some end-users might demand price differentiation between data packages in order to enjoy a better quality of specific services and hence would be willing to pay for that additional service. So according to Picot: "*From a regulatory standpoint QoS offerings by means of NGN are acceptable in principle, but should only be allowed with a basic service free of any discrimination and with transparent information about all business conditions involved regarding special treatment of selected services".*[24]

Generally speaking, the three main cases of network discrimination can be distinguished:[25]

1. **Data traffic (applications and services) being blocked –** this form of discrimination usually applies to vertically integrated network providers. The motivation to discriminate is primarily due to economic reasons. In order to maximize profits, network operators are willing to exclude certain services and applications of competing market players. The most prominent case regarding this form of network discrimination consists of European mobile network operators (e.g. Deutsche Telekom AG) blocking or restricting Skype and other VoIP services for users on their network.[26] Considering the fact that Skype, for instance, is a service that normally consumes a small amount of bandwidth, it is obvious that discriminatory behavior was not based on any real need of traffic management or Quality of Service issues.

2. **Data traffic is being slowed down –** Discrimination does not only happen by blocking (which means dropping) packets. Access providers could also artificially slow down (quality degradation of data transmission) or prioritize specific services and applications according to their own preferences, hence causing extra delays for packets in passing through the network, referred to technically as "jitter." The level of jitter affects some applications more than others. When e.g. browsing the World Wide Web, modest jitter will cause, at worst, a slight delay in downloading pages. On the other hand, VoIP applications rely on steady streaming of interactive and real-time communication and thus suffer heavily from increased jitter.[27] As stated above, providers are arguing that this practice is necessary in situations, when they have to manage high capacity utilization of their networks. Nevertheless, this form of discrimination gives providers room for charging different rates for specific applications and services. This behavior bears the risk of unjustified discrimination of specific content, application and services.[28]

3. **Unwanted content is discriminated or blocked –** The third discriminatory behavior by network operators can be characterized as dealing with manipulation and blocking of content. Here, some examples of internet access providers having blocked specific websites for providing controversial and critical content of the network operator itself have been found. A prominent example is the German ISP freenet, which has blocked several websites for criticizing freenet´s business activities.[29]

The most prominent cases of discriminatory behavior of the European network operators have been reported in the past several years provoking a tremendous amount of public discourse over the necessity of explicit network neutrality regulation in Europe (similar to USA).[30] Under heavy public pressure, access providers were

forced to retract their previous discriminatory practices as was the case with ISPs blocking VoIP services, and to deploy new tools (DPI, QoS, Packet Shaping etc.) for reasonable network traffic management reasons only.[31] Hence, there is, nowadays, no significant evidence that network operators are engaging in unfair discrimination in a way that harms consumers or competition. However, having these instruments for inspecting the quality and content of data packages and also having indisputable incentives (both economic and technological) to use them, there might always exist a potential that operators would deploy the above mentioned tools in an unfriendly and harmful manner.[32] In addition, the massive growing increase in Internet traffic caused by an even greater deployment of current and new services (inter alia cloud computing, app economy, e-energy, BitTorrent) is augmenting the cost of transit for ISPs, many of which are offering flat-rate tariffs with unlimited Internet access to their customers. Hence, it should not surprise that an ISP might be eager to implement strategies to reduce the amount of network traffic produced by the users connected.[33] Following this logic, the next section examines the analytical (methodological) framework which is applied in order to investigate whether certain ISPs are (still) using new technology (in this case DPIs) in a consumer unfriendly manner, thus prioritizing, discriminating and blocking particular services and applications (BitTorrent).

3. ANALYTICAL FRAMEWORK - A CROSS-PROVIDER ANALYSIS[34]

This chapter at hand introduces the methodological framework used to explore consumer discrimination amongst ISPs. In order to answer the question whether certain ISPs are using new technology (most of all DPIs) in a consumer harmful manner, thus prioritizing, discriminating and blocking particular services and applications (in this case BitTorrent), a cross-provider analysis is applied. The results are then compared with the GTCs as agreed between the consumers and the ISPs at consideration. Using this framework, the most known discriminatory practices are then analyzed in the context of the European (German, French and Italian) access providers.

3.1 Data and methodological framework

As the debate over network neutrality violations continues apace, the “normal” Internet users are more or less uninformed about their own internet performance,[35] even though being directly affected.[36] In order to enable users to detect whether they are subject to traffic and network discrimination several tools have been developed with the aim of making any discriminatory behaviour of network operators transparent to users. Therefore, a cross-provider analysis is applied in order to provide more insight

into network management activities of European ISPs with a special emphasis on DPI deployment.

The results presented in this section are based on M-Lab data (Glasnost Test) and processing algorithms by “The Network is Aware" project. For an in-depth analysis of the Glasnost Test see Appendix.[37] Furthermore, In order to answer the question, whether such practices breach the ISP’s contract with the consumer – in other words, whether customers are being adequately informed about the very same actions – the results considering discriminatory practices are compared with the General Terms and Conditions (GTC) as agreed between the ISPs (in the case at hand, Kabel Deutschland, Free (Iliad) and FastWeb) and their clients.

3.2 Preliminary results

3.2.1. DPI deployment by European ISPs

The results of the cross-provider analysis considering German, Italian and French (fixed-line) ISPs are presented in Tables 1, 2 and 3 respectively. The column on the far right shows the percentage of times Glasnost tests indicated that the ISP was manipulating BitTorrent using DPI. As stated before, the test generates a false positive of up to 10% for the time before August 2009 and of 4-5% thereafter. That means that for some ISPs not using DPIs in order to deliberately throttle or block BitTorrent at all, the test might show some positive results. Furthermore, the number of valid tests (third column from the left) is of significant relevance in order to gain reliable results in the last column – the more valid tests conducted, the more reliable results will be gathered. For instance, ISPs for whom only 11-30 tests per quarter (only 1-2 tests per week) have been gathered will be highly variable and thus less reliable than ISPs for whom there are >450 tests per quarter. For that reason the analysis additionally does not show results for ISPs with less than 10 results per quarter (reducing false positives to below 10 per cent).

The results presented in Tables 1, 2 and 3 clearly show that almost all ISPs in the selected countries deployed DPIs for the given time period in order to block BitTorrent applications. The data shows that the largest cable operator in Germany, Kabel Deutschland, is blocking P2P applications in large amounts – 69% of the tests have been blocked by Kabel Deutschland in the first quarter of 2011 (see Table 1). There is a similar situation in Italy and France with tests showing high percentages of blocked BitTorrent applications by some large ISPs – 42% of the tests have shown DPI deployment by FastWeb[38] in the second quarter of 2009 and 65% by Opitel[39] in the first quarter of 2009 in Italy (see Table 2) and 13% by Iliad[40] in France in the fourth quarter of 2009 (see Table 3).

