WIK • Report

Study for Broadband Stakeholder Group (BSG)

Review of the Open Internet Codes

Authors:
Dr Martin Waldburger
Dr René Arnold

WIK Wissenschaftliches Institut für Infrastruktur
und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany

Bad Honnef, 16 November 2015

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Contents

Executive summary

The UK has been following a self-regulatory approach to the Open Internet and traffic management since 2011. With the Code of Practice on the Open Internet and the closely associated Code on Traffic Management Transparency (together referred to here as the Codes), the Broadband Stakeholder Group (BSG) has gathered the major Internet Service Providers (ISPs) and mobile virtual network operators (MVNOs)as signatories to the Codes. Taken together, they represent over 90% of UK subscribers on both fixed and mobile contracts. The adjacent Open Internet Forum (OIF) offers an informal platform for exchange on issues among all interested stakeholders.

In light of the Connected Continent Regulation (10788/15) on the Open Internet, it is an opportune moment to review the UK Codes of Practice and in particular explore their effectiveness and compliance with the Connected Continent Regulation with the aim to develop the Codes further.

Effectiveness of the Codes

Our research showed that there is no single measure for the Codes' effectiveness as they aim to establish three general principles revolving around the Open Internet.

The first principle is the *prevalence of full internet access products* that allow end-users to access all legal content and services on the internet. Our review of ISPs' Internet Access Service (IAS) products found an obvious prevalence of full IAS products in the UK. In fact, almost all UK internet users have virtually full access to the internet. However, some ISPs block unsolicited services like spam to improve consumers' quality of experience. No signatory to the Codes continuously slows down any traffic on their network. Prioritisation of services and content is equally rare.

The second principle defines the *absence of negative discrimination of content and services*, especially when provided by third parties. Since the Codes were established, there have been no official complaints about negative discrimination of an Over-The-Top (OTT) service. Our review of IAS products indicated that almost no IAS product blocks or slows down specific content or services during peak times, which would indicate negative discrimination. This is a substantial change from the situation before the Codes were established, when negative discrimination had been broadly discussed in the media as a major issue that UK consumers face. Reasonable traffic management, for instance, to mitigate congestion is applied by UK ISPs.

Third, *transparency and competition* are established by the Key Fact Indicators (KFIs) defined in the self-regulation on traffic management. KFIs are an effective way to make traffic management measures transparent for consumers. Complemented by the fierce competition in the UK, any ISP that does not commit to the Codes may in turn be susceptible to consumer switching. This, alongside high levels of innovation by providers of British OTT services like BBC iPlayer, All4 and ITV Player, has helped

support a market environment where OTT services can thrive. In fact, UK consumers have the broadest choice of music and video streaming services across OECD countries, and OTT services providing services functionally similar to typical electronic communication products thrive in the UK. OTT services, enabled by an Open Internet, appear in turn to have driven demand for broadband connectivity and upgrades.[1]

Ofcom's evaluation of the effectiveness of the Codes concurs with our findings.

Compliance with the Connected Continent Regulation

The in-depth compliance analysis conducted in the context of this study revealed that the vast majority of concepts and principles of the Codes comply with the Regulation. This finding is reflected by the signatories who believe a positive aspect of the upcoming Regulation is that they adopt some of the underlying principles of the Codes.

There are only two issues where the Regulation implies additional duties or prerequisites for ISPs: 1) *the general principle that legal content, applications and services or categories thereof should not be blocked,* and 2) *the right to develop and offer managed services*. In these cases, the Codes can easily be altered to address the gaps that exist as compared to the Regulation's requirements.

On the other hand, the Codes also add value over and above the requirements laid out in the Regulation. ISPs' voluntary commitment to *make full IAS the norm in the UK* market is one of the Codes' cornerstones, but it is not reflected in the Regulation in the same way. With social norms and conduct of peers instead of a prescriptive set of rules being at the heart of the self-regulatory approach, one may expect this commitment to be more effective than governmental regulation which is often perceived as arbitrary by businesses. Equally, *transparency about traffic management for consumers* is dealt with more effectively by the Codes as compared to the Regulation, which requires such information to be described in the terms and conditions. The KFIs, however, bring the most important information upfront and make it comparable for consumers. In principle, this should facilitate switching and in turn increase competition in the UK. Finally, the Codes also cover *alternative products (other than IAS)* proactively whereas the Regulation remains unclear.

1 40% of audiences say that BBC iPlayer was "one of the reasons I like having broadband at home", and 13% said it was "one of the reasons I got broadband at home in the first place". The first percentage is based on a 2015 average of data from Pulse by GfK for the BBC; the second percentage is from Pulse by GfK for the BBC, based on 777 UK adults who used iPlayer on a computer in the last three months (October 2013: six years after the launch of iPlayer in 2007). See also, for example, WIK (2015): Competition and investment: An analysis of the drivers for superfast broadband. The WIK study found that "In general, regulatory factors appear to date to have had less influence over NGA coverage and take-up than market-based factors such as infrastructure competition or online video".

The way forward for the Codes

In sum, this review found the Codes to be compliant with the Regulation. There is some potential to update the Codes, in light of current and expected market developments. These include the Internet of Things (IoT), demand for innovative plans for consumers, and the potential for diverging incentives between ISPs and Content and Application Providers (CAPs)[2] as well as novel modes of new cooperation.

First and foremost, as the Regulation addresses both the Open Internet and measures to ensure transparency about traffic management for consumers, it seems appropriate to merge the two Codes into one. Identical signatories to the Codes make this straightforward.

Second, the Codes should offer UK-specific guidance to signatories, alongside the Body of European Regulators for Electronic Communications' (BEREC) guidelines, where the Regulation fails to do so. Thus, the Codes could specify a set of agreed principles and voluntary commitments as regards the offering of managed services and alternative services relevant for IoT roll-out, for example. Furthermore, the Codes could specify a set of agreed principles and voluntary commitments as regards reasonable traffic management practices.

Third, with the KFIs, the Codes have already outperformed the Regulation as regards consumer information and increased transparency for all stakeholders. We recommend building on this strength of the existing Code and developing the KFIs further in light of the results of Ofcom's and BEREC's extensive consumer research into this issue.

Finally, it is sensible to maintain the parts of the Codes referring to Ofcom's monitoring commitments as well as the voluntary process for raising concerns as they will remain relevant for signatories. Over and above the official complaint process, it should be noted that the continuous exchange in the OIF has helped significantly to achieve mutual understanding of good conduct and establish an atmosphere of trust between ISPs and CAPs. This will continue to be an important forum to discuss some of the emerging risks and opportunities in relation to the Open Internet which fall outside the Regulation.

2 As mass market IPTV becomes closer to becoming mainstream, Ofcom have noted that "the relationship between the ISPs as distribution platforms and broadcasters as content providers has not yet been tested. For example, there could be a concern that the ISPs could act as new gatekeepers over the distribution of broadcast services over IP. Especially if content providers have to rely on their managed services to provide a quality TV experience." Cf. Ofcom (2014): The future of free to view TV. A discussion document, Figure 5.3.

1 Introduction

The UK has been following a self-regulatory approach regarding the Open Internet[3] and traffic management since 2011. With the Code of Practice on the Open Internet[4] and the closely associated Code on Traffic Management Transparency,[5] (together referred to here as the Codes) the Broadband Stakeholder Group (BSG) has gathered the major Internet Service Providers (ISPs) and mobile virtual network operators (MVNOs)s as signatories to the Codes. Taken together, they represent over 90% of UK subscribers on both fixed and mobile contracts. The adjacent Open Internet Forum (OIF) offers an informal platform for exchange on issues among all interested stakeholders. The OIF plays an important role in the process of discussing and implementing the Codes. It is able to fulfil this role as it currently reaches more than 60 organisations representing a wide variety of stakeholders. It should be noted that only around a fifth of the organisations in the OIF are ISPs and network operators, thus signatories of the Codes. A similar number of organisations are from the content and media sector. Another fifth consists of advocacy groups.[6] Government/administration, network equipment, consultancy, e-commerce and mobile devices each represent at least 5% of participants in the OIF with. Furthermore, the OIF gathers organisations in IT solutions, price comparison, social networking, software and domain names.

In light of the adoption of the Connected Continent Regulation (10788/15)[7] and new provisions relating to the Open Internet,[8] it is an opportune moment to review the UK Codes of Practice. The review of the Codes sets out to fulfil the following objectives:

- Assess the effectiveness of the Codes, their principles and their impact on UK users.
- Assess the value of the UK's self-regulatory approach in the context of the Connected Continent Regulation.
- Assess the compliance of the Codes in light of the Regulation.
- Propose improvements to the two Codes.
- Consider whether the Codes could or should be combined.

---

3 This is often referred to in the public debate in relation to the net neutrality principle.

4 See http://www.broadbanduk.org/wp-content/uploads/2015/07/BSG-Open-Internet-Code-of-Practice-amended-November-2014.pdf – reproduced in Annex A to this report.

5 See http://www.broadbanduk.org/wp-content/uploads/2013/08/Voluntary-industry-code-of-practice-on-traffic-management-transparency-on-broadband-services-updated-version-May-2013.pdf – reproduced in Annex B to this report.

