NET NEUTRALITY —

ENDING NETWORK DISCRIMINATION IN EUROPE

by Giusy Cannella, Raegan MacDonald & Jochai Ben-Avie

PREFACE FROM SIR TIM BERNERS-LEE

When I began to design the WWW 24 years ago, I did not have to ask anyone's permission. Today, anyone can still build a new application on the Web without permission from me, their ISP, their cable company or anyone else. As a result, the Web has sparked a second renaissance of entrepreneurship and innovation, adding billions to productivity and economic growth, and catalysing exciting new solutions to social challenges such as making quality healthcare and education accessible to all.

The Web Foundation's annual country ranking, the Web Index[1], shows that European countries are currently leading the world in harnessing ICTs for economic gain and social progress. Six out of the top 10 countries on our Index, including the world's number one, Sweden, are in Europe.

But other nations are nipping at Europe's heels, and we believe that keeping the Web "open for innovation" is critical to Europe's future competitive advantage. At the heart of this is network (or net) neutrality. Put simply, net neutrality means every customer should be able to access every service, and every service should be able to access every customer. It is the Internet Service Providers' responsibility to make sure they interoperate so that that happens.

It must be also clarified that net neutrality is NOT asking for the Internet for free. Rather, net neutrality is about keeping the internet open and without discrimination. Nor does net neutrality prevent the good management of the net in times of overload: what it precludes is discriminatory throwing away of packets on the basis of a commercial or political agenda. Just as a discrimination-free web, with personal privacy, is important for commerce, it is nowadays essential for education, health, and a sound democracy.

Some are concerned that mandating net neutrality through regulation would impose regulation for the internet that could inhibit broadband deployment. One vision is that the industry and government alike can indeed maintain net neutrality on a voluntary basis. However, recent events insist that to trust present and future governments and industries to that extent with something so crucial, something whose abuse provides such power, is naïve. Yes, regulation to keep the internet open is still regulation. And generally, the internet thrives on lack of regulation.

But the core freedom of speech, and the rules against discrimination based on race, gender, skin color, and religion are indeed enshrined in law in developed countries to great benefit and acclaim. Why not net neutrality? Just as democracy depends on legislated freedom of speech, so freedom to connect, with any application, to any party, is the fundamental social basis of the internet, and, now, the society based on it.

The European Commission – as guardian of the fundamental principles underlying the European Union, and steward of its future prosperity – has the major responsibility to act on this challenge. As the Commission considers the arguments and evidence, I hope it will commit to finding a timely solution to advance net neutrality across the European Union. We must keep the internet open, competitive and innovative, so that Europe can continue to lead the world in science, knowledge and social progress.

Sincerely,
Prof. Sir Tim Berners-Lee Founding Director, The World Wide Web Foundation
October 2013

[1] The Web Index, The Web Foundation: http://bit.ly/rhWlF2.

1. INTRODUCTION

The internet's continuing success rests on its three foundational principles: 1) that all points in the network should be able to connect to all other points in the network (*the end to end principle*); 2) that all providers of the internet should make their best effort to deliver traffic from point to point as expeditiously as possible (*the best effort principle*); and 3) that everyone should be able to innovate without permission from anyone or any entity (*the innovation without permission principle*). Collectively, these principles are the foundation of the openness and neutrality of the internet.

In practice, this means that Internet Service Providers[2] (hereafter ISPs) must treat all internet traffic on an equal basis, no matter the origin or type of content or means (equipment, protocols, etc) used to transmit packets, leading to the term "network neutrality". Yet, every day, ISPs are violating these principles, engaging in what is effectively network discrimination, that is – as elaborated upon in this paper – discrimination that ISPs apply on traffic on the network.