Even though the results show unambiguous discriminatory conduct of ISPs in Germany, Italy and France towards P2P applications, there is also a clear trend of significant reduction in blocked BitTorrent tests. Figures 1, 2 and 3 illustrate the change in the percentage of blocked BitTorrent applications between January 2009 and January 2012 for Kabel Deutschland, FastWeb, Opitel and Iliad. The graphs show that ISPs are abruptly changing their BitTorrent blocking policies mostly beginning in the first quarter of 2009. There is a high likelihood that this is related to the case of Comcast, the largest cable operator in the United States. In 2008, Comcast´s BitTorrent blocking behavior has been revealed to the public causing massive critical media coverage towards Comcast. Eventually Comcast was fined by the Federal Communications Commission (FCC) forcing the ISP to change its network management policies.[41] Such course of action – if proven – might attract negative publicity and, hence, severely damage the ISP´s reputation.

Despite the fact that there is a trend to significantly reduce blocked BitTorrent tests, we still conclude that, for instance, Kabel Deutschland exhibited a high amount of blocked P2P applications in the first quarter of 2012 – 37%. From the data collated, it cannot be claimed conclusively whether blocking of BitTorrent by ISPs was, as a matter of fact, the result of reasonable network management activities – to ensure unwanted data traffic – or were the ISPs using DPI tools in order to deliberately discriminate BitTorrent traffic even in times of low network traffic. Many ISPs that have admitted to blocking BitTorrent flows claim that they do so only during peak load hours, when their networks are congested. In other words, they regard DPIs (and other instruments for network discrimination) as a remedy to solve the ever-present problems of data congestion and hence prioritize between packets and discard low-priority packets first, but only when that is absolutely necessary. However, Dischinger et al. (2008) have come to the conclusion – using a special designed toolset, called BTTest, which similar to Glasnost test enables end users to test whether their ISP is blocking BitTorrent – that BitTorrent flows are being blocked independent of the time of the day or the day of the week assuming that discriminating against P2P file sharing protocols is not the result of reasonable network management policies by ISPs.[42]

3.2.2. Comparing ISP's GTCs and DPI Application

As indicated by our preliminary results, the deployment of discriminatory measures by the ISPs in terms of blocking data traffic appears to be a widespread phenomenon although declining in frequency. In order to answer the question, whether such practices breach the ISP's contract with the consumer – in other words, whether customers are being adequately informed about the very same actions – the results regarding discriminatory measures are compared with the contractual General Terms and Conditions (GTC) as agreed between the ISPs (in the case at hand, Kabel Deutschland, Free (Iliad) and FastWeb) and their clients. Hence, the analysis focuses on the following three dimensions: (1) availability of service, (2) obligations of the customers and (3) contractual agreements based on GTCs concerning the blocking of services

by ISPs. Table 4 provides a tabular comparison of the analysed GTCs regarding the aforementioned three dimensions.

Our results demonstrate that across the board there is a high amount of similarities in the contractual terms regarding the average availability of Internet service (at least 97%, no data available for FastWeb). The contractual obligations of the customers are also almost identical amongst the analysed ISPs. Typical examples for such contractual duties are the provision of correct (personal) information, compliance with current legislation (e.g. prohibition of spamming, hacking, creating or spreading viruses etc.) and agreeing to fulfil the contractual (in particular financial) obligations.

The most common reasons listed for ISPs needing to block services ISPs relate to the maintenance of the network and customer breaching the contract. However, no information about the employment of DPI or the prioritising of own services at the expense of third party offerings is provided.

As a result, no significant evidence of contractual transparency regarding the employment of DPI and similar traffic management tools and the respective blocking or throttling of applications and services by the ISPs could be found. Despite contractual assurances regarding Internet availability the study demonstrates that the ISPs in question are not informing their customers of their traffic management practices, hence, infringing their contractual duties towards the end-users.

4. SUMMARY AND CONCLUSION

Previously published reports of access ISPs blocking BitTorrent have sparked an international debate on network neutrality. In this context, this paper makes some important contributions. The paper presents results from a large-scale measurement study that is based on a widely-used public Glasnost test. Our results show that almost all ISPs in the selected countries (Germany, Italy and France) deployed DPIs for the given time period in order to block BitTorrent applications. Moreover, the results exhibit that some very large ISPs are blocking P2P applications in tremendous amounts. Nevertheless, there is also a clear trend that ISPs are abruptly changing their BitTorrent blocking policies mostly due to bad publicity and the fear of jeopardizing their reputation if such behavior would be revealed. However, we still conclude that, for instance, Kabel Deutschland has blocked a high amount of tested P2P applications in the first quarter of 2012. Nevertheless, as this analysis will be developed more extensively as we progress and examine more data, we are endeavoring to investigate the further trends of this development and gain more insights into ISPs current DPI policies. From our data it cannot be decisively claimed whether blocking of BitTorrent by ISPs was, as a matter of fact, the result of reasonable network management activities or were the ISPs using DPI tools in order to deliberately discriminate BitTorrent traffic even in times of low network traffic.

Furthermore, by analysing GTCs of three well-established European Internet access providers, we found no significant evidence of contractual transparency regarding the

employment of DPI and similar traffic management tools and the respective blocking or throttling of applications and services by the ISPs leading to a conclusion that end-users are not well informed about network management activities of the ISPs

The current study is limited to detecting BitTorrent blocking, and there are a number of challenges that still must be overcome, representing interesting research areas for future work. As a next step, a development of analysis techniques for detecting other types of traffic manipulation beyond blocking, e.g., BitTorrent traffic shaping seems to be promising. Moreover, to gain a more comprehensive understanding whether ISPs are using new technology (not only DPIs) in a consumer unfriendly manner, further tests and the respective datasets might be included/flow into the analysis (e.g. ShaperProbe, NDT, Netalyzer). Also, some very important technical parameters like Ping, jitter, Latency should play a significant part in order to fully investigate whether ISPs are performing application-specific network discrimination. Moreover, GTCs of a number of additional European ISPs will be explored in more detail in order to support our preliminary statement that ISPs in Germany, France and Italy do not inform their clients about their common network management practices.

For regulators, this study provides evidence for the fact, that the existence of inter-provider competition does not hinder customer discrimination. This is not only the fact due to switching costs for the consumer between operators. It is moreover linked to the fact that the consumer might not even be aware of discriminatory measures, as he is not able to distinguish between the quality of the service or a potential discrimination by the ISP.

