CLIFFORD
CHANCE

Client briefing June 2016

New EU Net Neutrality rules – impacting the balance of power online

On 30 April 2016, new net neutrality rules became effective in the European Union under Regulation No. 2015/2120 (the **Regulation**). These rules aim to safeguard an open internet, in the sense that internet access service providers do not restrict end-users' ability to access and distribute online information or run online applications and services of their choice, using the devices of their choice. A good cause. However, if interpreted broadly or disparately by the various EU Member States, these rules may distort competition among network operators and online content and application providers in the internal market.

In this digital age, unencumbered internet connectivity is considered essential to enabling the exercise of fundamental rights such as the freedom of expression and information and the freedom to conduct a business, which are enshrined in the European Convention on Human Rights and the European Charter of Fundamental Rights. Through traffic management, the party enabling end-user access to the internet – the internet access service provider – is technically in a position to determine the extent to which online information and applications can be made available and accessed. It is this position of control that has led legislators around the world to enact rules governing net neutrality, which call for an equal treatment of internet traffic regardless of its content, origin or destination. The new net neutrality rules under the Regulation are the subject of the present briefing. The Regulation also contains rules governing roaming, which are not further discussed here. In relation to net neutrality, we would point also to the recent Recommendation on net neutrality issued by the Council of Europe on 13 January 2016, which contains similar, more principle-based net neutrality provisions.

Access and non-discrimination

Article 3 of the Regulation sets forth the principal net neutrality rules, and formulates:

- a right for end-users to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice via their internet access service, irrespective of their location or that of the provider, or the location, origin or destination of the information, content, application or service concerned; and
- an obligation for internet access service providers to treat all traffic equally, without discrimination, restriction or interference, and irrespective of the sender and receiver, or the content, services or applications concerned.

Reasonable network management

The end-users' internet access rights are a manifestation of the aforementioned fundamental freedoms, and, like these freedoms, do not apply without limitation. The Regulation allows internet access providers to implement reasonable traffic management measures to enable an efficient use of network resources and the optimization of overall transmission quality. In order to be considered 'reasonable', these measures must be transparent, non-discriminatory and proportionate, and may not be based on commercial considerations but only on objectively different technical quality of service requirements of specific categories of traffic. These traffic management measures may furthermore not monitor the specific content of traffic (*eg*, by deep packet inspection) and may not be maintained for longer than necessary.

Exceptions

Traffic management measures which go beyond what is considered 'reasonable', and in particular measures that block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, are only permitted insofar as necessary:

- to comply with EU legislation or (EU-compliant) national legislation, or with measures implementing this legislation, including the orders of competent courts or public authorities;
- to preserve the integrity and security of networks, services provided over those networks and of end-users' terminal equipment; or
- to prevent impending network congestion and mitigate effects of exceptional or temporary network congestion, provided equivalent categories of traffic are treated equally.

These three categories of exceptions are discussed in further detail in the below. The exceptions are positioned as a *limitative* list and are to be interpreted strictly. Generally, the Regulation provides in Art. 10(3) that any national measures, including self-regulatory schemes, that do not comply with the net neutrality obligations imposed on internet access service providers in the Regulation (including the traffic management exceptions) may be maintained only until 31 December 2016.

Exception 1: Compliance with laws and orders

The exception for compliance with applicable laws and the orders of competent courts and public authorities includes, for example, measures as have been taken by access providers pursuant to court orders in various Member States to block piracy websites that enable the downloading of copyright-infringing content. The European Court of Justice (ECJ) ruled that such measures are permitted, provided a right balance is struck between the fundamental rights involved (ECJ 27 March 2014, Case C-314/12, *UPC Telekabel Wien*). An injunction issued by a Belgian court ordering a network provider to filter all traffic to all its customers for infringing content as a preventative measure for an unlimited period was not considered to strike such a balance (ECJ 24 November 2011, Case C-70/10, *Scarlett Extended*). The European Court of Human Rights (ECHR) has ruled that blocking access to the internet or parts of the internet for whole populations or segments of the public can never be justified, including in the interests of justice, public order or national security (ECHR 18 December 2012, *Yildirim v. Turkey,* concerning the blocking of Google Sites services in Turkey at the instigation of the Turkish government).

National laws in Member States permitting the blocking of internet access will have to be compliant with EU legislation and are ultimately subject to judicial review by the ECJ and ECHR. This calls to mind the so-called 'three-strikes' piracy law (or Hadopi law) enacted in France in 2009, which permitted the blocking of an individual's internet access upon repeated copyright infringements in respect of online content. The controversial access-blocking penalty under this law, although never tested by EU courts for compliance with fundamental freedoms, was reversed by the French government in 2013. In the UK, the Digital Economy Act also provides a basis to implement technical measures blocking or restricting an individual's internet access in the event of repetitive online copyright infringements although these anti-piracy measures have to date not been implemented.