6 Representing the interests of consumers, employers, civil society, commercial broadcasters, network operators, ISPs, regional and local initiatives to build NGA (Next-Generation Access), VoIP (Voice over IP) and OTT (Over-the-Top) application providers, the UK's technology and gaming industries.

7 See http://data.consilium.europa.eu/doc/document/ST-10788-2015-INIT/en/pdf.

8 In addition to provisions regarding the Open Internet, the Regulation covers aspects of mobile roaming, which is not addressed in any way in this study.

The review was carried out in close coordination with the BSG and the signatories of the Codes. This is also reflected in the method for the review, which included both a short questionnaire[9] to consult all members of the OIF and additional telephone interviews with OIF members and signatories of the Codes.[10] Extensive desk research and a compliance analysis, including a review by a legal expert,[11] comprised the major research methods employed for this review.

The present report reflects our findings and proposes changes to the Codes in order to ensure that they are compliant with the Regulation and fit for the foreseeable future. The report is structured as follows. We begin by contextualising our task in the history of Open Internet regulation in the UK, the wider frame of net neutrality regulation as well as the current Connected Continent Regulation. This is followed by highlighting and discussing the effectiveness of the Codes in the UK. The report proceeds with a section that documents the outcome of our in-depth compliance analysis of the Codes and the Regulation. The report culminates in a vision on how to develop the Codes based on the insights gathered and in consideration of relevant marked developments.

9 The questionnaire was sent out on 25 August 2015 by Matthew Evans and Samira Gazzane. Reminders were sent and another personal reminder was given at the OIF meeting on 17 September 2015. In total, we received six responses to the questionnaire.

10 We aimed to cover views from all types of stakeholders, e.g. ISPs, Content and Application Providers (CAPs) and consumer watchdog organisations. In the interviews, we spoke to the following stakeholders: BBC, BT, Three, UKIE and Virgin Media. We also spoke with DCMS and Ofcom.

11 Maxime Piron, Centre for Computer Research, Law and Society (CRIDS), University of Namur, Belgium.

2 Context

In this section, we contextualise our review of the Codes. First, we describe briefly the history of the Codes in the UK and the motivation behind them. Second, we discuss the current perspective on the Codes in the UK. Finally, we link these insights to the broader context of the upcoming Connected Continent Regulation on the Open Internet as part of the Telecoms Single Market package.

The public debate on the Open Internet and net neutrality – including in North America – is still relatively new. In 2010, with a Federal Communications Commission decision in place that allowed paid prioritisation,[12] the public debate was also started in the UK. For instance, 19 organisations from the UK sent an open letter to Ed Vaizey MP demanding that the UK drew up legislation to secure the Open Internet and ban discriminatory business practices. The letter also asked the Government to require Ofcom to closely monitor the market and react accordingly if fair practices of traffic management were not adhered to by ISPs. In addition to "[p]rotecting the Open Internet through a judicious implementation of the new EU legislation for electronic communications", the letter demanded an effective self-regulatory approach.[13]

Furthermore, before the Codes were drawn up and signed, there had been allegations of throttling and blocking by ISPs in the UK. For instance, the BBC accused BT of throttling their iPlayer, while BT commented that the BBC should not expect a free ride for their data-hungry service.[14] On mobile networks, however, blocking and throttling, especially with regards to VoIP (Voice over IP) and P2P (Peer-to-Peer) traffic, appeared to be a widespread phenomenon in 2010/11.[15]

In this context, the first Code of Practice on transparency of traffic management was signed in 2011. The Code was the result of a complex and intense process facilitated by the BSG. The process in itself deserves to be acknowledged as a significant achievement as it ultimately brought content and network providers closer together. In addition to drafting the Code, the BSG's role included coordinating the involved stakeholders. The support Government and Ofcom provided at that stage contributed substantially to the successful completion of the Code. The Code addressed the concern that the public would not be informed about which traffic management practices were used. Through Key Fact Indicators (KFIs), consumers were able to learn the specific terms and conditions that their ISP applied for traffic management. The KFIs

12 BBC (2010): Q&A – The network neutrality debate. Available at: http://www.bbc.com/news/technology-10924691.

13 WIRED (2010): UK web companies demand net neutrality legislation. Available at: http://www.wired.co.uk/news/archive/2010-12/02/uk-web-companies-demand-net-neutrality-legislation – the full letter is reproduced in Annex C to this report.

14 The Telegraph (2010): Ofcom to examine UK net neutrality. Available at: http://www.telegraph.co.uk/technology/broadband/7366583/Ofcom-to-examine-UK-net-neutrality.html and Ars Technica (2009): What a non-neutral 'net looks like, UK-style. Available at: http://arstechnica.com/tech-policy/2009/06/what-a-non-neutral-net-looks-like/.

15 BBC (2011): ISPs defend plans for two-tier net. Available at: http://www.bbc.com/news/technology-12791376.

further allowed consumers to compare ISPs' offers directly and easily as they come in a standardised format. While this was perceived by the public as a step in the right direction, it was still questioned if full disclosure of traffic management practices as opposed to a commitment to the Open Internet would suffice to sustain open and fair competition on the web.[16]

In light of these arguments, the second Code of Practice on the Open Internet was drawn up and signed in 2012. However, at that point, three of the larger UK ISPs did not sign this Code: EE, Virgin Media and Vodafone. They only signed the amended Code in 2015.[17]

Today, the signatories to the Codes of Practice on transparency of traffic management and the Open Internet comprise more than 90% of all broadband subscriptions in the UK. Many supporters of the Codes that are not signatories are members of the BSG and the OIF covering stakeholders who represent primarily Content and Application Providers (CAPs), such as Amazon or the BBC, as well as advocacy groups such as consumer watchdog organisations.

With all relevant UK ISPs having signed the Open Internet Code, the self-regulatory and principles-guided approach has received broad support. For instance, Ed Vaizey (Communications Minister) concluded that the UK was "ahead of the curve" in its approach to ensuring fair competition and innovation online.[18] Furthermore, Jo Connell (Chair of the Communications Consumer Panel) said: "*The Code usefully supports open access to the internet and builds on previous commitments by ISPs to provide transparent information to consumers about their traffic management policies. We are delighted that EE, Virgin and Vodafone have now agreed to become signatories. The Code has gained significant interest internationally as a positive example of industry responding to a developing consumer need.*"[19]

In June 2015, the European Parliament, the European Council and the European Commission finally agreed on a Regulation that covers the Open Internet and mobile roaming. While this Regulation takes on board some of the fundamental concepts of the self-regulatory Codes in the UK,[20] it differs from the Codes because of its legal effects and because its provisions are more detailed and prescriptive than the Codes, which are principle-based.

---

16 Daily Mail (2011): At last, broadband providers agree to reveal how much they restrict your internet connection. Available at: http://www.dailymail.co.uk/sciencetech/article-1366181/Broadband-providers-agree-reveal-restrict-Internet-connection.html#ixzz3nc0D9TaQ.

17 BSG (2015): Remaining ISPs commit to the UK's Open Internet Code. Available at: http://www.broadbanduk.org/2015/01/19/remaining-isps-commit-to-the-uks-open-internet-code/.

18 Quoted in Hirst, D. (2015): Regulating the web: The Open Internet and net neutrality. Briefing Paper No. 7183; May 2015 – House of Commons Library, London, p. 10.

19 BSG (2015): Remaining ISPs commit to the UK's Open Internet Code. Available at: http://www.broadbanduk.org/2015/01/19/remaining-isps-commit-to-the-uks-open-internet-code/.

20 ISPreview (2015): Watered down EU deal to protect open internet and end roaming charges. Available at: http://www.ispreview.co.uk/index.php/2015/06/watered-down-eu-deal-to-protect-open-internet-and-end-roaming-charges.html.

It should also be noted that during negotiations, the UK Government sought to maintain the flexibility that the Open Internet Code of Practice offers, for example by arguing for the retention of protection options, such as parental controls, public WiFi filtering and the Internet Watch Foundation blacklist, currently considered as acceptable exceptions to traffic management. Some of these elements have since been removed from the final political compromise achieved in late June 2015. The legislative process will end in November 2015, once the European Parliament and Council have officially approved it.

Against this backdrop, this is an opportune moment to review the two Codes of self-regulatory practice in the UK. It seems obvious that some amendments to both the Open Internet and Traffic Management Transparency Codes may need to be made to reflect new EU rules (see Section 4). Given that the EU Regulation promotes both transparency of traffic management and the concept of an Open Internet, combining the two Codes into one should also be considered. The analysis and interpretation of the Regulation will be an iterative process, as further guidance from the UK Government and Ofcom might be needed as implementation work progresses. During the implementation stage of the Regulation, the BSG will be providing input to Ofcom and BEREC (Body of European Regulators for Electronic Communications) in the development of guidelines for Member States.