REFERENCES

Aggarwal, V., Feldmann, A. and Karrer, R. P. (2007): *An Internet Coordinate System to Enable Collaboration between ISPs and P2P Systems*. Proceedings of the 11th International ICIN Conference. Deutsche Telekom Laboratories / TU Berlin.

Bendrath, R. and Mueller, M. (2011): *The end of the net as we know it? Deep packet inspection and internet governance.* New Media Society. Thousand Oaks, CA: Sage.

BEREC (Body of European Regulators for Electronic Communications) (2010): *Response to the European Commission´s consultation on the open Internet and net neutrality in Europe*. BoR (10) 42.

Bullinger, G. M. (2010): *Aktueller Begriff Netzneutralität*. Wissenschaftliche Dienste. Nr. 014/10. Berlin: Deutscher Bundestag.

Cave, M. and Crocioni, P. (2011): *Net neutrality in Europe.* Communications & Convergence Review 2011, Vol. 3, No. 1, pp. 57-70.

Chirico, F., Van der Haar, I. and Larouhe, P. (2007): *Network Neutrality in the EU*. TILEC Discussion Paper No. 2007-030.

Comcast (2008): *Description of planned network management practices to be deployed following the termination of current practices.* Attachment B. Philadelphia: Comcast.

Dischinger, M., Mislove, A., Haeberlen, A. and Gummadi, K. P. (2008): *Detecting BitTorrent blocking.* Vouliagmeni: Internet Measurement Conference.

Dischinger, M. et al. (2010): *Glasnost: Enabling End Users to Detect Traffic Differentiation*. San Jose, CA: USENIX Symposium on Networked Systems Design and Implementation (NSDI).

Federal Communications Commission (FCC) (2008): *Comments of Comcast Corporation before the Federal Communications Commission.* WC Docket No. 07-52. Washington, DC: FCC.

Felten, E. W. (2006): *Nuts and Bolts of Network Neutrality.* Center for Information Technology Policy Department of Computer Science and Woodrow Wilson School of Public and International Affairs Princeton University.

Grove, N. and Agic, D. (2012): *Network Neutrality: A Cross-Provider Analysis*. Proceedings of the 12th Pacific Telecommunications Council, 2012.

Holznagel, B., Picot, A., Deckers, S., Grove, N. and Schramm, M. (2010a): *Strategies for Rural Broadband: An economic and legal feasibility analysis. 1. Edition, Wiesbaden: Gabler.*

Holznagel, B., Picot, A. and Grove, N. (2010b): *Submission to the European Commission addressing the questionnaire: For Public Consultation on the Open Internet and Net Neutrality in Europe*. Brussels: European Commission.

Kocsis, V. and de Bijl, P. W. J (2010): *Network neutrality and the nature of competition between network operators.* Journal of International Economics and Economic Policy 2010, Vol. 4, No. 2, pp. 159-184.

Kroes, N. (2010): *Net neutrality in Europe.* Address at the ARCEP Conference. Speech/10/153. Paris, 13th April 2010.

Larabie, C. L. (2010): *Net Neutrality and the Public Interest: A Comparative Analysis of Canada, the UK, Australia and Japan.* Graduate Major Research Papers and Multimedia Projects. Paper 7.

Lehr, W. H., Gillett, S. E., Sirbu, M. A. and Peham J. M. (2006): *Scenarios for the Network Neutrality Arms Race.* Presented at the 34th Research Conference on Com-

munication, Information and Internet Policy (TPRC). September 29-October 1, 2006. Arlington, VA.

Marcus, S.J., Nooren, P. Cave, J. and Carter, K. R. (2011): *Network Neutrality: Challenges and responses in the EU and in the U.S.* Brussels: European Parliament.

Marcus, S.J. and Monti, A. (2011): *Network operators andcontent providers: Who bears the cost?* Final Report. Analytical study for submission to Google. Bad Honnef: WIK-Consult.

Marsden, C. T. (2010): *Net Neutrality. Towards a Co-regulatory Solution*. New York: Bloomsbury Academic.

Mueller, M. (2011): *DPI Technology from the standpoint of Internet governance studies: An introduction.* Syracuse University School of Information Studies.

Ofcom (2010): *Traffic Management and 'net neutrality'*. A Discussion Document. London: Ofcom.

Picot, A. and Cave, M. (2008): *Workshop Next ("Now") Generation Access (NGA): How to Adapt the Electronic Communications Framework to Foster Investment and Promote Competition for the Benefit of Consumers? Summary, Briefing Notes and Presentations.* Brussels: European Parliament.

van Schewick, B. and Farber, D. (2009): *Point/Counterpoint. Network Neutrality Nuances. A discussion of divergent paths to unrestricted access of content and applications via the internet.* Communications of the ACM February 2009, Vol. 52, No. 2, pp. 31-37.

van Schewick, B. (2007): *Towards an Economic Framework for Network Neutrality Regulation*. Journal on Telecommunications and High Technology Law, Vol. 5, pp. 329-391.

van Schewick, B. (2010a): *Internet Architecture and Innovation.* Cambridge: MIT Press.

van Schewick, B. (2010b): *Network Neutrality: What A Non-Discrimination Rule Should Look Like*. Stanford Public Law Working Paper No. 1684677. Stanford Law and Economics Olin Working Paper No. 402.

Williamson, B., Black, D., Punton, T. (2011): *The open internet – a platform for growth*. A report for the BBC, Blinkbox, Channel 4, Skype and Yahoo. London: Plum Consulting.

Internet

FastWeb (2011): *Resoconto Sulle Rilevazioni di Qualità dei Servizi Internet*: - *Offerte FAMIGLIA*, http://www.fastweb.it/downloads/PDF/famiglia/qualita_servizi_Internet_primo_semestre_2011_delibera.pdf, June 06, 2012.

FastWeb (2012a): *Condizioni Generali di Contratto Offerta Fissa – Offerte FAMIGLIA*, http://www.fastweb.it/downloads/PDF/famiglia/cgc_fissa_res.pdf, June 06, 2012.

FastWeb (2012b): *Condizioni Generali di Contratto Offerta Home Pack – Offerte FAMIGLIA*, http://www.fastweb.it/downloads/PDF/famiglia/CGC_homepack.pdf, June 06, 2012.

FastWeb (2012c): *Carta dei Servizi Telefonia Fissa – Offerte FAMIGLIA*, http://www.fastweb.it/downloads/PDF/famiglia/CDS_fissa.pdf, June 06, 2012.

FastWeb (2012d): *Condizioni Generali di Contratto Offerta Fissa – Offerte PARTITA IVA*, http://www.fastweb.it/downloads/PDF/business/qualita_carta_servizi/cgc_fissa_shp.pdf, June 06, 2012.

