Bird & Bird

Bird & Bird LLP
Zuid-Hollandplein 22
2596 AW The Hague
The Netherlands
Tel +31 (0) 70 353 8800
Fax +31 (0) 70 353 8811
twobirds.com

To: BEREC
Attn: NN-Consultation@berec.europa.eu
From: Marjolein Geus and Frank Simons
Date: 15 July 2016
Our Ref:: NOMINUM – Public consultation on draft BEREC Guidelines on implementation of net neutrality rules
Subject: Contribution on behalf of Nominum, Inc.

1. ABOUT NOMINUM

Nominum has been at the forefront of the development of the internet since 1999. It was the first to develop commercial-grade DNS products, which to date form an important part of the very core of the internet. More than 100 service providers use Nominum DNS worldwide. The Nominum products are deployed in over 40 countries and process 1.6 trillion queries each and every day.

DNS platforms have now evolved into an ideal basis for innovative applications that allow end-users to protect themselves on the internet. These applications allow for effective protection against internet based threats such as viruses and other malicious software. Likewise, through 'parental control' applications, they can give end-users control to determine which information they wish to receive and which not.

Nominum offers such applications to Internet Service Providers (hereinafter: ISPs), which can offer them to end-users as a service. Such services provide functionality similar to more traditional, end-user equipment-based applications, but with improved user-friendliness and broader application to any end-user device connected to the internet.

2. THE DRAFT GUIDELINES

Nominum fully supports the aim of Regulation (EU) 2015/2120 (hereinafter: the Regulation) and BEREC's draft Net Neutrality Guidelines (hereinafter: the Draft Guidelines) to preserve end-user choice and the internet as an open platform for innovation.

Nominum is grateful for the opportunity to submit its views on the Draft Guidelines. It wishes to use this opportunity to highlight the position of DNS policy based parental control applications.

Such applications are offered to end-users independent of Internet Access Services (hereinafter: IAS) and in no way (directly or indirectly) circumvent net neutrality principles. They constitute 'applications and services' which the Regulation aims to protect and are not in themselves targeted by the Regulation.

We suggest BEREC clarifies this in the definitive guidelines.

3. DNS POLICY BASED PARENTAL CONTROL

DNS policy based parental control applications are an important innovation to more traditional filtering software installed on individual user devices.

Such applications:

- Protect any end-user device, independent of, for example, manufacturer or (mobile or desktop) operating system, and without the need to install software on every individual device. This is an important innovation in comparison to traditional, end-user equipment based parental control applications. DNS policy based applications provide end-users with the same functionality, with less effort and across more (types of) devices.

- Are offered independent of IAS. They are offered as add-on services by ISPs or as stand-alone services by service providers that are not ISPs. ISPs offer such add-on services in a similar manner as they offer more traditional parental control software to their end-users for download – they are offered to the end-user as an option and the end-user can decide to use the solution or not.

- Offer the end-user the same level of control as when using more traditional filtering software installed on end-user devices. DNS policy based solutions can be offered switched-off by default and can be switched on and off by the end-user at any time though a web-browser interface (i.e. without a need to wait for the ISP to manually alter configuration or respond in any other way). They provide the end-user extensive control over the configuration of the filtering, inter alia though the ability to configure end-user specific 'white lists' and 'black lists'.

- Do not interfere directly with internet traffic. In this respect, DNS policy based applications work entirely different from, for example, so called deep packet inspection technology. Deep packet inspection technology continuously monitors all traffic on an ISP's network at the IP packet/content level. In contrast, DNS policy based services perform initial analysis at the domain name level. Only once a domain is identified as containing content that the end-user has indicated he or she does not wish to receive are more detailed filtering mechanisms applied (such as proxy-technologies).

- Do not affect the underlying IAS, either with regard to openness, speed, quality, tariffs or in any other way. DNS policy based applications can be offered to end-users switched-off by default, without any incentives to be switched on or off, leaving the choice entirely to the end-user and leaving the underlying IAS entirely neutral.