3 The effectiveness of the self-regulatory Codes in the UK

In this section, we demonstrate the effectiveness of the Codes in the UK. To understand the effectiveness of the Codes in depth, we draw from various sources such as press articles, Ofcom communications and journal articles as well as primary research conducted with the signatories of the Codes, CAPs, UK Government, Ofcom and advocacy groups representing consumers and the UK's gaming industry.

Our research showed that there is no single measure for the Codes' effectiveness as they aim to establish three general principles revolving around the Open Internet in the UK and reflecting the specificities of the UK market. These general[21] principles are (1) the prevalence of full internet access products that allow end-users to access all legal content and services on the internet; (2) the absence of negative discrimination of content and services, especially when provided by third parties; and (3) transparency and competition, which go hand in hand in the UK market for electronic communication services. Before we discuss the effectiveness of the Codes in achieving these aims, we begin by drawing on the literature on general characteristics of self-regulatory approaches highlighting some of their key advantages. We close this section with a brief summary of Ofcom's and the signatories' evaluation of the Codes' effectiveness.

3.1 General characteristics of self-regulatory approaches

Self-regulatory approaches have been discussed widely in the literature. Common areas for self-regulation include advertising, alcoholic beverages and environmental practices. Based on a review of the literature conducted by the Information Technology and Innovation Foundation,[22] there are obvious advantages of self-regulation depending on the policy objectives and surrounding framework conditions of the specific case. Self-regulation appears to be particularly efficient, however, for areas where there is rapid evolution of industry practice, many new entrants into the relevant market, and sustained innovation. In such competitive and rapidly changing environments, governmental regulation may unduly burden industry (in particular new entrants), raise production costs for businesses (costs that are ultimately borne by consumers) and create barriers for innovation. Self-regulation tends to be more flexible to accommodate evolutionary (or even disruptive) changes more quickly.[23]

---

21 The detailed compliance analysis, whose outcome is documented in Section 0, builds on these three general principles, but assesses the Codes' compliance on the basis of the specific concepts and principles that underline the respective voluntary commitments that the Codes' signatories agreed to adhere to.

22 Castro, D. (2011): Benefits and limitations of industry self-regulation for online behavioral advertising. Information Technology and Innovation Foundation.

23 Castro, D. (2011): Benefits and limitations of industry self-regulation for online behavioral advertising. Information Technology and Innovation Foundation. Miller, J.C. (1985): The FTC and voluntary standards: Maximizing the net benefits of self-regulation. The Cato Journal.

While this advantage of self-regulation depends strongly on the competitive environment, self-regulation will be more effective compared to governmental regulation as regards sustained internalisation[24] of ethical practices and principles by participating businesses largely independent from the competitive environment. Commonly, self-regulation is based on social norms and conduct of peers instead of a prescriptive set of rules that may be perceived as arbitrary by businesses. Thus, commitment and compliance with self-regulation tends to be better than for governmental regulation.[25]

Beyond commitment and compliance, self-regulation may also benefit from more appropriate rules as they are drawn up by industry experts, who know the background of their respective industry first-hand. Using such a participatory approach and thus a bottom-up design process for regulation usually ensures that regulation is actually applicable and reflects the reality of the industry. It is, however, critical that there is an effective self-policing organisation. Such an organisation should have a complaint resolution process and ideally include stakeholders from diverse areas of the respective industry representing various business models, sizes and interests. Such a forum is likely to investigate and resolve complaints and violations more rapidly than governmental institutions. Furthermore, a common resolution process for complaints may in itself be advantageous as it facilitates exchange and discussion among stakeholders with potentially conflicting interests resulting in better mutual understanding and sustained resolution.[26]

Finally, self-regulation can be particularly efficient when there are many multinational corporations in the respective industry. There may be questions of sovereignty of (in particular national) governmental regulation that are not an issue with self-regulation.[27]

However, there are, of course, also potential problems with self-regulatory approaches. A commonly discussed issue is the so-called free-rider problem. Firms may still profit from the positive perception that it creates for the industry as a whole even if they do not subscribe to the respective self-regulatory Code of Practice.[28] Also, there may be issues that are obviously better regulated by governmental action than self-regulatory approaches. This is the case when regulation relates to issues where strict regulatory action has clear-cut economic or social benefits that due to unilateral business interests

24 Sustained internalisation means that individuals or organisations adopt certain principles and practices and that they act accordingly by themselves, without any need for external pressure or control.

25 Castro, D. (2011): Benefits and limitations of industry self-regulation for online behavioral advertising. Information Technology and Innovation Foundation. Karmel, R. S. (1988): Securities industry self-regulation – Tested by the crash. Washington and Lee Law Review, Volume 45, Issue 4.

26 Castro, D. (2011): Benefits and limitations of industry self-regulation for online behavioral advertising. Information Technology and Innovation Foundation. Michael, D. C. (1993): Federal Agency use of audited self-regulation as a regulatory technique. Administrative Conference of the United States. Campbell, A. J. (1999): Self-regulation and the media. Federal Communications Law Journal, Volume 51, Issue 3.

27 Bernstein, S. and Vashore, B. (2007): Can non-state global governance be legitimate? An analytical framework. Regulation & Governance 1.

28 Hemphill, T. A. (1992): Self-regulating industry behavior: Antitrust limitations and trade association codes of conduct. Journal of Business Ethics 11, no. 12.

across all stakeholders are unlikely to be solved efficiently by the industry themselves, such as cigarette labelling. In any case, regulatory certainty is important for any industry and a precursor for a positive innovation environment.

The Codes fit all the mentioned requirements for which self-regulation has been found to be more effective than governmental regulation. First of all, the Codes have been drawn up by the industry. This accompanying coordination process, facilitated by the BSG, has been and continues to be intense, but the industry-led nature of the process has proven to lead to sustained support. It is equally important that the Codes reflect a fiercely competitive context in the UK, both in terms of internet access and access to applications and content. The Codes have come to exist in a competitive, fast-moving and highly innovative environment, which is a prerequisite for successful self-regulation. The Codes are built on this principle.

3.2 Effectiveness of the Codes' principles

The self-regulatory Codes in the UK establish three overarching principles that enable monitoring of their effectiveness: (1) the prevalence of full internet access products that allow end-users to access all legal content and services on the internet; (2) the absence of negative discrimination of content and services, especially when provided by third parties; and (3) transparency and competition, which go hand in hand in the UK market for electronic communication services. In this section, we discuss each of these principles and the respective achievements facilitated by the Codes of Practice in turn.

The prevalence of full internet access products in the UK is clearly the most important principle that the Codes imply. For this review, we have analysed the KFI tables of the signatories to the Codes. In total, we identified 54 entries in KFI tables that referred either to individual products offered by ISPs or to types of products. However, it is difficult to deduce a fully detailed overview on the level of each and every individual internet access product currently available in the UK.[29] Nonetheless, from our analysis the prevalence of full internet access products is obvious and documented in the following tables.

Before going into detailed considerations regarding the effectiveness of the Codes, it is important to acknowledge the effectiveness of the process for discussing compliance with the Codes. This process takes place among the signatories of the Codes and the participants in the OIF, with the BSG acting in a mediating role by ensuring that KFI tables exist, that these tables are compliant, and by collecting and raising any issues emerging among stakeholders.

29 It should be noted that this exercise would be difficult even if there was a full data set of KFIs on the individual product level. As tariffs and products change continuously, e.g. due to promotions, and the published product characteristics do not necessarily cover special features available in retention pricing, a perfectly complete picture of all products available at a specific point in time is extremely difficult if not impossible to achieve.

Table 3-1 shows a detailed account of which ISPs who are signatories to the Codes block specific content or services. All ISPs offer their customers virtually full access to the internet. Thus, we can confirm the prevalence of full internet access products in the UK. However, it should be mentioned that some ISPs block some services and content to improve consumers' quality of experience, for example by blocking spam.

Table 3-1: Availability of all legal[30] online services and content in the UK (signatories to the Codes)

Signatory	**Full internet access for all products**	**What legal services and content are blocked?**[31]
BT	Yes	n/a
EE	All legal content and services can be accessed by consumers on all EE products	Unsolicited mail i.e. spam is blocked. For mobile contracts, unauthenticated SMTP[32] is blocked
Orange	Yes	n/a
T-Mobile	All legal content and services can be accessed by consumers on all T-Mobile products	Unsolicited mail i.e. spam (unauthenticated SMTP) is blocked. VoIP, FTP,[33] VPN,[34] and tethering are allowed only on the larger mobile phone plans
Giffgaff	All legal content and services can be accessed by consumers on all Giffgaff products	Tethering is blocked
KC	Virtually all legal content and services can be accessed by consumers on all KC products	TCP[35] port 445 is blocked to prevent virus retransmission
O2	Yes	n/a
Plusnet	Yes	n/a

30 Legal services are defined in the Open Internet Code as follows: "Legal services: this definition excludes any service, content, application or protocol that an ISP is required to block by UK law or a court order and child abuse images as informed by the list provided by the Internet Watch Foundation."

31 Blocking for reasons to prevent unsolicited mail is typically proactive. Measures to implement parental control, e.g. contentblock for Vodafone, may be deactivated on request by adult customers.