FastWeb (2012e): *Condizioni Generali di Contratto Vendita Apparati – Offerte PARTITA IVA*, http://www.fastweb.it/downloads/PDF/business/qualita_carta_servizi/cgc_prodotti_shp.pdf, June 06, 2012.

FastWeb (2012f): *Carta dei Servizi Telefonia Fissa – Offerte PARTITA IVA*, http://www.fastweb.it/downloads/PDF/business/qualita_carta_servizi/carta_servizi_tel_fissa_shp.pdf, June 06, 2012.

Free (2011): *Conditions Générales de Vente des Offres Free Haut Debit Applicables Á Compter Du 9 Septembre 2011*, https://adsl.free.fr/cgv/last/cgv.html, June 6, 2012.

Kabel Deutschland (2012): *Internet und Telefon - Allgemeine Geschäftsbedingungen Internetanschlüsse*, http://www.kabeldeutschland.de/static/media/AGB_Internet_Telefon.pdf, June 06, 2012.

Table 1: BitTorrent Throttling by ISPs, Germany, Glasnost data, Q1 2009 – Q1 2012

Operator Name	Quarter	Number Of Valid Tests	Range of Valid Tests	Pct of Tests Showing DPI
Deutsche Telekom	2009Q1	163	151 450	4%
Kabel Deutschland	2009Q1	106	91-150	59%
Telefonica O2 Germany	2009Q1	103	91-150	1%
Unitymedia	2009Q1	16	11-30	0%
Vodafone Germany	2009Q1	59	31-60	2%
Deutsche Telekom	2009Q2	174	151-450	5%
Kabel Deutschland	2009Q2	268	151-450	58%
Telefonica O2 Germany	2009Q2	136	91-150	4%
Unitymedia	2009Q2	18	11-30	11%
Vodafone Germany	2009Q2	68	61-90	7%
Deutsche Telekom	2009Q3	171	151-450	4%
Kabel Deutschland	2009Q3	489	>450	50%
Telefonica O2 Germany	2009Q3	113	91-150	4%
Unitymedia	2009Q3	55	31-60	2%
Vodafone Germany	2009Q3	65	61-90	2%
Deutsche Telekom	2009Q4	204	151-450	4%
Kabel Deutschland	2009Q4	242	151-450	40%
Telefonica O2 Germany	2009Q4	146	91-150	6%
Unitymedia	2009Q4	26	11-30	8%
Vodafone Germany	2009Q4	108	91-150	6%
Deutsche Telekom	2010Q1	174	151-450	6%
Kabel Deutschland	2010Q1	164	151-450	35%
Telefonica O2 Germany	2010Q1	117	91 150	8%
Unitymedia	2010Q1	31	31-60	3%
Vodafone Germany	2010Q1	91	91-150	7%
Deutsche Telekom	2010Q2	94	91-150	6%
Kabel Deutschland	2010Q2	179	151-450	40%
Telefonica O2 Germany	2010Q2	75	61-90	4%
Unitymedia	2010Q2	14	11263	7%
Vodafone Germany	2010Q2	56	31-60	5%
Deutsche Telekom	2010Q3	32	31-60	3%
Kabel Deutschland	2010Q3	111	91-150	32%
Telefonica O2 Germany	2010Q3	11	11-30	0%
Vodafone Germany	2010Q3	12	11-30	0%
Deutsche Telekom	2010Q4	21	11-30	10%
Kabel Deutschland	2010Q4	40	31-60	33%
Telefonica O2 Germany	2010Q4	17	11-30	0%
Deutsche Telekom	2011Q1	14	11-30	0%
Kabel Deutschland	2011Q1	32	31-60	69%
Telefonica O2 Germany	2011Q1	13	11-30	0%
Vodafone Germany	2011Q1	15	11-30	0%
Deutsche Telekom	2011Q2	11	11-30	0%
Kabel Deutschland	2011Q2	11	11-30	45%
Kabel Deutschland	2011Q3	12	11-30	8%
Telefonica O2 Germany	2011Q3	10	11-30	0%
Deutsche Telekom	2011Q4	10	11-30	0%
Kabel Deutschland	2011Q4	26	11-30	15%
Telefonica O2 Germany	2011Q4	20	11-30	0%
Deutsche Telekom	2012Q1	19	11-30	5%
Kabel Deutschland	2012Q1	38	31-60	37%
Telefonica O2 Germany	2012Q1	39	31-60	8%

Source: Own illustration based on M-Lab Data (http://deeppacket.info)

Table 2: BitTorrent Throttling by ISPs, Italy, Glasnost data, Q1 2009 – Q1 2012

Operator Name	Quarter	Number Of Valid Tests	Range of Valid Tests	Pct of Tests Showing DPI
Fastweb	2009Q1	252	151-450	32%
H3G	2009Q1	45	31-60	7%
NGI	2009Q1	52	31-60	33%
Opitel	2009Q1	382	151-450	65%
Telecom Italia	2009Q1	1045	>450	4%
Tiscali	2009Q1	254	151-450	17%
Vodafone	2009Q1	93	91-150	10%
Wind	2009Q1	442	151-450	3%
Fastweb	2009Q2	226	151-450	42%
H3G	2009Q2	53	31-60	13%
NGI	2009Q2	136	91-150	25%
Opitel	2009Q2	326	151-450	60%
Telecom Italia	2009Q2	990	>450	5%
Tiscali	2009Q2	200	151-450	9%
Vodafone	2009Q2	101	91-150	3%
Wind	2009Q2	360	151-450	3%
Fastweb	2009Q3	101	91-150	31%
H3G	2009Q3	64	61-90	8%
NGI	2009Q3	34	31-60	12%
Opitel	2009Q3	193	151-450	46%
Telecom Italia	2009Q3	519	>450	5%
Tiscali	2009Q3	95	91-150	6%
Vodafone	2009Q3	45	31-60	9%
Wind	2009Q3	222	151-450	4%
Fastweb	2009Q4	188	151-450	9%
H3G	2009Q4	91	91-150	16%
NGI	2009Q4	73	61-90	68%
Opitel	2009Q4	325	151-450	50%
Telecom Italia	2009Q4	829	>450	8%
Tiscali	2009Q4	185	151-450	25%
Vodafone	2009Q4	107	91-150	15%
Wind	2009Q4	347	151-450	10%
Fastweb	2010Q1	142	91-150	10%
H3G	2010Q1	96	91-150	9%
NGI	2010Q1	31	31-60	74%
Opitel	2010Q1	263	151-450	51%
Telecom Italia	2010Q1	854	>450	8%
Tiscali	2010Q1	169	151-450	22%
Vodafone	2010Q1	107	91-150	17%
Wind	2010Q1	413	151-450	14%
Fastweb	2010Q2	53	31-60	8%
H3G	2010Q2	17	11-30	6%
Opitel	2010Q2	30	31-60	40%
Telecom Italia	2010Q2	362	151-450	7%
Tiscali	2010Q2	42	31-60	14%
Vodafone	2010Q2	56	31-60	16%
Wind	2010Q2	138	91-150	8%
Fastweb	2010Q3	11	11-30	9%
H3G	2010Q3	20	11-30	0%
Opitel	2010Q3	22	11-30	27%
Telecom Italia	2010Q3	108	91-150	5%
Tiscali	2010Q3	19	11-30	5%
Vodafone	2010Q3	12	11-30	0%
Wind	2010Q3	57	31-60	4%
Fastweb	2010Q4	26	11-30	19%
H3G	2010Q4	13	11-30	15%
Opitel	2010Q4	31	31-60	35%
Telecom Italia	2010Q4	136	91-150	4%
Tiscali	2010Q4	38	31-60	21%
Vodafone	2010Q4	18	11-30	6%
Wind	2010Q4	66	61-90	3%
Fastweb	2011Q1	38	31-60	3%
Opitel	2011Q1	20	11-30	25%
Telecom Italia	2011Q1	149	91-150	10%
Tiscali	2011Q1	49	31-60	12%
Vodafone	2011Q1	15	11-30	0%
Wind	2011Q1	74	61-90	7%
Fastweb	2011Q2	11	11-30	0%
Telecom Italia	2011Q2	67	61-90	3%
Tiscali	2011Q2	15	11-30	33%
Wind	2011Q2	25	11-30	4%
Telecom Italia	2011Q3	22	11-30	5%
Tiscali	2011Q3	13	11-30	8%
Wind	2011Q3	16	11-30	0%
Telecom Italia	2011Q4	12	11-30	8%
Wind	2011Q4	11	11-30	18%
Telecom Italia	2012Q1	42	31-60	10%
Tiscali	2012Q1	13	11-30	8%
Wind	2012Q1	29	11-30	0%