Exception 2: Security protection

Within the ambit of security protection, the monitoring and filtering of traffic to protect against malware and cyber attacks using network-level firewalls and other security measures are not an infringement of net neutrality regulations. Of course, the implementation of security measures that may impact net neutrality pursuant to relevant security and service continuity obligations imposed by EU and national legislation, such as contained in the e-Privacy Directive 2002/58/EC, the Universal Service Directive 2002/22/EC and the forthcoming Directive on Network and Information Security, are also covered by the exception for compliance with laws and orders discussed in the above.

Exception 3: Network congestion

The third exception category permits a provider to take measures going beyond reasonable traffic management measures in order to avoid or mitigate the effects of temporary or exceptional network congestion. Under the Regulation, temporary congestion is understood to comprise an overflow of network transmission capacity during a short period of time due to a sudden increase in the number of users in addition to the regular users, or a sudden increase in demand for specific content, applications or services. Mobile networks are in particular considered susceptible to temporary congestion, as they are subject to more variable conditions than fixed line networks, including physical coverage impediments and a variable number of active users with changing locations.

Although temporary congestions might be predictable – which distinguishes them from exceptional congestions – the circumstances leading to the congestion might not recur so often or for such duration as to economically justify an expansion of network capacity. Exceptional congestion is understood to mean unpredictable and unavoidable congestion, which might be caused by technical failures or emergency situations resulting from circumstances beyond a provider's reasonable control.

It is stated in the Regulation (recital 15) that recurring and more long-lasting congestion should not benefit from this exception, but should be addressed through investments in network capacity. In this context, the Regulation (Art. 5(1)) authorizes national regulatory authorities to impose on internet access service providers requirements with regard to technical characteristics, minimum quality of service requirements and other appropriate and necessary measures in order to promote the continued availability of non-discriminatory internet access at levels of quality that reflect technological advancements.

Spam and parental controls

Notably, a fourth exception originally included in the proposed text of the Regulation, which allowed internet access service providers to block unsolicited commercial communications (spam) and to implement parental controls at the explicit prior request or with the explicit prior consent of end-users, was stricken during European Council negotiations. Given the limited scope of exceptions to traffic management measures involving the blocking of traffic, it would appear then that network-embedded filtering of online content by an internet access service provider is not permitted, at least not by default as is the case with certain providers in the United Kingdom which require end-users to opt-out of default filtering of content deemed unsuitable for minors. These practices will have to be adjusted.

Whether such network-embedded filtering can be made available to end-users on an individual opt-in basis is debatable. A strict interpretation of the Regulation appears to disallow any monitoring of the contents of internet traffic by access providers and any blocking or filtering beyond the three defined exception categories. Arguably, however, the implementation of traffic filtering measures by an access provider on the basis of the informed, explicit, voluntary and revocable request of an end-user does not go against the prime objective of the net neutrality rules to safeguard end-users' freedom of choice. This would not appear to be fundamentally different from the situation in which an end-user purchases and uses its own (device-embedded, browser- or web-based) filtering software, a right which is not affected by the Regulation. A practical problem though, may be to administer and technically implement the filtering choice of each individual end-user where multiple users are serviced under the same internet access subscription or connection.

Commercial considerations

The Regulation clearly does not permit the use of traffic management measures to treat certain applications and services more favorably in a technical sense for commercial considerations (*eg*, by blocking or throttling access to competing applications and services). However, the net neutrality rules do not contain an outright prohibition for internet access providers to offer commercial incentives to promote the use of certain online applications and services above others, for instance by including certain applications and services for free in internet access subscriptions, applying zero rating (or toll free/sponsored data schemes) or otherwise offering financial incentives to end-users to use specific applications and services.

In the Regulation (recital 7), the line is drawn where (internet access) agreements or the commercial practices of internet access providers would limit the end-users' exercise of their rights to access and distribute information and content and to use and provide applications and services of their choice, in the sense that such agreements and commercial practices would "*by reason of their scale, lead to situations where end-users' choice is materially reduced in practice*". The Regulation points out that the assessment of agreements and commercial practices should therefore take into account the respective market positions of the internet access service providers and of the providers of content, applications and services that are involved. There is cause for national regulatory and other competent authorities to intervene when agreements or commercial practices would result in the undermining of "*the essence of the end-users' rights*".

This makes sense, recognizing that the principal aim of the net neutrality rules is to safeguard end-users' freedom of choice and not to operate as an instrument of competition regulation to ensure a commercially level playing field. Market forces may operate freely unless this would compromise the essence of end-users' rights. One might imagine this can be the case if agreements are struck between access providers and providers of online content, applications or services who are so dominant (in terms of

scope of operations, rights to content, financial power or otherwise) as to entirely push from the market competing content, applications or services providers, leading to a *de facto* limitation of end-users' online freedom of choice.