32 The Simple Mail Transfer Protocol is the standard application layer protocol in the internet for sending (from mail client to mail server) and forwarding (from mail server to mail server) email messages.

33 The File Transfer Protocol is an application layer protocol for transmitting electronic files (uploading or downloading from/to client to/from server) over IP-based networks.

34 Virtual Private Networks form a logical communications network which is accessible only to authorised users within a communications network. They allow a user to access remote network resources via a secure (encrypted) communications tunnel.

35 The Transmission Control Protocol is the standard transport layer protocol for a reliable, connection-oriented, and packet-switched data exchange on the internet.

Sky	Yes[36]	n/a
TalkTalk	Yes	n/a
Tesco Mobile	Yes	n/a
Three	Yes	n/a
Virgin Media	Yes	n/a
Vodafone	Yes (if contentblock is deactivated)	Contentblock blocks adult and gambling content

Table 3-2 illustrates that no signatory to the Codes continuously slows down any traffic on their network.

Table 3-2: Continuous throttling of specific services in the UK (signatories to the Codes)

Signatory	**Are any services, content, applications or protocols always slowed down?**	**If so, what?**
BT	No	n/a
EE	No	n/a
Orange	No	n/a
T-Mobile	No	n/a
Giffgaff	No	n/a
KC	No	n/a
O2	No	n/a
Plusnet	No	n/a
Sky	No	n/a
TalkTalk	No	n/a
Tesco Mobile	No	n/a
Three	No	n/a
Virgin Media	No	n/a
Vodafone	No	n/a

36 Applies for domestic internet access products. Sky also issues a KFI table for Sky WiFi, for which some URLs to inappropriate content are blocked. It should be noted that the commitment to protect children in particular from accessing inappropriate content through a public WiFi network is supported by the signatories. The Codes have been amended in order to make reference to this commitment.

Table 3-3 shows that prioritisation of services and content is also rare amongst signatories to the Codes in the UK. However, traffic management is applied to ensure quality of experience for consumers of bundles that include IPTV. Furthermore, some mobile operators prioritise emergency voice traffic.

Table 3-3: Continuous prioritisation of specific services in the UK (signatories to the Codes)

Signatory	**Are any services, content, applications or protocols always prioritised?**	**If so, what?**
BT	No	n/a
EE	No on mobile plans. Yes on data plans	VoIP calls, online gaming, and certain network services
Orange	No	n/a
T-Mobile	No	n/a
Giffgaff	No	n/a
KC	No	n/a
O2	Yes	Emergency voice traffic
Plusnet	Yes	VoIP and gaming
Sky	No	n/a
TalkTalk	No	n/a
Tesco Mobile	Yes	Emergency voice traffic
Three	No	n/a
Virgin Media	No	n/a
Vodafone	No	n/a

Table 3-4: Delivery of managed services in the UK (signatories to the Codes)

Signatory	**Are any managed services delivered?**	**If so, what?**
BT	Yes	BT Vision traffic
EE	No	n/a
Orange	No	n/a
T-Mobile	No	n/a
Giffgaff	No	n/a
KC	No	n/a

O2	No	n/a
Plusnet	No	n/a
Sky	No	n/a
TalkTalk	Only on broadband and TV bundles	TV multicast traffic
Tesco Mobile	No	n/a
Three	No	n/a
Virgin Media	No	n/a
Vodafone	No	n/a

Data allowances are a common commercial practice employed by ISPs to limit the data usage of their customers. The specific terms and conditions vary substantially across the specific products and may also depend on promotions or retention offers. Thus, it seems impossible to represent them here in a concise table. Our analysis of the information provided by signatories to the Codes in their KFIs as regards allowances shows that they apply mostly for mobile data plans while fixed internet access products are commonly unlimited. Traffic management measures are a common means of enforcing allowances. When the data usage limit is reached,[37] data services are either terminated or throttled. Heavy user policies are exceptional and commonly apply only during peak times or when the data limit has been reached. The ISPs that apply heavy user throttling (Orange, T-Mobile, Giffgaff, O2, Tesco Mobile, Virgin Media) usually detail their measures in their fair usage policies.

Table 3-5: Traffic management practices to optimise network utilisation in the UK (signatories to the Codes)

Signatory	**Is traffic management used during peak hours?**	**Typical peak hours**[38]
BT	No	Weekdays: 16:00–24:00 Weekends: 09:00–24:00
EE	Yes	Weekdays: 08:00–02:00 Weekends: 08:00–02:00
Orange	Yes	Weekdays: 08:00–24:00 Weekends: 08:00–24:00
T-Mobile	Yes	Weekdays: 08:00–02:00 Weekends: 08:00–02:00

37 A 2014 report for the BSG investigating out-of-home internet use in the UK suggests that "[…] many consumers are influenced in their usage by the level of their data allowance – which is rarely exceeded, regardless of its size". Cf. Kenny, R. (2014): Out-of-home use of the internet. Broadband Stakeholder Group. p. 3.

38 Varying formatting is used in the KFI tables of different signatories. We use a unified format (following the 24-hour clock system) in the table for better overview and comparison.

Giffgaff	Yes	Weekdays: 15:00–24:00 Weekends: 15:00–24:00
KC	No	Weekdays: 18:00–24:00[39] Weekends: 18:00–24:00[40]
O2	No	No information available
Plusnet	No	Weekdays: 20:00–22:00 Weekends: 20:00–22:00
Sky	No	Weekdays: 17:00–24:00 Weekends: 00:00–24:00
TalkTalk	No	not specified
Tesco Mobile	No	not specified
Three	Yes	Weekdays: 15:00–24:00 Weekends: 15:00–24:00
Virgin Media	Yes	Weekdays: 16:00–24:00 Weekends: 11:00–24:00
Vodafone	No	not specified

Table 3-5 shows that some providers and in particular mobile ISPs use traffic management during peak times. We conducted an in-depth analysis of the specific traffic management measures taken as regards differentiation of access to:

- Peer-to-Peer (P2P)
- Newsgroups
- Browsing/email
- VoIP
- Gaming
- Audio streaming
- Video streaming
- Music downloads
- Video downloads
- Instant messaging
- Software updates

This analysis indicates that almost no internet access product blocks or slows down specific content or services during peak times. This is a strong indicator that ISPs indeed adhere to the Codes' principle to avoid negative discrimination, i.e. to refrain

39 Except for the Weekday product where peak hours on weekdays are 16:00–08:00.
40 Except for the Weekday product where peak hours on weekends are 16:00–08:00.

from traffic management based on commercial rivalry. Signatories to the Codes in the UK are found to apply reasonable traffic management where the focus is on safeguarding overall quality of experience by dealing with situations of congestion and by protecting the integrity of the network.

An analysis of the public debate and media reports in the UK for the time before the Codes came into existence shows that incidents of negative discrimination were occasionally reported. Nowadays, negative discrimination of services and content is no longer apparent in the UK. The situation has therefore changed markedly from the situation before the Codes were established. As also highlighted in Section 3.2, negative discrimination of content and services online used to be relatively widespread. In particular, ISPs blocked or throttled either data-hungry services such as the BBC iPlayer or services directly competing with their own service offerings such as VoIP on mobile networks. Today, reports of blocking refer most commonly to illegal content. For instance, TalkTalk has recently been reported to be throttling Imgur, a website that allegedly contains child abuse imagery.[41] It was argued that TalkTalk were unduly applying throttling to the whole domain instead of individual URLs, which caused some inconvenience for users.[42] Current reports about unfair traffic management, i.e. discriminatory practices, could not be identified in our desk research.

The most important effect of the Codes, however, relates to the transparency established by introducing KFIs into the market. Complemented by the fierce competition that exists in the UK market for electronic communications on both the wholesale and end-user levels, the Codes have had a marked impact.

First and foremost, any ISP that does not sign the Codes of Practice appears to be exposed to a reputational risk. There is substantial public pressure for any ISP to commit to the Codes of Practice and non-conformity may be interpreted negatively, for example that the ISP is using undue or even unfair traffic management practices.

Second, as consumers can switch their ISP easily and are likely to shy away from ISPs that block or throttle legal content and/or applications,[43] competitive pressures seem to be working. Several signatories mentioned that ISPs have been monitoring their competitors' behaviour as documented in the KFIs. When an ISP signalled changed behaviour in their KFI table, other ISPs would react accordingly and amend their own KFIs. This reflects in our analysis of KFIs in the UK in the above, where we found that there is in fact almost no Internet Access Service (IAS) product that still includes traffic

41 In instances like this, it is important to recognise the trade-off between protection of minors, which is a key UK Government goal, and Open Internet principles.

42 Wired (2014): TalkTalk is throttling Imgur. Available at: http://www.wired.co.uk/news/archive/2014-04/01/talktalk-throttling-imgur.