In May 2012, the Body of European Regulators for Electronic Communications (BEREC) published the findings of a joint investigation with the European Commission regarding traffic management. It revealed an increased trend of operators restricting access to services and sites. The most frequently reported restrictions are the blocking and/or throttling of peer-to-peer (P2P) traffic, on both fixed and mobile networks, and the blocking of internet telephony (Voice over IP), mostly on mobile networks.[3]

Access strongly believes that the only way to stop arbitrary discrimination online is to enact legislation enshrining network neutrality in law. Around the world there have been few, but, significant legislative initiatives to codify network neutrality. In 2010, Chile[4] was the first country to adopt legislation explicitly laying out network neutrality principles, followed by the Netherlands[5] which, in 2011, became the first European Union Member State to guarantee that "providers of public electronic communication networks which deliver internet access services and providers of internet access services do not hinder or slow down applications and services on the internet." In 2012, Slovenia[6] also enshrined the fundamental principle of net neutrality in law, and other countries – such as Brazil, Belgium, France, Germany and Luxembourg[7] – are currently moving in the same direction. We strongly urge the European Union to follow their examples and thereby ensure that net discrimination does not occur in any Member State.

The purpose of this paper is to provide more detailed insight into the issues surrounding the network neutrality debate in the European context. As this debate is often highly technical and subject to many misunderstandings, this paper will provide a brief clarification on some of these main topics, particularly the definition of network discrimination, what constitutes "reasonable" traffic management and its impacts on the economy and the fundamental rights to privacy, data protection, and freedom of expression.

2. BENEFITS OF NET NEUTRALITY

As of June 2012, more than 2.7 billion people[8] – over a third of the world's population – have access to the internet, with more than 600,000 new users connecting each and every day.[9] These figures are particularly substantial if we look at the European Union where, of 500 million inhabitants, 67.5% of the population is connected to "the network of networks".[10]

[2] By "Internet Service Providers" (ISPs) we are referring to any legal person that provides internet access service to the public. Many but not all of ISPs are telephone companies or telecommunications providers.

[3] Findings from BEREC's and the European Commission's joint investigation, 2012: http://bit.ly/UUDm6N.

[4] Bill 4915: Amendment to the Chilean Telecommunications Act, original text: http://bit.ly/b3oY0z, article in English on the law: http://bit.ly/a2y698.

[5] Summary from Bits of Freedom of the amended Dutch Telecommunications Act: http://bit.ly/jzE63v.

[6] Slovenia reinforces net neutrality principles, radiobruxelleslibera, 2013: http://bit.ly/TycLzs.

[7] Study: Net neutrality policies vary in EU countries, PCWorld, 2013: http://bit.ly/15zFIBk.

[8] International Telecommunication Union: The World in 2013 - ICT Facts and Figures: http://bit.ly/15zXF3k.

[9] Infographic on internet usage, Royal Pingdom, 2012: http://bit.ly/ysK7Rd.

[10] Digital Agenda Scoreboard 2012, European Commission: http://bit.ly/QruIL9.

Unfettered access to the internet is becoming recognised as a basic human right.[11] Frank la Rue, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, has underlined the fact that the internet is a gateway through which fundamental rights can be realised, notably the freedoms of expression and association, but also the rights to access culture and education.[12] Furthermore, an open and neutral internet – without discriminatory interference of any sort – safeguard the fundamental rights to privacy and data protection. As Sir Tim Berners-Lee pointed out in the preface of this paper, these rights are fundamental for the thriving of healthy democracies.

The importance of an open and neutral internet has also been recognised by several respected institutions: from the Council of Europe,[13] and the OECD,[14] to the World Bank, for the exercise of human rights, and also as a platform for economic growth. In particular, a World Bank report reveals that there is a direct correlation between the increase of high speed internet connection and development across all levels of the economy and society.[15]

In 20 years, the digital market has become quite possibly the greatest driver for job creation, innovation, and competitiveness the world has ever known. This has been possible thanks to an open and neutral platform allowing web entrepreneurs to enter the market and innovate with groundbreaking ideas.

In a joint letter[16] delivered at a June 2013 event in the European Parliament organised by Access[17] to discuss the importance of network neutrality, a coalition of 20 European startups asked EU Commissioner for the Digital Agenda Neelie Kroes to keep the internet open and neutral so they can continue to innovate "without permission" of ISPs that may want to play the role of gatekeepers.

However, ISPs in Europe are frequently discriminatory, a practice that must be stopped if fundamental rights are to flourish and the economic benefits of the Digital Single Market[18] are to be realised.