Given this commercial "leeway" and in view of the obligation for Member States to align their national laws with relevant provisions of the Regulation, it would appear that national rules which strictly prohibit internet access providers to differentiate the charges for their internet access services depending on the online services or applications that are offered or used through the access services (such as are currently, for example, maintained in the Netherlands) are not compatible with the Regulation.

Specialized services

Article 3(5) of the Regulation provides that providers of public electronic communication services, including internet access service providers, and providers of content, applications and services are free to offer services other than internet access services which are optimized to meet requirements for a specific level of quality. The Regulation provides the, not very enlightening, examples of "services responding to a public interest" and "new machine-to-machine communication services". In an explanatory fact sheet accompanying the proposal for the Regulation, the European Commission indicated that these "specialized services" are services like IPTV, high-definition videoconferencing or healthcare services like telesurgery, all of which use the internet protocol and the same access network but require a significant quality enhancement or technical guarantees that cannot be ensured in a best-effort open internet offering.

Specialized services may only be offered if the network capacity is sufficient to provide them in addition to internet access services. They may not be usable or offered as a replacement for internet access services, and may not be offered to the detriment of the availability or general quality of internet access services for end-users.

Transparency

The net neutrality rules are flanked by extensive transparency obligations, pursuant to which internet access service providers must publish and include in each internet access contract clear and comprehensible information on:

- the traffic management measures deployed by the provider and their potential impact on the quality of internet access services and the privacy of end-users;
- volume limitations, speed and other quality of service parameters applied by the provider and their potential impact on internet access services and the use of online content, applications and services;
- specialized services offered by the provider and their possible impact on end-user internet access services;
- the minimum, normally available, maximum and advertised download and upload speed of the internet access services in case of fixed networks, or of the estimated maximum and advertised speed in the case of mobile networks, and how significant deviations may impact end-users' rights under the Regulation;
- the remedies available to consumers in the event of continuous or recurring discrepancy between the actual performance of the internet access service as regards speed or other quality of service parameters and the performance indicated in the points above.

The internet access provider is furthermore required to implement transparent, simple and efficient procedures to address end-users' complaints about the internet access services. For internet access service contracts concluded or renewed after 29 November 2015, the Regulation provides that a discrepancy between actual and agreed performance as noted in the above shall, where the discrepancy is established by any monitoring mechanism certified by national regulatory authorities, be deemed to constitute non-conformity of performance, triggering consumer remedies under national law.

Conclusion

Net neutrality is surrounded by conflicting interests and is (therefore) a politically sensitive issue. While telecommunications companies are seeking to reposition themselves in the communications value chain by leveraging their control over the internet access connections, providers of online content, applications and services work to minimize that leverage and maximize their own access to the end-users, arguing for strict net neutrality. In the middle are the end-users demanding high-speed, high-quality online access to everything everywhere and at any time, at the lowest prices and with the option to filter out undesirable content. No wonder then, that the Regulation was some time in the making and is apparently the result of considerable compromise between the EU Member States.

The net neutrality rules certainly go some way in protecting open internet access and are a positive reinforcement of end-users' fundamental freedoms in relation to the internet.

That said, key elements of the rules remain subject to interpretation, including the extent to which internet access service providers:

- can implement end-user requested filtering solutions (to counter spam, enable parental controls, block ads, etc.);
- can offer commercial incentives in their internet access charges that promote the use of particular online services and applications;
- can offer specialized services on top of internet access services; and
- will be obliged to invest in network capacity and technology to ensure minimum quality of service requirements.

It remains to be seen whether Member States will not seek to interpret these elements in different ways, according to their own political agendas. Notably, for example, the Dutch government is seeking to retain its strict price discrimination prohibition in a recent legislative proposal and the UK government is reportedly not amused at all by the prospect of having to rewind the achievements in promoting parental control filtering at a network level by internet access providers.

A diverging application of the net neutrality rules in the various EU Member States will, however, easily lead to a distortion of competition among network operators and providers of online content, applications and services in the Member States. This is apparent if, for instance, zero-rating would be forbidden in one and permitted in another Member State, or if internet access providers would be subject to differing quality of service requirements from one Member State to the other. Hopefully, some level of consistency in the application of the Regulation will be achieved through BEREC (the Body of European Regulators for Electronic Communications), who is charged under the Regulation with issuing guidelines to that effect by 30 August 2016.

Contacts

Jaap Tempelman
T: +31 20 7119 192
E: jaap.tempelman@cliffordchance.com

Richard Jones
T: +44 20 7006 8238
E: richard.jones@cliffordchance.com

Andrei Mikes
T: +31 20 7119 507
E: andrei.mikes@cliffordchance.com