- Are not what in the Draft Guidelines are referred to as 'sub-internet services'. The latter concept, as described in the Draft Guidelines, suggests that the ISP determines the level of access offered by such service, without the end-user being able to alter this after he or she has purchased the service. In contrast, DNS policy based parental control applications addressed in this document provide the end-user with full control at all times.

- Are currently used and promoted in for instance the UK, the Netherlands, Australia and Ireland and highly valued by end-users.

4. POSITION UNDER NET NEUTRALITY REGULATION

Nominum is aware that, prior to the adoption of the current Regulation, discussions have taken place – both with regard to the Regulation and in the context of existing Member State[1] legislation – on how parental control applications should be treated under net neutrality rules.

A key aspect in these discussions has been the level of end-user control. BEREC confirmed the importance of end-user control in its 2012 'Guidelines for quality of

[1] For example, such discussions took place in the Netherlands, where strict net neutrality rules were introduced in 2013. Parental control solutions such as those offered by Nominum were allowed under these national rules (Dutch Parliamentary Documents (*Kamerstukken*) II 2010/11, 32549, nr. 29, p. 4-5) and Parliamentary Documents (*Kamerstukken*) I 2011/12, 32549, nr. L, p. 2).

service in the scope of net neutrality', emphasising criteria such as what the default settings are and how easily the settings can be activated and deactivated:

> *"An end-user who asks his/her ISP to block some content, for example through parental control, also provides an objective justification for blocking, as long as this user's decision is well informed, can easily be rescinded and does not affect other end-users. Traffic management practices that the end-user can control will often be seen as more reasonable than measures that are taken unilaterally by the ISP, in light of the regulatory aim of avoiding harm to end-users. However, the fact that an end-user subscribes to a restricted service does not necessarily imply that these restrictions are approved or controlled by the user. Assessment of whether the end-user really is able to control these measures depends on criteria such as what the default settings are and how easily the settings can be activated and deactivated."*[2]

These principles have not changed under the current Regulation. It is clear from the text and the purpose of the Regulation that end-user controlled parental control applications, such as those described in section 3, should be considered to constitute applications which are not part of an IAS and are therefore not targeted by the Regulation.

For DNS policy based applications, this is even more so due to the fact that these do not interfere with the internet traffic itself and therefore to not constitute traffic management (see section 3, fourth bullet) as referred to in BEREC's 2012 guidance.

End-user choice as the underlying principle of the Regulation

End-user choice is the key underlying principle to the Regulation. Central to the Regulation is that *"[e]nd-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, [...]"*. This is expressed in (inter alia) recital (1) and article 3 (1) of the Regulation and in various places in the Draft Guidelines.

The Regulation also ensures that end-users can use applications which enable them to filter information as they wish and which protect them against receiving information which they do not want to receive or from accessing websites which they do not want to access. DNS policy based parental control applications fall within the category 'applications and services' which article 3(1) of the Regulation aims to ensure access to.

[2] BEREC Guidelines for quality of service in the scope of net neutrality, BoR (12) 131, 26 November 2012, p. 50-51.

Any other interpretation of the Regulation would be contrary to the basic principle of the Regulation and the broader fundamental right for end-users to choose not to receive or be exposed to information or content which they do not wish to receive or be exposed to.

Protection of children online

This is even more apparent where parental control applications are employed to protect children.

The EU has taken several initiatives to promote the protection of children online. In 2012, the European Commission published a "European Strategy for a Better Internet for Children".[3] In this strategy document, it explicitly confirms that parental control applications should be made wider available and that:

> *"Industry should ensure the availability of parental controls that are simple to configure, are userfriendly and accessible for all on all internet-enabled devices available in Europe. The tools should be efficient on any type of device and for any type of content, including user-generated content. They should comply with best practices to ensure accountability and transparency. [...]"*[4]

DNS policy based parental control applications fulfil this objective, even more so than traditional, end-user device based applications that by their nature are not *"efficient on any type of device"*. Any interpretation of the Regulation to not allow such applications would contravene EU policy in this field.