43 Arnold, R.; Waldburger, M.; Morasch, B.; Schmid, F.; Schneider; A.; Cilli, V.; van der Peijl, S. & Wauters, P. (2015): The value of network neutrality to European consumers – Full results report. Body of European Regulators of Electronic Communications. Riga. Arnold, R.; Waldburger, M.; Morasch, B.; Schmid, F.; Schneider; A.; Cilli, V.; van der Peijl, S. & Wauters, P. (2015): The value of network neutrality to European consumers – Summary report. Body of European Regulators of Electronic Communications. Riga.

management practices apart from the ones that ensure the functioning of the network. This development is very much in line with the expectations drawn from the literature in Section 3.1 on general characteristics of self-regulatory approaches. Against this backdrop, it is not surprising that consumers in the UK today commonly expect their IAS to be unrestricted and usually also unlimited (as regards data volume).

The most obvious indication of whether the Codes of Practice are effective is to analyse the availability of and consumer satisfaction with Over-The-Top (OTT) services in the UK. If the Codes are efficient, one would also expect a competitive market for OTT services in which those OTT services that offer services similar to the ones offered by ISPs directly can thrive. This complements the role of OTT providers themselves who, by providing attractive innovative services which UK consumers love, have to date helped disincentivise broadband providers from discriminating against the services consumers have paid for connectivity to access. A first indication for the Codes' effectiveness in this respect may be taken from the fact that so far there has not been a single official complaint under the procedure established by the Codes.[44] Analysis of the OTT services market in the UK further supports the idea that the Codes have been effective in sustaining healthy competition among various OTTs as well as between OTTs and ISPs.

This analysis clearly shows a strongly competitive environment of OTT services in the UK. Legitimate online music streaming has grown substantially over recent years. In the UK, consumers can choose between 62 legal online music services[45] and can access all four major commercial audio-visual content platforms (Google, iTunes, Netflix, Amazon Prime Instant Video).[46] This is a significantly better variety than in most OECD countries. As regards OTT services that directly compete with services offered by ISPs, Ofcom data shows that similar to other European markets, the average number of SMSs (text messages) has been decreasing sharply since WhatsApp and similar messaging services became popular with consumers. Concretely, the average number of SMSs sent by UK users reduced by 44% on average for pre-paid users and 27% on average for pay monthly users respectively between 2011 and 2014.[47] Equally, VoIP has become a normal means of communication for a significant share of UK consumers. It is particularly popular with younger consumers, and smartphones have become the most important device to make such VoIP calls.[48] This popularity is mirrored by a decrease in minutes of outbound voice calls per user by 29% on fixed lines and 10% on mobile (pay monthly) contracts. The number of outbound calls remained more or less stable for pre-paid mobile contracts during the same period.[49]

---

44 It should be noted that there has been one case where a complaint was filed informally among the members of the OIF. This issue was quickly resolved outside the official complaints procedure.
45 Intellectual Property Office (2015): International comparison of approaches to online copyright infringement: Final report. A Study by BOP Consulting and DotEcon. Report 2015/40.
46 Ibid. and own research.
47 Ofcom (2015): The communications market report.
48 Ibid.
49 Ibid.

The UK also has a very successful Video-On-Demand market: “Out of Europe’s top five economies, the UK has both the broadest free-to-air catch-up viewing and the strongest commercial revenues – more than two-and-a half times greater than the next biggest market.”[50]

3.3 Ofcom’s evaluation

Ofcom have taken on monitoring commitments for the signatory ISPs’ adherence to the Codes and in particular in relation to their efforts to make traffic management measures transparent to consumers.[51] Ofcom have documented their evaluation in their latest infrastructure report.[52]

Ofcom’s findings can be summarised as follows:

- “Unlimited packages are popular: approximately 80% of fixed broadband customers are subscribed to uncapped packages.”[53]
- “Most mobile operators impose data caps on some of their packages.”[54]
- “Traffic management is used by operators to control the speed of data transfer for certain applications or services in order to manage network capacity use. It is most often used where congestion occurs – at particularly busy times, or busy parts of the network. This can mean giving priority to services that are time-sensitive (like VoIP) and de-prioritising and/or actively slowing down services that are less time-dependent, such as peer-to-peer (P2P) traffic.
  The type of traffic management employed varies across ISPs. Many ISPs do not apply traffic management and may advertise their service as ‘truly unlimited’, both in terms of data use and throttling of certain services (i.e. reducing data speeds for certain services).[55] Others apply traffic management in some form, sometimes to different degrees across different broadband packages. In some packages, particular types of traffic are given greater priority, and consumers who particularly value a type of service can choose packages that prioritise such traffic. A common form of traffic management is to place restrictions on P2P[56] services such as BitTorrent. This is because the design of some P2P software

50 BBC (2015): Public service content in a connected society. Clause 2.42. Numbers based on Ofcom (2014): International Communications Market Report.
51 Ofcom’s approach to traffic management and net neutrality dates back to 2010, thus before the Traffic Management Code (2011) and the Open Internet Code (2012) had been established. It highlights that “[w]hilst traffic management potentially offers some benefits to consumers there are also concerns that firms could use traffic management anti-competitively”. Ofcom have maintained the approach to date. It is documented in detail at http://stakeholders.ofcom.org.uk/consultations/net-neutrality/.
52 Ofcom (2014): Infrastructure report 2014.
53 Ibid., p. 156.
54 Ibid., p. 156.
55 Although network congestion may still mean that performance for customers can degrade, particularly during peak load periods.
56 Peer-to-peer is a distributed application that uses end-users’ computers as nodes to deliver service applications.

increases data use across a network to fill the available capacity. This can degrade performance for other applications or users sharing the same capacity. Furthermore, P2P downloads are not typically as time-dependent as other applications (such as music or video streaming, gaming and VoIP). In controlling P2P traffic, ISPs and operators can keep network infrastructure costs down without adversely affecting the typical user experience. However, the impact of traffic management on users of P2P services can be significant. In some cases speeds of P2P traffic can be reduced to a fraction of the speed of other traffic on the network."

- "MNOs [mobile network operators] in particular have been known to impose restrictions on the use of VoIP. For example, in the past, Vodafone UK customers were able to use VoIP services only on the more expensive packages. However, traffic management policies and usage restrictions are evolving over time in response to changing customer behaviour and competition in the marketplace. VoIP and video-calling applications such as Viber, Google Hangouts, Skype and Facetime are becoming increasingly popular among consumers."[57]
- "UK MNOs now have stopped offering packages with VoIP blocks; Vodafone[58] and EE are now signatories to the Open Internet Code of Practice. Virgin Media has also joined the Code, so all major fixed ISPs are also covered. We welcome these positive developments in transparency."[59]
- "We have reviewed the KFIs, and asked communications providers to confirm that they adhere to them. Our conclusion is that, broadly, transparency about traffic management practices has improved, and in general traffic management policies are less restrictive than previously. In particular, MNOs have dropped specific service blocks on mainstream packages."[60]

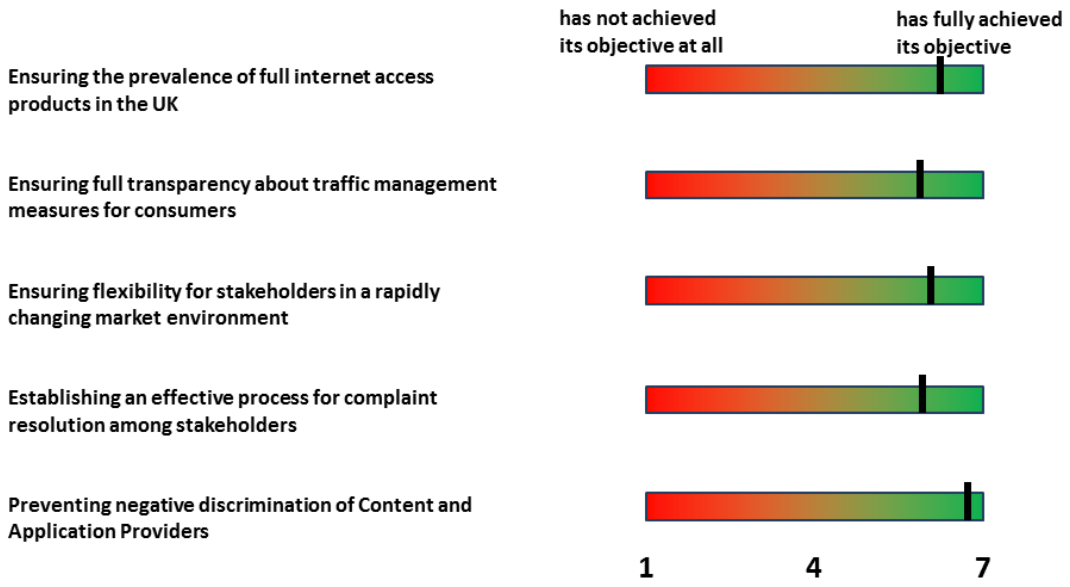
Thus, in essence, Ofcom evaluate the effectiveness of the Codes of Practice to be positive as they conclude in the 2014 infrastructure report that the signatories to the Codes "[…] are committed to an effective self-regulatory model, a key part of Government policy on Net Neutrality".[61]

57 Ofcom (2014): Communications market report.
58 Vodafone has abandoned VoIP restrictions, but it continues to block VoIP on relevant legacy contracts that pre-date July 2014.
59 Ofcom (2014): Infrastructure report 2014. pp. 156–157.
60 Ibid., p. 158.
61 Ibid., p. 153.