Source: Own illustration based on M-Lab Data (http://deeppacket.info)

Table 3: BitTorrent Throttling by ISPs, France, Glasnost data, Q2 2008 – Q2 2010

Operator Name	Quarter	Number Of Valid Tests	Range of Valid Tests	Pct of Tests Showing DPI
France Telecom	2009Q1	142	91-150	3%
Iliad	2009Q1	227	151-450	8%
Numericable-Completel	2009Q1	48	31-60	2%
SFR	2009Q1	69	61-90	6%
France Telecom	2009Q2	300	151-450	4%
Iliad	2009Q2	306	151-450	11%
Numericable-Completel	2009Q2	76	61-90	4%
SFR	2009Q2	167	151-450	3%
France Telecom	2009Q3	173	151-450	5%
Iliad	2009Q3	136	91-150	9%
Numericable-Completel	2009Q3	34	31-60	3%
SFR	2009Q3	77	61-90	1%
France Telecom	2009Q4	188	151-450	12%
Iliad	2009Q4	210	151-450	13%
Numericable-Completel	2009Q4	67	61-90	4%
SFR	2009Q4	88	61-90	8%
France Telecom	2010Q1	171	151-450	8%
Iliad	2010Q1	149	91-150	4%
Numericable-Completel	2010Q1	46	31-60	7%
SFR	2010Q1	102	91-150	7%
France Telecom	2010Q2	71	61-90	3%
Iliad	2010Q2	75	61-90	11%
Numericable-Completel	2010Q2	26	11-30	4%
SFR	2010Q2	50	31-60	12%
France Telecom	2010Q3	42	31-60	5%
Iliad	2010Q3	41	31-60	7%
Numericable-Completel	2010Q3	10	11-30	10%
SFR	2010Q3	27	11-30	7%
France Telecom	2010Q4	18	11-30	6%
Iliad	2010Q4	19	11-30	0%
France Telecom	2011Q2	10	11-30	0%
Iliad	2011Q2	38	31-60	3%
Numericable-Completel	2011Q2	10	11-30	0%
SFR	2011Q2	12	11-30	8%
France Telecom	2011Q3	11	11-30	0%
SFR	2011Q3	10	11-30	10%
France Telecom	2011Q4	17	11-30	0%
Iliad	2011Q4	34	31-60	6%
France Telecom	2012Q1	25	11-30	0%
Iliad	2012Q1	35	31-60	3%

Source: Own illustration based on M-Lab Data (http://deeppacket.info)

Table 4: Tabular comparison of GTC-statements of three European telecommunications companies regarding the dimensions: Country, Availability, Customer Commitments and Blocking of Services by ISP

ISP	Country	Availability	Customer Commitments	Blocking of Services by ISP
Kabel Deutschland	Germany	>= 98%	Following activities are prohibited: ➔ Spamming ➔ Counterfeiting of sender information or other header information ➔ Collecting of information without the permission of the proprietor ➔ Accessing and scanning of an operating system and/or a network as well as the unauthorised monitoring of data streams without the permission of the proprietor ➔ Utilising a third party´s mail server for sending messages without the permission of the proprietor ➔ Proliferation of viruses, worms, Trojan horses etc. ➔ Installing software on a computer other than the contractually agreed one ➔ Developing and proliferating software copies ➔ Completely or partially modifying, adjusting, translating, leasing, distributing software or using it as a basis for similar products ➔ Distributing authorisation codes for the installation of software, subscription number and registration keys ➔ Gaining unauthorised third parties access to devices provided by KD	➔ if necessary due to public security reasons, statutory provisions, reliability of network operation, maintenance of network integrity, data security or due to necessary operational or technical works ➔ if customer culpably violates his obligations in a repeated and severe manner after being unsuccessfully warned by setting a deadline