3. WHAT IS NETWORK DISCRIMINATION?

Access defines "network discrimination" as the tendency of ISPs to intentionally and arbitrary apply restrictions to users' access to the open and neutral internet.[19] Generally speaking, network discrimination can take place, *inter alia*, in the following ways:

- **Blocking of applications and services:** In order to maximise profits, some ISPs – that also offer their own services and applications online – exclude certain services and applications of competing market players. The most prominent case of this form of network discrimination is European mobile providers (like Deutsche Telekom) blocking or restricting the use of Voice over IP (VoIP) services (like Skype and Viber) for their customers.[20]

- **Slowing or "throttling" internet speeds:** Some ISPs slow down specific services (like YouTube) and applications (like Skype), or ask users to pay an extra fee to have access to these internet platforms. Given the high latency (delay) sensitivity of many applications, ISPs are able to compromise the correct functioning of these services by slowing them down, preventing the services from running properly. Often ISPs – especially telecommunication companies – do this to favour their own voice calling services over VoIP services, thereby crushing competition.

[11] United Nations Declares Internet Access a Basic Human Right, The Atlantic, 2011: http://bit.ly/isO8oq.

[12] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 2011: http://bit.ly/kNHvvm.

[13] Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet, 2008: http://bit.ly/SVo83y.

[14] OECD Input to the United Nations Working Group on Internet Governance (WGIG), 2005: http://bit.ly/148Irfl.

[15] Summary of the 2009 World Bank Group Report: http://bit.ly/qVaKp.

[16] Open Letter by European CEO's to the European Commission: http://bit.ly/18Q3CdY.

[17] Guaranteeing competition and the open internet in Europe, program and video of the full event: http://bit.ly/18P5kME.

[18] Digital Agenda for Europe, Digital Single Market: http://bit.ly/13GUKnu.

[19] Q&A on Network discrimination in Europe, Access, 2013: http://bit.ly/11fUriz.

[20] Deutsche Telekom Restricts Skype On iPhone, InformationWeek, 2009: http://ubm.io/13HPjRe.

- **Blocking websites:** ISPs often block websites for a number of reasons – to secure their network, or to avoid competition, and sometimes for social, public relations or political reasons. In the UK, for instance, Orange Telecom blocked the French digital rights advocacy group, La Quadrature du Net's website on pre-paid mobile accounts.[21]

- **Preferential treatment of services and platforms:** ISPs can also impose data caps on internet access contracts while granting data allowance exceptions to a company's own proprietary streaming services (like Deutsche Telekom to its own "T-Entertain").[22] They can (and do) also grant preferential treatment to select services – such as Orange France with the popular music streaming service Deezer[23] – ahead of other competitors, effectively imposing anti-competitive limitations on markets such as those for legal online music. Moreover, generally only large, well-established companies can afford this preferential treatment, resulting in a further stifling of innovation.

4. WHAT IS "REASONABLE" TRAFFIC MANAGEMENT?

Discriminatory practices are often justified by ISPs[24] as "reasonable" traffic management implemented to limit congestion on their networks. However, there is a fine line between preventing saturation by slowing down or throttling certain streams and degrading the quality of competing services. This leads to another question in this debate: what do acceptable traffic management practices look like?

Traffic management is "reasonable" when it is deployed for the purpose of technical maintenance of the network, namely to block spam, viruses, or denial of service attacks, or to minimise the effects of congestion, whereby equal types of traffic should be treated equally – as established by the Dutch net neutrality law. Traffic management techniques should only be used on a temporary basis, during exceptional moments.

When traffic management practices are put in place to pursue other purposes or are used on a permanent basis, they should be considered as unreasonable. Furthermore, discriminatory practices – such as blocking and throttling competing services – should be clearly prohibited by law as they threaten citizens' fundamental rights and undermine the proper functioning of the online marketplace.