3.4 Signatories' evaluation of the Codes' effectiveness

For the purpose of this review, we asked the signatories of the Codes to participate in a short survey[62] that comprised both closed and open questions about the Codes' effectiveness. Figure 3-1 depicts the average responses we received for the closed questions (on a seven point bipolar Likert-type scale).

Figure 3-1: Respondents' average rating of the Codes' effectiveness



Overall, the responses suggest that signatories to the Codes find that they have been very effective. They most strongly agree that they have been effective in preventing discrimination of CAPs in the UK. This response is in line with our finding in the previous section that in fact services provided by CAPs thrive in the UK market and are able to compete with services offered by ISPs directly. The item "Ensuring the prevalence of full internet access products in the UK" achieved almost the same level of agreement from signatories. This is also reflected in the analysis of the KFIs for the most relevant products offered by signatories to the Codes in the UK, where we confirmed a strong prevalence of such products. The remaining items "Ensuring full transparency about traffic management measures for consumers", "Ensuring flexibility for stakeholders in a rapidly changing market environment" and "Establishing an effective process for complaint resolution among stakeholders" all received high agreement by signatories as regards their effectiveness, albeit slightly less than the two items discussed previously. The stakeholders' responses[63] given to the open questions in the questionnaire as well as in the telephone interviews conducted by us shed some light on the reasons behind this result.

62 In total, six out of 13 signatories of the Open Internet Code of Practice completed the questionnaire.
63 Stakeholders from the BSG and the OIF.

As regards transparency for consumers based on the KFIs, some respondents were somewhat doubtful as to whether these would actually be an effective way of informing consumers about traffic management. Respondents in particular referred to the results of the Kantar study[64] on consumer preferences for and perceptions of ISPs' offers for fixed and mobile internet access with a specific perspective on KFIs' merits that in their view indicated that KFIs are in fact not as approachable and comprehensible as they had been intended to be. We discuss this further in the following section in light of results from our own study commissioned by BEREC[65] and other relevant literature. In the final section of this report, we also provide recommendations on how to further develop the KFIs based on our results from the BEREC study and other insights gathered in the UK.

As regards the flexibility of the Codes, all but one[66] respondent acknowledged the self-regulatory approach in the UK as providing the necessary degree of flexibility to adapt to changes in a dynamic and competitive market environment. Respondents mentioned that this may imply a variety of activities, such as ISPs altering their practices flexibly according to changing operational needs, ISPs developing and offering innovative managed services and/or alternative products for consumers according to changing demand in the market, and ISPs in general ensuring a good experience for end-users in response to changing service offerings and end-user expectations. The Codes were characterised by respondents as being highly effective for offering the desired degree of flexibility since they are perceived to provide an unbureaucratic framework with clear and established procedures and contact points. One respondent emphasised in addition that the voluntary, self-regulatory nature of the Open Internet Code is a driver for flexibility since it "[…] has been agreed to by the providers, who are best at knowing their market, its evolution, and how best to achieve the goals set out in the Codes in this context".

Finally, regarding the complaint process, respondents mentioned that it has never really been tested. This, on the one hand, was interpreted positively and similar to our interpretation in the previous section, i.e. that the Codes and process of drawing up the Codes has resulted in sustained exchange and discussions among all stakeholders involved. This in turn has facilitated mutual understanding and the possibility to resolve minor conflicts informally and quickly. On the other hand, it was argued that without having handled an official complaint, the actual effectiveness of the complaint process is unknown.

---

64 Kantar Media (2013): Transparency in internet traffic management. Report prepared for Ofcom.

65 Arnold, R.; Waldburger, M.; Morasch, B.; Schmid, F.; Schneider; A.; Cilli, V.; van der Peijl, S. & Wauters, P. (2015): The value of network neutrality to European consumers – Full results report. Body of European Regulators of Electronic Communications. Riga.; Arnold, R.; Waldburger, M.; Morasch, B.; Schmid, F.; Schneider; A.; Cilli, V.; van der Peijl, S. & Wauters, P. (2015): The value of network neutrality to European consumers – Summary report. Body of European Regulators of Electronic Communications. Riga.

66 One respondent stated a neutral position on this aspect.

Otherwise, the responses to the open questions as well as during the interviews were by and large supportive of the Codes' effectiveness and relevance in an environment that is due to change in line with the upcoming Connected Continent Regulation. In fact, the responses reflected many of the results that we have presented in this report so far. Most prominently, participants in the survey and the interviews mentioned the following points as positive elements of the Codes:

- The principle-based nature of the Codes that build on social norms and conduct of peers instead of a prescriptive set of rules.
- The potential to renegotiate the terms of the Codes with all signatories to adapt to future market developments. It has been highlighted though that the phrasing of the Codes has remained largely unchanged since their inception, which was interpreted as an indication of their efficacy.
- Open and transparent approach to offering products other than full internet access products.
- Process of exchange and discussion in drawing up of the Codes from the bottom-up and also continued exchange of thoughts and positions in the OIF. This process has facilitated mutual understanding between ISPs and OTTs greatly and has led to informal resolution or avoidance of conflicts that may have arisen under a more prescriptive top-down regulation regime.
- The Codes, in particular the Traffic Management Transparency Code has facilitated fair competition and a level playing field for all signatories. It was added that they have been an effective facilitator in making full internet access products the norm in the UK consumer market for broadband services.
- It has registered positively with signatories that the upcoming Regulation adopts some of the underlying principles of the Codes.

4 Compliance analysis of the Codes and the EU Regulation

The provisions of the Connected Continent Regulation (10788/15) on an Open Internet are expected to apply from 30 April 2016. In addition, BEREC will develop "guidelines for the implementation of the obligations of national regulatory authorities under" Article 5, which refers to supervision and enforcement. The BEREC guidelines are expected to be available in August 2016.[67]

In light of the Regulation and in anticipation of the BEREC guidelines, this section analyses the provisions of the Open Internet Code of Practice and the Traffic Management Transparency Code of Practice for their degree of compliance with the respective provisions of the Regulation. The analysis is structured along the concepts and principles that underline the commitments of both Codes. Depending on the specific degree of compliance found, the relevance of the concept or principle in question is considered.

4.1 Commitment 1 of the Open Internet Code of Practice

4.1.1 Concept of the Open Internet

The concept of the Open Internet relates closely to the definition of "best-efforts" internet access[68] provided in the glossary section of the Code. While the definition is largely in line with Article 3(3)[69] of the Regulation, it may need to be altered. The use of "attempt" and "more or less equal terms" is problematic and risks the definition being deemed non-compliant with Article 3(3).[70] In case "more or less" should not be removed from the definition, though different wording should be found, Recital 8[71] of the Regulation may give direction as to how.

---

67 The BEREC guidelines are supposed to be available nine months after the Regulation enters into force. The Regulation is expected to enter into force by publication in the Official Journal in November 2015 (entry into force is not to be confused with the time when the Regulation's provisions become applicable, which will be on 30 April 2016). The nine-month time limit implies that the BEREC guidelines need to be available by August 2016.

68 "'Best-efforts' internet access: as articulated in Ofcom's document, best efforts operates on the principle by which ISPs attempt to convey all traffic on more or less equal terms. This results in an 'open internet' with no specific services being hindered or blocked, although some may need to be managed during times of congestion."

69 "Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used." Note that the Regulation uses the specific terminology of the Open Internet in recitals, headings of articles and in the title of the Regulation, while the respective provisions in articles refrain from using it.

70 Ofcom guidance on the interpretation of these terms is needed as they relate to Ofcom's approach to net neutrality as outlined in a 2011 statement; see http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/.

71 "According to general principles of Union law and settled case-law, comparable situations should not be treated differently and different situations should not be treated in the same way unless such treatment is objectively justified."

4.1.2 General principle that legal content, applications and services, or categories thereof should not be blocked

The general principle of the Code is reflected in the Regulation. When focusing on the intended effect of the principle, namely that end-users have access to legal content, applications and services, the Code is consistent with the Regulation. There are, however, differences to be considered as to how the Code and the Regulation intend to achieve this objective.

The Regulation in Article 3(1) grants end-users the explicit right to access (and distribute) content and to use (and provide) services and applications, whereas this right may be limited by law at Union or Member State level as regards the definition of what is lawful content, services or applications. The Code refrains from issuing any such right as it addresses the intended effect via ISP commitments. It relates to the concept of full internet access by establishing[72] that full internet access means a service that permits a consumer to access any legal content, applications or services.

Although rights and duties (instruments of the Regulation) and self-commitments (instruments of the Codes) are different legal instruments, the effect created by the Code's self-commitments can be considered in line – i.e. they comply – with the right given to end-users as part of the Regulation. The Regulation, however, goes further than the Code. The Code understands the commitment to permit access to legal content as a no-blocking[73] commitment. The Regulation, on the other hand, addresses[74] a scope beyond no-blocking. The third subparagraph of Article 3(3) bans traffic management measures other than reasonable traffic management and lists explicitly that providers of IASs "shall not block, slow down, alter, restrict, interfere with, degrade or discriminate […]".[75]

In light of a Regulation that sets out more fundamental duties for providers of IASs than the voluntary non-blocking commitment of the Code, and considering the subsidiarity principle, the Code's no-blocking provisions appear to be compliant, but should take into account that the Regulation goes further than the Codes. Hence, these provisions may remain in the Code but should address any gaps, since the Regulation governs these issues fully (and even implies additional duties for providers).