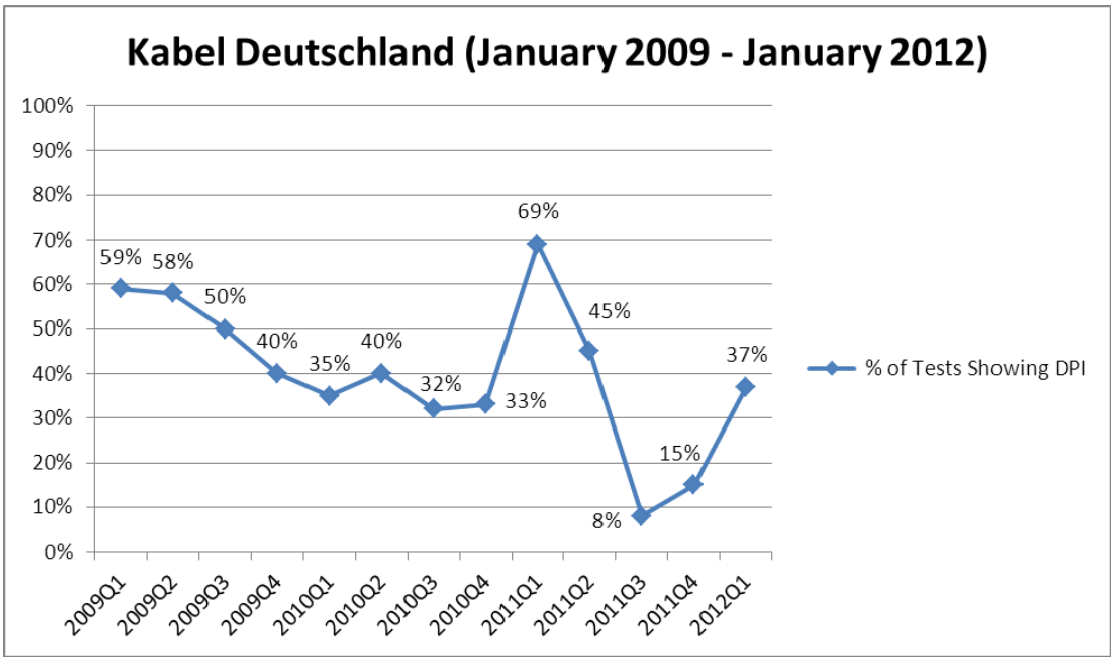
ISP	Country	Availability	Customer Commitments	Blocking of Services by ISP
Free (Iliad)	France	>= 97% for telephone services >= 99% for e-mail (sending and receiving) >= 98% for displaying and updating homepages	<u>Customer is obliged to:</u> ➔ Provide accurate personal information ➔ Maintain the connection to the local loop ➔ Ensure compatibility of the equipment ➔ Comply with all the requirements for the installation and use of the network element ➔ Fulfil his financial obligations vis-à-vis Free ➔ Comply with current legislation: • Data traffic should not violate national and international laws and regulations • Content should not induce crime and offenses, racial or any other discrimination, suicide and should not contain elements of child pornography • Subscriber shall not infringe the rights of third parties (intellectual property rights) • Subscriber agrees not to use services for purposes of infringement (piracy), download files in an unlawful manner or make available protected files (music or video files), make intrusions into computer systems (hacking), spread viruses or programs intended to harm, spamming ➔ Use decent and respectful language ➔ Not to misuse devices and services at his disposal (Gaining unauthorised third parties access to devices provided by Free)	➔ Free is obliged to provide access to services according to standards and contractual specifications 24/7 ➔ For reasons of maintenance or updating, Free may suspend access to all or part of the services for a consecutive period of 24h ➔ In case of a complete interruption of services for a continuous period exceeding 48h and upon the request of the subscriber, Free agrees to refund the subscriber for the fees corresponding to the last calendar month for which the service was to be provided ➔ In order to significantly improve network throughput and increase the capacity of the network, the subscriber authorises Free to use the available capacity and bandwidth of his/her line (this should have no impact on the subscriber´s Internet performance and will not cause interference on his/her line) ➔ Free is not held responsible for any delays or failure caused by force majeure or unforeseeable circumstances

ISP	Country	Availability	Customer Commitments	Blocking of Services by ISP
FastWeb	Italy	--	Customer is obliged to: ➔ Provide accurate personal information ➔ Accept limitations and restrictions regarding the access to the ADSL-service as listed in the offer ➔ Acknowledge that statements in the GTC relating to the speed of Internet-access have to be understood with reservation until technical assessments will be done ➔ Ensure compatibility of the equipment ➔ Not to misuse devices and services at his disposal (gaining unauthorized third parties access to devices provided by FastWeb) ➔ Agree that FastWeb is able to update the Internet access automatically for quality improvements ➔ Accept interventions in the network for service improvements ➔ Acknowledge that the speed of the services depends on specific technical and functional characteristics of the web-access ➔ Accept that services are provided only for non-commercial purposes ➔ Comply with current legislation and the rights of any third party: • Data traffic should not violate relevant laws and regulations • Content should not contain obscene, aspersive or any other Illegal elements • Subscriber shall not infringe the rights of third	➔ If customer culpably violates his contractual obligations in a repeated and severe manner after being unsuccessfully warned by setting a deadline ➔ If necessary due to technical problems, reliability of network operation, unplanned maintenance of network infrastructure ➔ In the case of planned maintenance work, FastWeb has to inform the customers at least 5 days before realization ➔ If the amount of consumption is regarded as "abnormal". As a protective measure, FastWeb is able to block the access or services after informing the concerning customers ➔ FastWeb is not held responsible for any delays, failure or other technical problems caused by unpredictable circumstances or manipulations ➔ FastWeb assumes no responsibility for any delays and/or inefficiencies that are assigned to services or actions of third-party providers ➔ FastWeb is entitled to carry out interventions in services on customer request ➔ FastWeb is not liable for any problems caused by the discontinuity between different networks

	parties (intellectual property rights) • Subscriber agrees not to use services for purposes of infringement (piracy), download files in an unlawful manner or make available protected files (text, music or video files), spread viruses or programs intended to harm, spamming ➔ Accept changes in the contract conditions after being informed by FastWeb	

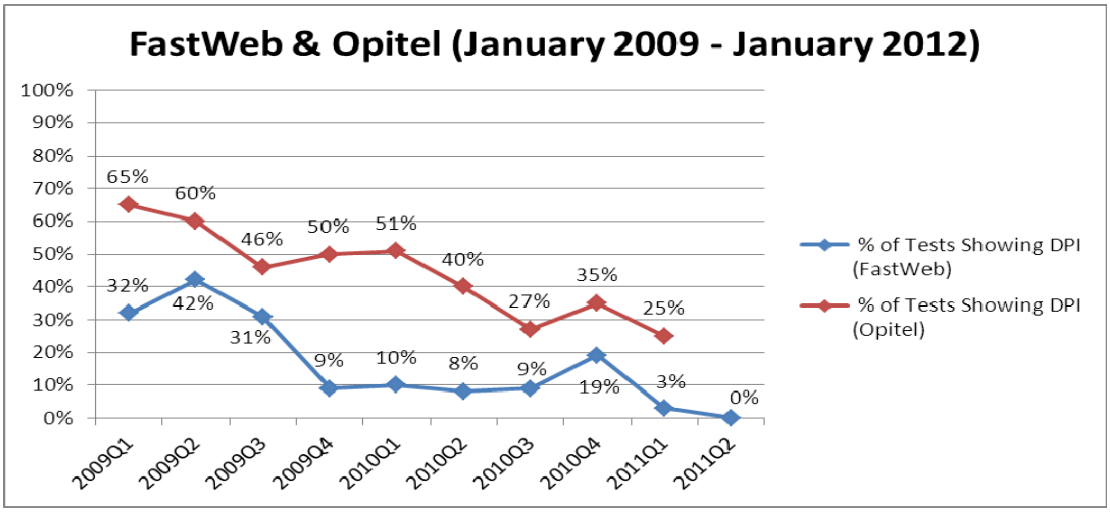
Source: Own illustration based on General Terms and Conditions of Kabel Deutschland, Free (Iliad) and FastWeb[43]