However, many ISPs claim that the exponential growth in web usage, particularly bandwidth intensive video applications, along with the alleged rise in infrastructure costs, cause congestion on the network and that without a degree of traffic management, congestion would make it impossible for users to enjoy sufficient quality of service. In response to the alleged "data explosion", ISPs are making greater use of traffic management techniques in order to provide "guaranteed quality of service", which is the ability to provide different priority to different applications, services, or data.[25] However, guaranteeing a certain quality of service to the detriment of other types of data, applications, services, etc., at their sole discretion is a violation of the best effort principle, and therefore can not be defined as reasonable traffic management.

Access believes that allowing ISPs to offer guaranteed quality of service exclusively to one or more applications within the same class of applications (for example between VoIP applications) should be prohibited.[26] Indeed, this type of preferential treatment interferes with users' ability to use the applications and services of their choice without interference from ISPs. It also enables these latter to use the provision of quality of service as a tool to distort competition among applications within a class, which is exactly what network neutrality would safeguard against.

[21] Open Rights Group, 2012, Orange UK blocking La Quadrature du Net: http://bit.ly/zRpALj.

[22] Deutsche Telekom's "anti-net-neutrality" plans alarm German government, Gigaom, 2013: http://bit.ly/17jT8QR.

[23] Orange partners with Spotify rival Deezer, Cable.co.uk, 2011: http://bit.ly/16079AV.

[24] The open internet – a platform for growth, Plum consulting, 2011 – page 19: http://bit.ly/19eh5x6.

[25] The collapse in the value if the mobile and gigabyte: myth and reality, Analysys mason, 2012: http://bit.ly/166CKUq.

[26] Telco Action Plan, Access, 2012: http://bit.ly/J0QWQ9.

The Body of European Regulators for Electronic Communications (BEREC) has recognised that quality of service guarantees are simply not needed. A recent BEREC report points out that: "While not providing a guaranteed quality level of data delivery, the best effort approach of the internet does not imply low performance, and in fact results in most cases in a high quality of experience for users, even for delay-sensitive applications such as VoIP."[27]

While we agree that ISPs should be able to manage their networks, we believe traffic management should only be allowed as narrowly tailored deviations from the rule, and should not include arbitrary or permanent restrictions by ISPs, as these practices go clearly against the "end-to-end" and "best effort" principles that are fundamental to the internet's functioning. In the end, the best way ISPs can manage traffic is to invest in network infrastructure to increase the networks' capacity and avoid congestion.

5. WHAT ARE THE FUNDAMENTAL RIGHTS IMPACTS OF FILTERING TECHNOLOGIES?

The increasing use of perpetual and unjustified traffic management also raises questions about privacy of communications. In order to implement a variety of traffic management practices, such as blocking, shaping, or filtering, several ISPs deploy tools such as Deep Packet Inspection (DPI),[28] a technology that allows them to examine data traveling over the internet and recognise what sort of packet it is – a virus or simply an email, for example – and therefore to interfere with such communications.

Although DPI is often used by ISPs to detect and mitigate attacks to their networks (e.g. a virus or other malicious software), this technology can also be deployed for reasons that fall far outside the scope of securing the network. Indeed, this highly intrusive tool can be used not only to implement discriminatory practices – such as blocking or prioritisation of certain types of traffic – but also to monitor and even copy all information that travels across a network. This is not hypothetical, it happens everyday in countries like China, Iran, and Russia – whose governments frequently deploy this technology to censor political speech and suppress dissenting activity online.[29] It is also implemented in democratic countries such as Germany and the United Kingdom.[30]

By inspecting communications data, ISPs may breach the privacy of communications, which is a fundamental right guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. In line with the opinion of the European Data Protection Supervisor, these filtering techniques must only be used "in conformity with the applicable data protection and privacy safeguards, which lay down limits as to what can be done and under which circumstances."[31]

The Dutch net neutrality law, the first of its kind in Europe, does an exemplary job addressing this.[32] This law not only prohibits ISPs from throttling or filtering the connections of their customers, it also provides strict guidelines on the techniques that can be employed for unjustified traffic management (and wiretapping). Specifically, the use of filtering software as an advanced surveillance tool – which would include Deep Packet Inspection – is prohibited without the express consent of the user or the company being served with a valid legal warrant.

[27] BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines, 2012: http://bit.ly/TE4SUo.