Promoting innovation

Moreover, DNS policy based parental control applications constitute a further innovation of more traditional user device-based filtering applications. This innovation fits with the general trend towards traditional software applications evolving into services made accessible via the internet.

Safeguarding such innovation is also a key objective of the Regulation where it *"aims [...] to guarantee the continued functioning of the internet ecosystem as an engine of*

[3] Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, European Strategy For A Better Internet For Children, COM(2012) 196 final, 2 May 2012.
[4] European Strategy For A Better Internet For Children, COM(2012) 196 final, p. 11.

innovation". This is reflected in recital 1 of the Regulation as well as in various other recitals and in the Draft Guidelines.

Interpretation of the Regulation to allow traditional parental control software installed on end-user devices, but to not allow (more innovative alternatives offered as a service would be at odds with the aim of the Regulation to promote innovation.

Level playing field

Moreover, interpretation of the Regulation as to not allow ISPs to offer DNS policy based parental control applications would disturb the level playing field envisaged by the European Commission in its Digital Single Market strategy.

DNS policy based parental control applications are currently being offered by both ISPs and non-ISPs. This is in itself evidence that such applications should be considered to be independent of the underlying IAS.

Moreover, if such services were to be considered to be targeted by the Regulation, this would only affect ISPs. It would not affect non-ISPs offering the same service because they do not also offer IAS and are therefore not subject to net neutrality regulation.

This would constitute an arbitrary, unnecessary discrimination between market players, on which the European Commission wrote in its communication on the Digital Single Market:

> *"Telecoms operators compete with services which are increasingly used by end-users as substitutes for traditional electronic communications services such as voice telephony, but which are not subject to the same regulatory regime. The review of the telecoms rules will look at ways of ensuring a level playing field for players to the extent that they provide competing services and also of meeting the long term connectivity needs of the EU."*[5]

In this context, interpretation of the Regulation as to not allow ISPs to offer DNS policy based applications would be in contradiction with the European Commission's policy in respect of the Digital Single Market to create a level playing field between regulated ISPs and others offering the same services while not being subject to the same regulatory regime.

[5] Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, A Digital Single Market Strategy for Europe, Brussels, 6 May 2015, COM(2015) 192 final, p.10.

5. CLARIFICATION OF THE DRAFT GUIDELINES

In order to avoid any misunderstanding on the position of end-user controlled, DNS policy based parental control applications (as described in section 3), the following phrase could be added to paragraph 22 of the Draft Guidelines:

> *"22. Secondly, end-users have the right to use and provide applications and services. "Use and provide" means that the right applies both to consumption and provision of applications and services. "Applications and services" means both applications (including client and server software) as well as services (including filtering services which are operated under the control of the end-user)."*

For consistency, and to avoid confusion regarding any distinction between more traditional, end-user equipment-based applications and more innovative, DNS policy based alternatives, the reference to "terminal equipment-based" in paragraph 75 could be deleted:

> *"75. By way of example, ISPs should not block, slow down, alter, restrict, interfere with, degrade or discriminate advertising when providing an IAS, unless the conditions of the exceptions a), b) or c) are met in a specific case. In contrast to network-internal blocking put in place by the ISP, ~~terminal equipment based~~ restrictions put in place by the end-user are not targeted by the Regulation."*

6. CLOSING REMARKS

Nominum would be grateful if BEREC would take the suggestions as set out above into consideration when establishing the definitive guidelines. Nominum would be happy to provide more insight into the functioning of the applications described in section 3 if BEREC so wishes. For this purpose, or for any other information regarding this document, Nominum can be contacted through the contact details below.

Bird & Bird
Marjolein Geus / Frank Simons

Nominum
Robert Verheecke, CFO