Figure 1: Percentage of blocked BitTorrent connections changed between January 2009 and January 2012, Kabel Deutschland, Germany



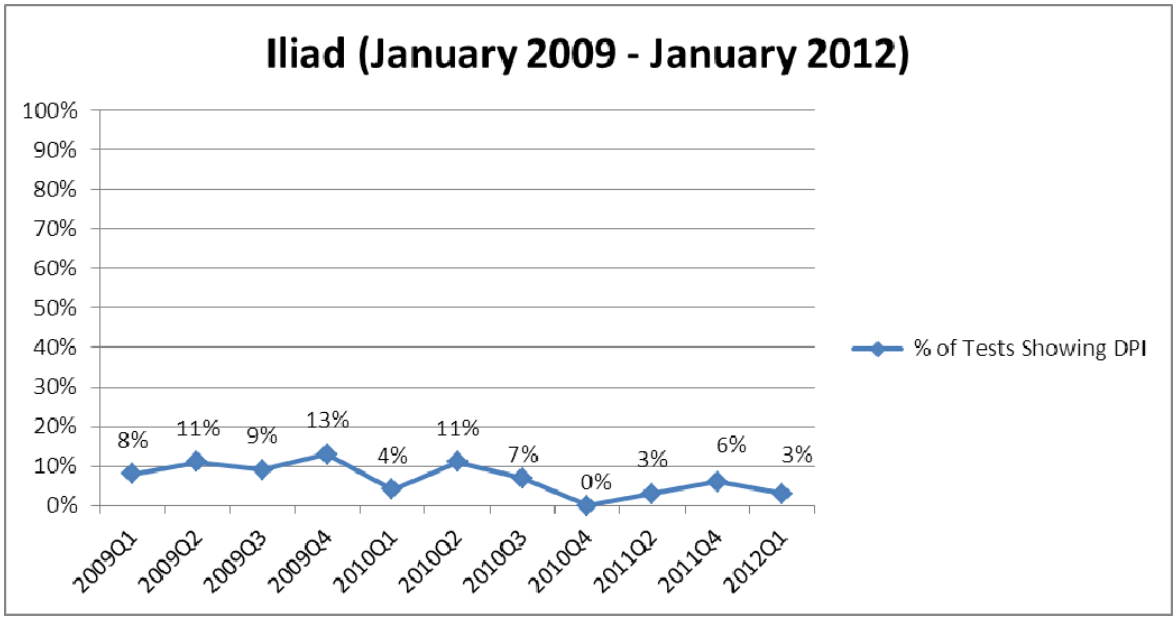
Source: Own illustration based on results from Figure 2

Figure 2: Percentage of blocked BitTorrent connections changed between January 2009 and January 2012, FastWeb and Opitel, Italy



Source: Own illustration based on results from Figure 3

Figure 3: Percentage of blocked BitTorrent connections changed between January 2009 and January 2012, Iliad, France



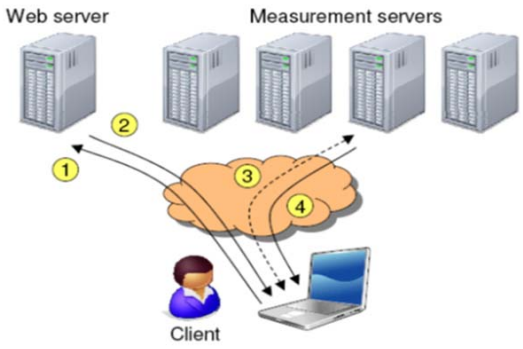
Source: Own illustration based on results from Figure 4

Appendix

Glasnost Test

M-Lab – launched by Google in 2009 – offers several internet measurement tools which can help users to measure the speed of their connection, run diagnostics and identify if their ISP is blocking or throttling particular applications. In particular, this analysis primarily focuses on Glasnost Test. The goal of this internet performance tool is to make access networks, such as residential cable, DSL, and cellular broadband networks, more transparent to their customers. Glasnost attempts to detect whether an Internet access provider is performing application-specific traffic shaping. Currently, internet users can test if their ISP is throttling or blocking email, HTTP or SSH transfer, Flash video, and P2P apps including BitTorrent, eMule and Gnutella. Thus, using the Glasnost test an Internet user can discover whether BitTorrent[44] is completely blocked, throttled (running slowly) or running normally (no interference). After contacting the Glasnost Web server the client receives the address of a measurement server (see items 1 and 2 in Figure 1), which allows him/her to load a java applet and subsequently run the test – applet starts to emulate a sequence of flows. The measurement server records the user's IP address, and all data packets received by the server from his/her computer or sent by the server to the computer. In addition, it monitors errors in the communication with the server and the throughput of the transfers for those communication "flows," and sends them to the server (see items 3 and 4 in Figure 4).[45]

Figure 4: The Glasnost System[46]



All the M-Lab raw data (ca. 25 TByte of data) are organized into tarballs, where each tarball contains all the data (measurements) collected during one hour, by one tool running on one M-Lab server. The same counts for Glasnost test. Furthermore, the Glasnost test collects data beginning in April 2008 and continues to the present time. However, the results are based upon data for the period January 2009 – January 2012. Nevertheless, this analysis will be developed more extensively in cooperation with "The Network is Aware" project led by Syracuse University School of Information

Studies and Delft University of Technology, as more data has been processed and examined. In addition, the analysis concentrates primarily on Italian, French and German ISPs. In the following a brief description of the data format upon which the analysis at stake is based is provided. Each line of the dataset contains:[47]

asn, yearmo, nobtm, btm_port, btm_protocol, inconclusive
where:

- ***nobtm***: number of tests (run from that ASN in that month), that are indicative of no BitTorrent manipulation (throttling or blocking) in place.
- ***btm_port***: number of tests that are indicative of BitTorrent traffic manipulation. The traffic was identified by port numbers.
- ***btm_protocol***: number of tests that are indicative of BitTorrent traffic manipulation. The traffic was identified by actual BitTorrent protocol headers.
- ***inconclusive***: number of tests for which any verdicts cannot be made.