[28] Deep Packet Inspection (DPI) is a computer network surveillance technique that uses device and technologies that inspect and take action based on the contents of the packet i.e. it considers the complete payload of packet rather than just the packet header (definition from the Institute of Electrical and Electronics Engineers (IEEE), 2011: http://bit.ly/16MssuV.

[29] The Kremlin's new Internet surveillance plan goes live today, Privacy International, 2012: http://bit.ly/Sr9vDb.

[30] A quick guide to Cameron's default Internet filters, Open Rights Group, 2013: http://bit.ly/163FYpT.

[31] Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 2011: http://bit.ly/14Lmrxw.

[32] See footnote 5.

6. THE CURRENT STATE OF PLAY IN EUROPE

Since the Summer of 2010 the European Commission has launched two public consultations to explore issues of internet traffic management, but despite the evidence revealed by BEREC's investigations, no concrete actions have been undertaken to prevent network discrimination.

At the end of 2012 the European Parliament adopted two resolutions supporting the need for legislation that would enshrine net neutrality in order to ensure the completion of the European Digital Single Market.[33]

The European Commission is currently looking to publish its "**Recommendations on the Open Internet and Network Neutrality**" by the end of 2013/early 2014, which according to the Commission's website will include guidance on transparency, elements of traffic management, switching, and the responsible use of traffic management tools.[34]

In parallel, the European Commissioner for the Digital Agenda Neelie Kroes has recently issued a proposal for a **Regulation for a Telecoms Single Market**,[35] that includes binding measures for the telecoms sector to achieve the Commission's goal of a "Connected Continent". However, while according to the Commission's press release[36] the proposed Regulation will "encourage more competition between more companies" and guarantee "net neutrality, innovation and consumer rights", it fails to deliver on a number of fronts. Below we will highlight some of the major concerns.

Although the legislative text contains provisions (Article 23) that would prohibit ISPs to "block, slow down, degrade or otherwise discriminating against specific services, content or applications," it makes these provisions meaningless by allowing ISPs to enter into commercial agreements with content providers in order to prioritise internet traffic. One of the most problematic outcomes of such special deals would be that big content providers would be able to enter into commercial deals with ISPs to ensure that their traffic is always delivered first and faster.

Furthermore, the Regulation would allow ISPs to impose "data-caps" on internet access contracts while granting priority to their own services (like Deutsche Telekom to its own "T-Entertain").[37] In this way, access providers grant preferential treatment to selected services, while competitors' services are discriminated against, effectively imposing anti-competitive limitations on online markets and leading to a "two-tier internet". The sum of these provisions would equal the exact opposite of net neutrality.

Indeed, Commissioner Kroes, once a strong proponent of network neutrality,[38] seems to have abandoned her commitment to ensure an open and neutral internet. Her approach, which is now confirmed in the proposed Regulation, has wavered in speeches between bold statements stating her desire to ensure that all EU citizens have access to an open and neutral internet,[39] while at other times suggesting that a sufficient solution to such pervasive discrimination would be to compel telecommunication companies to be transparent[40] so citizens can make "informed choices".[41] This suggests that as long as telecommunication companies disclose whether or not they apply restrictions on internet usage, they can act discriminatorily. According to this logic, such transparency will enable users to "switch" service providers and internet offers "without countless obstructions" if they are not getting the full internet they expect.

This approach problematically suggests that competition and enhanced transparency might be sufficient to protect net neutrality. But transparency and "switching" are simply not a solution if there is no real competition in the market.[42] These elements will not effectively guarantee the freedom to impart and receive information the way an open and neutral internet provides.

[33] European Parliament's Report on Completing the Digital Single Market: http://bit.ly/13GVoRK and EP's Report on a Digital Freedom Strategy in EU Foreign Policy: http://bit.ly/UwhGwG.

[34] Digital Agenda for Europe, Open Internet: http://bit.ly/12NzCbK.

[35] Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent. 2013: http://bit.ly/18cs2hW.

[36] Commission proposes major step forward for telecoms single market, press release, 2013 http://bit.ly/18PXSNZ.