---

72 See the Code's explanatory text for Commitment 1 and the respective glossary item.

73 "Signatories to this code support […] the general principle that legal content, applications and services, or categories thereof should not be blocked."

74 The Regulation combines a further-reaching end-user right with the providers' duty in Article 3(3) to treat all traffic equally and the respective provisions on reasonable traffic management measures.

75 Recital 15 refers to a "general prohibition on blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services, or specific categories thereof".

4.1.3 Products that offer full internet access are the norm

The commitment that full internet access products are the norm shows similarities with Article 5(1) of the Regulation: "National regulatory authorities […] shall promote the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology." The same article obliges national regulatory authorities to publish annual reports on the respective monitoring and findings. The main difference between the Code and the Regulation in this respect is that the Code covers a voluntary commitment of providers (plus Ofcom's commitment to monitor the prevalence of full internet access products), while the Regulation addresses only national regulatory authorities. It should be noted that the Regulation refrains from specifying how a national regulatory authority should promote non-discriminatory internet access.[76]

When comparing Code and Regulation with respect to the instruments they rely on, the Code appears to be further developed than the Regulation: the providers' self-commitment represents an instrument that is absent in the Regulation. In this light, and since the Code's self-commitment is not in conflict with any of the Regulation's provisions, the Code is deemed compliant and relevant in this aspect.

It should be noted though that this assessment is notwithstanding any compliance assessment of "alternative types of products" (see Section 4.1.4). If alternative types of products were found to be non-compliant with the Regulation, it would follow that only internet access products without restrictions[77] and managed services would be allowed. This scenario would render the self-commitment in its current form redundant. It could, however, regain relevance in this scenario if it was altered to address managed services instead of alternative types of products.[78] The self-commitment would then determine the relation between best-efforts internet access and managed services (the former being the norm). This relation is an important aspect in the Regulation, especially Article 3(5), which gives providers of IASs the right to offer (what the Code would call) managed services under certain conditions as long as the "network capacity is sufficient to provide them in addition to any internet access services provided".

4.1.4 Ability to offer alternative types of products

The Code covers the ability for providers to offer alternative products. An alternative product "does not support full internet access, i.e. […] certain classes of content, applications and/or services are blocked […]". Providers who offer alternative products

76 Note also the difference in wording between full internet access (Code) and non-discriminatory internet access (Regulation).

77 Except restrictions emerging from reasonable traffic management or from a provision in Article 3(3)(a) to (c).

78 In the sense of the Code, alternative types of products do not necessarily include managed services, nor are alternative types of products necessarily managed services. See Section 4.1.4 for more details.

refrain from labelling them as internet access products, and they "commit to effectively communicating any restrictions on such products".

It is important to note the differences between alternative products and managed services. Each of them constitutes a distinct concept in the Code. Managed services, which are discussed in Section 4.2.1, may be part of an alternative product, but alternative products might be offered independent from any managed service. Think, for example, of a smart fridge that comes with an embedded SIM card,[79] by which the smart fridge is enabled to send and receive encrypted messages to and from a small set of pre-configured IP addresses. The terms and conditions for this product state that its communication facilities may only be used for the intended use. Since the embedded SIM cannot be easily tampered with and since the product does not need any service quality beyond the reliable[80] delivery a regular TCP-based communication offers, no traffic management is required.

While the Code refers to both internet access products and alternative products, the Regulation only[81] addresses internet access. Article 1(1)[82] restricts the Regulation's scope to the provision of internet access.[83] This definition of the scope of the Regulation might have important consequences for the question of whether alternative products (as defined in the Code) are compliant with the Regulation. If alternative products do not qualify as IASs, alternative products will not fall within the scope of the Regulation. The Regulation would therefore not apply to alternative products. Compliance would be of no concern,[84] and providers could continue to offer such alternative products under the provisions of the Code.

Thus, the key question to assess the above scenario is to what extent a product would have to differ from IASs in order to qualify as a product outside of the Regulation's scope. The answer lies in the Regulation's definition of IASs as outlined in Article 2(2). There are two conditions to be considered. The first condition determines which aspects must not have an impact on the assessment of whether a product qualifies as an IAS.

---

79 Also referred to as e-SIM.

80 "Reliable" in the context of a connection-oriented transport protocol like TCP means that the receipt of data is explicitly acknowledged by the recipient to the sender. Non-acknowledged data is assumed to be lost on the way from sender to receiver and is consequently re-transmitted until successfully acknowledged. All data is numbered, allowing for both sender and receiver to know the current state of the communication and allowing clear identification of the original sequence at the recipient.

81 Note that the Regulation uses terminology in Article 3(5) that resembles the Code's terminology of alternative products: Article 3(5) refers to "services other than internet access services". However, the Regulation means (what the Code calls) managed services, not (what the Code calls) alternative products, as the Regulation refers to services "[…] which are optimised for specific content, applications or services, or a combination thereof […]".

82 See also Recital 1.

83 "This Regulation establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights."

84 The other way around, compliance would most certainly be a concern if alternative products qualified as internet access services. These products would then risk being in conflict with the Regulation's principle of equal treatment of traffic, in particular the requirement to treat traffic "[…] without […] restriction […]", stipulated in Article 3(3). They would also risk being in conflict with Article 3(2), which states that "agreements between providers of internet access services and end-users […] shall not limit the exercise of the rights of end-users laid down in […]" Article 3(1).

The second condition determines the aspects that shall have an impact on the assessment.

The first condition is the Regulation's principle of technological neutrality.[85] Neither the network technology nor the terminal equipment used shall play a role in determining what an IAS entails. Applied to the above smart fridge example, this implies that for instance the use of a SIM card or the choice for mobile communication does not affect whether the product qualifies as an IAS.

The second condition comprises "a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet […]". As the Regulation defines its scope in relation to the provision of internet access and due to the Regulation's technology-neutral notion of internet access that focuses on connectivity, alternative products would seem to be outside of the Regulation's scope if they only give access to a significantly limited number of end points in the internet. Where to draw a line exactly remains to be seen, but connectivity appears to be at the very core of the question. In the smart fridge example, the product could hardly qualify as internet access or a replacement for IASs, since it is by design far from providing connectivity[86] to a majority of (let alone virtually all) end points of the internet.

The aspect of being a potential replacement[87] for IASs refers to the Regulation's take on managed services as outlined in Article 3(5). Although it is important to reiterate that alternative products are not necessarily managed services, it is obvious that managed services are likely to play a role in some alternative products. If that is the case, it is essential for the overall alternative product's compliance to consider the Regulation's requirements for managed services (see Section 4.2.1) in addition to the connectivity aspect discussed in the above.

In sum, to retain the ability to offer alternative products, ISPs have to ensure that such products do not qualify as IASs. Without prejudice to the outcome of that process, it is clear that the difference between alternative products and internet access needs to be

85 See also Recital 2.

86 Note that Recital 4 demands providers of internet access services not to "restrict connectivity to any accessible end-points of the internet". However, the provider in the smart fridge example offers a product that is not intended to provide internet access. Products other than internet access services are not within the scope of the Regulation and therefore the smart fridge example is not affected by Recital 4. Obviously this assessment depends on how connectivity is construed. As the smart fridge uses TCP, data is sent over the internet. Technically speaking, reduced connectivity is more of an application layer issue than a network layer issue, according to the internet's layered communications model. The smart fridge would have connectivity to virtually all end points (as the Regulation provides) from a network layer perspective, even if the connectivity is reduced in the application layer. If connectivity according to the Regulation would have to be construed from a purely network layer-oriented perspective, the smart fridge would not qualify as an alternative product as it would fall into the scope of the Regulation. However, if reducing connectivity by pre-configuring IP was construed as not having connectivity to all end points because the application layer is not in line with the definition of connectivity, then the smart fridge would not be within the scope of the Regulation.

87 It may in general be advisable for the Code to replace "alternative product" with "different product", or similar, in order to avoid any misleading signal that might emerge in terms of these products being alternatives – in the sense of possible replacements or substitutes – for internet access.

substantial – avoiding the term internet access and communicating any restrictions effectively to consumers will be necessary but not sufficient prerequisites to underpin the (technical) difference.

4.2 Commitment 2 of the Open Internet Code of Practice

4.2.1 Right to develop and offer managed services

The Regulation might not call them managed services, but obviously means (what the Code calls) managed services when it refers in Article 3(5) to "[…] services other than internet access services which are optimised for specific content, applications or services, or a combination thereof […]". Both Code and Regulation allow providers to offer managed services.