It is, however, important to mention, that the Glasnost test produces a false positive of up to 10% prior to August 2009, and around 5% after that.[48] In other words, there is a certain possibility for an ISP who might not throttle BitTorrent to have a positive test result of 8-10% (before August 2009) or 4-5% (after August 2009). Regarding traffic discrimination, a false positive means that a certain ISP is falsely accused of engaging in discriminatory acts (in this case of throttling and/or blocking BitTorrent) so that the user would experience traffic differentiation, which might not be the case.[49]

This, furthermore, means that results for ISPs with only a small number of valid tests may vary significantly. For example, if there are only 2 tests a month and one is a false positive, the rate would be 50%. Hence, the more tests that are run from a certain ISP, the more stable and accurate the results become for that ISP. For that reason we recommend that results for ISPs with less than 30 valid tests per quarter are not being used, reducing the overall false positive to below 10 per cent.

ENDNOTES:

[1] In our analysis, we treat companies with their own infrastructure (network owners) and Internet Service Providers that use this infrastructure equally referring to them as network operators.
[2] End-users are the users of applications and services and can be consumers and producers as well; both are paying fees for having internet access.
[3] Nevertheless, there have been some notable cases of network neutrality infringements in Europe which will be discussed later on in this paper.
[4] "The Network is Aware" project is led by Syracuse University School of Information Studies and Delft University of Technology. You can find more information about that project at http://deeppacket.info.
[5] It is important to stress that p2p applications are not referring exclusively to BitTorrent and similar "copyright-infringing" services. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads among peers. P2P concept is used by a numerous of different applications: beside content distribution such as BitTorrent, Kazaa or Gnutella, Skype and other VoIP services, Zattoo (an Internet Protocol Television system), cloud computing or even YouTube, MySpace and many more can be stated as peer-to-peer systems. See Aggarwal et al., (2007). p. 1.
[6] The Glasnost test was recently expanded to other protocols such as Flash videos, Email, HTTP, SSH etc.
[7] For a detailed overview of recent developments in broadband with a special emphasis on the debate over network neutrality, including its technological and economic underpinnings, the implications for business models going forward, and the legal, regulatory, policy and business responses that have been attempted and that are currently in play, see Marcus, et al., (2011). See also Grove & Agic, (2012).
[8] See van Schewick, (2010b). p. 1.
[9] See Holznagel et al., (2010b). p. 2. See also Picot & Cave, (2008). p. 25.
[10] See Picot & Cave, (2008). p. 25.
[11] For a detailed discussion of the many definitions and concepts of net neutrality, see Marcus, et al., (2011).
[12] See Holznagel et al., (2010b). p. 2. See also van Schewick, (2007). p. 331ff. For a detailed discussion on various definitions of the term "net neutrality", see Larabie, (2010). p. 3ff.
[13] See van Schewick, (2007). p. 331-332. See also Kocsis & de Bijl, (2010). p. 160.
[14] See van Schewick, (2007). p. 331-332.
[15] See Marcus, et al., (2011). p. 18.
[16] See van Schewick, (2010a). p. 10.
[17] See van Schewick, (2007). p. 332. See also Kocsis & de Bijl, (2010). p. 162.
[18] For a detailed analysis of these techniques, see Marcus, et al., (2011). For a comprehensive analysis of DPI tools, see Mueller, (2011).
[19] See Picot & Cave, (2008). p. 25.
[20] See Holznagel et al. (2010a).
[21] See Picot & Cave, (2008). p. 25.
[22] However, a report, written by telecoms experts Plum Consulting, claims the cost of delivering additional gigabytes of data have been wildly exaggerated by the ISPs, being around €0.01-0.03 per GB. See Williamson et al., (2011). p. 17-18.
[23] See Chirico, et al., (2007). p. 26.
[24] Picot & Cave, (2008). p. 26.
[25] See Holznagel et al., (2010b). p. 4.
[26] There are clear instances of mobile network operators (e.g. Deutsche Telekom) blocking or charging extra prices for rivalry VoIP services (e.g. Skype) over their respective networks in order to promote their own VoIP product. See Marcus, et al., (2011). p. 57.
[27] See Felten, (2006). p. 4.
[28] See Holznagel et al., (2010b). p. 4.
[29] See Holznagel et al., (2010b). p. 4.
[30] BEREC has reported cases of 1) blocking, or charging extra for VoIP services in mobile networks by certain mobile operators in Austria, Croatia, Germany, Italy, the Netherlands, Portugal and Romania; and 2) blocking or throttling

of P2P file-sharing or video streaming in France, Greece, Hungary, Lithuania, Poland and the United Kingdom. See BEREC, (2010). p. 3. See also Marcus, et al., (2011). p. 56.

[31] See Dischinger et al., (2010). p. 4-5.

[32] For a detailed discussion of both economic and technological incentives ISPs might have to engage in discriminatory activities, see van Schewick, (2010a).

[33] See Dischinger et al., (2008). p. 1.

[34] The Glasnost data have been analyzed by "The Network is Aware" project at Syracuse University School of Information Studies and Delft University of Technology. You can find more information about that project at http://deeppacket.info.

[35] Whilst referred to Internet performance in traditional manner

[36] See Dischinger et al., (2010). p. 1.

[37] See also Grove & Agic, (2012).

[38] FASTWEB is one of the main telecommunications providers in Italy providing voice, Internet, cable television, IPTV and FTTH connection.

[39] Opitel (Teletu) is a telecom subsidiary of Vodafone Omnitel NV offering fixed telephone services and Internet access via ADSL.

[40] Iliad is a French provider of telecommunication services that offers fixed telephony services, prepaid phone cards and internet access providing and hosting services.

[41] See Dischinger et al., (2010). p. 4-5. See also Comcast, (2008) and FCC, (2008).

[42] The authors have come to this conclusion by analyzing data for US ISPs Comcast and Cox. See Dischinger et al., (2008). p. 5-6.

[43] FastWeb, (2011), FastWeb, (2012a), FastWeb, (2012b), FastWeb, (2012c), FastWeb, (2012d), FastWeb, (2012e), FastWeb, (2012f), Free, (2011) and Kabel Deutschland, (2012).

[44] BitTorrent is a popular peer-to-peer file-sharing protocol that accounts for a large and rapidly growing fraction of the data bytes sent over the Internet. See Dischinger et al., (2008). p. 1.

[45] For detailed workings of the Glasnost test, see Dischinger et al., (2010).

[46] Source: Dischinger et al., (2010). p. 5

[47] The complete dataset from the DPI Project can be seen and downloaded at: http://homepage.tudelft.nl/r0d9v/glasnost_asn_monthly_to201004.txt.

[48] See Dischinger et al., (2010). p. 8-9.

[49] The opposite stands for false negative. See Dischinger et al., (2010). p. 4.