[37] Deutsche Telekom's 'anti-net-neutrality' plans alarm German government, Gigaom, 2013: http://bit.ly/17jT8QR.

[38] EDRi's timeline reporting Commissioner Kroes' statements on net neutrality: http://bit.ly/12NzFo6.

[39] The politics of the completing the telecoms single market, speech from Commissioner Kroes, May 2013: http://bit.ly/18xhiue.

[40] Internet et applications de filtrage: une histoire de choix et de recettes, Liberation, 2013: http://bit.ly/U160q0.

[41] The EU, safeguarding the open internet for all, speech from Commissioner Kroes, June 2013: http://bit.ly/13ichRK.

[42] Consumer Focus' Report "Lost on the broadband super highway", 2012 - page 5: http://bit.ly/SJtHkK.

The proposed Regulation has already been the subject of heated debate, even within the European Commission, as revealed by EDRi in a leaked internal Commission document.[43] In particular, DG Justice raised concerns that the Regulation could undermine the Charter of Fundamental Rights, namely freedom of expression. The document also warned of the dangers of encouraging preferential agreements between content and ISPs.

The Commissioner for Enterprise and Industry is equally concerned that such an undermining of net neutrality would have an adverse effect on EU entrepreneurs, an element ironically highlighted by Commissioner Kroes herself only a few short months ago.[44]

A Commission's internal vote showed that Commissioner Kroes' proposal did not have the support of a large majority of Commissioners, who share many of civil society's concerns, particularly regarding the aspects related to net neutrality.[45]

The legislation is now in the hands of the European Parliament, who have the opportunity to amend the draft text to reflect the position of a large, cross-party segment of the Parliament: to enshrine strong, enforceable network neutrality provisions in EU law.[46]

7. PRINCIPLES OF A NET NEUTRALITY LAW

In order to end network discrimination and ensure a thriving and neutral internet, we recommend that the following provisions are enshrined into law:

1. The internet must be kept open and neutral. Reachability between all endpoints connected to the internet, without any form of restriction, must be maintained.

2. All data traffic should be treated on an equitable basis no matter its sender, recipient, type, or content. All forms of discriminatory traffic management, such as blocking or throttling should be prohibited.

3. ISPs shall refrain from any interference with internet users' freedom to access content and use applications of their choice from any device of their choice, unless such interference is strictly necessary and proportionate to:

   i. As a transient and exceptional measure, mitigate the consequences of congestion, while treating the same kinds of traffic in the same manner;

   ii. Safeguard the integrity and safety of the network, the service, or a terminal device of the user (e.g. blocking viruses and DDOS-traffic);

   iii. Block the delivery of unsolicited commercial messages (e.g. spam), but only if the subscriber has given prior consent;

   iv. Respect specific legal obligations or

   v. Comply with an explicit request from the subscriber, provided the subscriber may revoke the request without any increase in subscription fee at any time.

4. Use of packet inspection software (including storage and re-use of associated data) should be reviewed by national data protection regulators to assess compliance with the EU's data protection and fundamental rights framework. By default, these types of inspection techniques should only examine header information.[47]

[43] Leak: Damning Analysis Of Kroes' Attack On Net Neutrality, EDRi, September 2013: http://bit.ly/17NfpYO.

[44] A Telecoms Single Market: Building a Connected Continent , Speech from Commissioner Kroes, May 2013: http://bit.ly/14Gviy1.

[45] EU may have to redraw telecoms plans - EU Commission official, Reuters, 2013: http://reut.rs/18Qcgo4.

[46] See footnote 33.

[47] Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 2012: http://bit.ly/15yLXXg.

5. Complete information on reasonable traffic management practices and justifications must be accessible and foreseeable to the public. Network operators should be transparent and accountable to any changes in practices.

6. Non-neutral treatment of traffic for "voluntary" law enforcement purposes must be prohibited unless there is a legal basis and predictable procedure in the country where the restriction is being implemented. Failure to require this would be a breach of Article 52 of the Charter of Fundamental Rights and articles 8 and 10 of the European Convention on Human Rights.

8. WHY EUROPE NEEDS NET NEUTRALITY LEGISLATION NOW

There are a variety of different approaches some states have pursued in order to uphold the principle of network neutrality; from legislative, to co-legislative, or through voluntary agreements in the private sector. Access believes that the only way to truly guarantee net neutrality in Europe is to enact strong and comprehensive legislation that clearly prevents ISPs from arbitrary discriminating online and avoids that commercial interests of major incumbent prevail on fundamental rights.

In Europe, the findings reported by BEREC prove that in the absence of a regulatory framework explicitly banning restrictions online such as blocking and throttling ISPs are incentivised to apply restrictions on applications and sites.

For those few countries that have taken proactive steps to address the threats to the open and neutral internet, some countries have opted for a self-regulatory approach, such as the United Kingdom's "Open Internet code of practice", a voluntary code of conduct for ISPs to promote the offering of "full and open internet access".[48] However, as sign-on is not mandatory, only a small number of ISPs have joined this set of commitments. It also contains loopholes: while the code specifies that specialised or restricted services shall not be labeled "internet access", it emphasises transparency (and not, for instance, banning of discriminatory practices) around any restrictions applied to users' internet access.

Some states have opted for a co-regulatory approach, where the legislator and the private sector co-operate. This is the case of the Norwegian Post and Telecommunication Authority (NTPA) that - in collaboration with ISPs, content providers, industry organisations and consumer protection agencies - has established the "Guidelines for Internet neutrality" - a set of principles to safeguard net neutrality.[49]

However, these principles do not have any formal legal status and the Norwegian authority is not able to issue sanctions to those ISPs who do not comply with these principles. The proposed framework is also not as robust to cover all bases of discrimination - for instance, the guidelines states that the blocking of child pornography should be considered as "reasonable traffic management". As elucidated in Access' proposed principle No. 6, that "voluntary" law enforcement purposes must be prohibited unless there is a legal basis and procedure in the country where the restriction is being implemented. Any failure to require this would be a breach of Article 52 of the Charter of Fundamental Rights.

This co-regulatory solution, while certainly providing further protections than the self-regulatory model, still does not provide the necessary guarantees that binding legislation would ensure.

[48] Open internet code of practice: Voluntary code of practice supporting access to legal services and safeguarding against negative discrimination on the open internet, United Kingdom, 2012: http://bit.ly/11pesU0.

[49] Network neutrality, Guidelines for the Internet neutrality, Norway, 2009: http://bit.ly/1arK7q0.

Indeed, Professor Tim Wu of Columbia University - who coined the term "net neutrality" - revealed in his studies that despite the benefits offered to citizens and to both access and content providers from a neutral platform, ISPs more often favour their own services and prioritise short-term over long-term interests.

As evidence has shown that if businesses believe that it is not in their best interest to remain neutral, then neither self-regulation nor co-regulation will successfully persuade them to act in a manner that is thought to be contrary to their commercial interests.[50]

9. CONCLUSION

Network neutrality legislation will ensure that the internet remains open, democratic, and innovative throughout the European Union. Furthermore, anti-net discrimination legislation will allow the free flow of content, applications, and services, and a diversity in the types of equipment and protocols that may be used. This would effectively guarantee a level playing field for all web sites and internet technologies, to the benefit of both European citizens and all companies conducting business in the European Digital Single Market, especially startups.

Europe has long been an international policy standard-setter, especially on issues concerning human rights, and network neutrality should be no exception. Strong legislation will not only provide European citizens with the right to access an unfettered internet free from discrimination, but could also set an important standard for the preservation and promotion of the open and neutral internet around the world, benefiting users globally.

To realise and protect the full potential of the internet to enable and promote the flourishing of human rights, Europe needs a strong and comprehensive net neutrality legislation now.

Access (AccessNow.org) is an international NGO that defends and extends the digital rights of users at risk around the world. Combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information, please contact Raegan MacDonald (raegan@accessnow.org) or Giusy Cannella (giusy@accessnow.org) or visit https://www.accessnow.org/netdiscrimination.

[50] Network Neutrality, Broadband Discrimination, Tim Wu, 2002: http://bit.ly/aGLNxM.