There are only subtle differences in how the Code and the Regulation address managed services: as regards their permission, the Code speaks of the providers' "right" to offer them, while the Regulation states that providers "shall be free"[88] to do so. As regards the very notion of managed services, the Regulation characterises them as "optimised" services in response to "requirements of the content, applications or services for a specific level of quality", while the Code defines[89] these services to "prioritise certain traffic", speaks of their potential to "guarantee a certain level of performance", and refers to a corresponding "quality of service arrangement".

In light of mostly consistent notions of managed services in the Code and in the Regulation, the right for providers in the Code to offer them is deemed compliant with the Regulation. Consequently, only very few aspects of the Code's definition might need further inspection and potentially clarification. Quality of service arrangements may be an example, provided that the Regulation addresses contractual agreements between providers and end-users in Article 3(2) and Recital 7, but not, at least not explicitly, between providers of IASs and CAPs.[90] Another example may be that for managed

---

88 See also Recital 16 which holds that "[p]roviders of electronic communications to the public, including providers of internet access services, and providers of content, applications and services should therefore be free to offer services which are not internet access services and which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet the requirements of the content, applications or services for a specific level of quality". Note that Recital 16 allows multiple types of providers, not only providers of internet access services, to offer managed services.

89 "Managed services: as articulated in Ofcom's document, such services are delivered when ISPs prioritise certain traffic according to the value they ascribe to it. Managed services can involve an ISP offering a quality of service that can guarantee a certain level of performance, so that the content, service or application can be delivered without risk of degradation from network congestion. Such a quality of service arrangement can be made between an ISP and a content, application or service provider or directly between an ISP and a consumer. An example could be the prioritisation of an IPTV service."

90 It should be noted in this context that the European Commission's Fact Sheet mentions "[…] that there can be no paid prioritisation of traffic in the Internet access service". See http://europa.eu/rapid/press-release_MEMO-15-5275_de.htm.

services, the Code acknowledges that "ISPs prioritise certain traffic according to the value they ascribe to it", whereas the Regulation holds that any optimisation "[…] is necessary in order to meet requirements of the content, applications or services for a specific level of quality". Code and Regulation thus see somewhat differing reasons to motivate the prioritisation/optimisation of a managed service. While these two examples illustrate that the Code and the Regulation adopt similar notions of managed services, there are still some differences to be considered as the following paragraph outlines.

It should be noted that the Regulation imposes prerequisites for managed services that the Code does not cover. Providers of such services need to be able to demonstrate that the respective optimisation is necessary. Recital 16 demands that "[n]ational regulatory authorities should verify whether and to what extent such optimisation is objectively necessary to ensure one or more specific and key features of the content, applications or services and to enable a corresponding quality assurance to be given to end-users, rather than simply granting general priority over comparable content, applications or services available via the internet access service and thereby circumventing the provisions regarding traffic management measures applicable to the internet access services." Further prerequisites introduced by the Regulation in Article 3(5)[91] embrace that managed services may only be offered if there is sufficient network capacity,[92] that they may not be a replacement for internet access and that they "shall not be to the detriment of the availability or general quality of internet access services for end-users". Articles 4 and 5 lay down the corresponding contractual information as well as monitoring and reporting duties.

In sum, Code and Regulation are found to apply largely consistent notions of managed services albeit using different terminology. Only very few and detailed aspects of the Code's provision would need further inspection; overall, the Code appears compliant with the Regulation as regards managed services. However, as the Regulation imposes additional prerequisites for managed services, the Code's provisions on managed services might be deemed compliant, although they are recommended to address any gaps.

4.2.2 Concept of reasonable traffic management and preventing negative discrimination

The Code and the Regulation both cover the concept of reasonable traffic management.[93] Furthermore, they both develop the concept of reasonable traffic management based on the same principle, namely that reasonable traffic management shall not be motivated by commercial considerations, meaning that negative

91 See also Recital 17.
92 Note that the Code also refers to the relation between managed services and internet access services, but it does so by recognising "[…] the importance of best efforts internet access being a viable choice for consumers alongside any managed services that might be developed and offered".
93 The Code under Commitment 2, the Regulation primarily in Article 3(3).

discrimination – degrading "[…] the content or application of a specific provider(s)", as the explanatory text in the Code puts it – shall be avoided. The signatories to the Code commit themselves to the prevention of negative discrimination; the Regulation prescribes it. The intended effect though is the same so that the Code may be deemed compliant with the Regulation in this regard.

Nonetheless, some of the traffic management practices that the Code lists in its explanatory text on Commitment 2 risk being in conflict with the Regulation. The following overview discusses each of the traffic management practices and assesses their respective compliance with the Regulation:

- "managing congestion on its network": this practice is, per se, compliant with the Regulation under the provisions of Article 3(3)(c). It is, however, problematic[94] that the Code refrains from limiting the practice with respect to duration or frequency, which are both important aspects in the Regulation. Article 3(3) states that reasonable traffic management measures "shall not be maintained for longer than necessary". Recital 15 is very elaborate in explaining the applicable conditions of temporary and exceptional congestion, and in explaining that "[r]ecurrent more long-lasting network congestion which is neither exceptional nor temporary should not benefit from that exception but should rather be tackled through expansion of network capacity". The Recital leaves no doubt that reasonable traffic management for purposes of managing congestion is allowed as long as "[…] congestion occurs only temporarily or in exceptional circumstances".[95]
- "blocking services it is required to do so by law or a court order": this practice is compliant with the Regulation under the provisions of Article 3(3)(a) and Recital 13.
- "blocking sites and services included on the Internet Watch Foundation list", "deploying age verification/child protection/parental control tools for its consumers" and "deploying content filtering or make available content filtering tools where appropriate for public wi-fi access": the Regulation does not specifically mention these practices. End-users have the right to access services, content and applications of their choice. Providers of internet access services can block where this is necessary for Union or national legislation, or measures giving effect to such legislation.

94 This refers to a problem purely from a compliance point of view: the compliance analysis points to differences between the Code and the Regulation as regards duration and frequency of traffic management practices. The compliance analysis does not consider in any way the reasoning behind these differences, nor does it entail any assessment whether, or under which circumstances, the by-exception and temporary-only requirements of the Regulation appear sensible.

95 Recital 15 acknowledges that "[…] congestion might occur especially in mobile networks, which are subject to more variable conditions […]", but it is important to realise that this refers to temporary congestion only. In case it is "[…] predictable that such temporary congestion might occur from time to time at certain points in the network […]", the Regulation qualifies such predictable temporary congestions as non-exceptional ones – and it concludes for these cases "[…] that a capacity expansion would be economically justified".

- "supporting the delivery of managed services" and "ensuring elements of a consumer's contract are observed (e.g. data caps, download limits, heavy user policy)": although the Regulation does not mention these practices explicitly in the context of reasonable traffic management, it follows quite naturally that these practices must be allowed since they determine technical necessities to implement managed services and contractual agreements, both of which are governed in the Regulation in Article 3(5) and Article 3(2), respectively.
- "safeguarding the security and integrity of its network": this practice is compliant with the Regulation under the provisions of Article 3(3)(b) and Recital 14.

4.3 Commitment 3 of the Open Internet Code of Practice and the commitments of the Traffic Management Transparency Code of Practice

Commitment 3 of the Open Internet Code of Practice entails that "ISPs remain committed to supporting the provision of clear and transparent information about their traffic management practices". This commitment materialises by means of the Traffic Management Transparency Code of Practice, in particular the KFI table.

The KFI table is an essential part of the Traffic Management Transparency Code, but it is important to note that the Code[96] provides the necessary context for consumers to understand and interpret the information in a KFI table. To this end, the Code describes traffic management practices and it explains the potential impact that traffic management practices may have – among other relevant factors – on a consumer's experience. The emphasis on effective consumer information is underlined by two of the six good practice principles that the Code lists and that its signatories commit themselves to adhere to. The first good practice principle ("Understandable") entails the use of "[…] non-technical and clear language […]". The second good practice principle ("Appropriate") means that "[…] the level of detail of the information provided will be adequate to meet the varying needs of different consumers".

The good practice principles and the respective information for consumers included in the Code demonstrate the degree to which the Code and the KFI table are designed with consumers in mind. It should be added that this is to some extent the consequence of an Ofcom-commissioned study[97] into the Code from a consumer's point of view. The study revealed that the information provided in the KFI table is generally transparent.

96 Note that, within the context of this section, the "Code" refers to the Traffic Management Transparency Code instead of the Open Internet Code of Practice, which is referred to by the "Code" in the other sections of the compliance analysis.

97 See http://stakeholders.ofcom.org.uk/binaries/research/broadband-research/1145655/traffic-kantar.pdf. The study investigated three primary questions: "What factors drive consumers' broadband purchasing decisions? What are consumer experiences of, and expectations for, their internet services? What is the current level of awareness, and understanding of, traffic management and the KFIs?"

However, since consumers were found to know on average only very little about how the internet works and, consequently, about traffic management, Ofcom concluded that "[…] UK internet users do not necessarily understand the potential relevance of traffic management to their product choices".[98] These insights have led to Ofcom's consumer guide to traffic management[99] as well as to recommendations with regard to consumer-oriented improvements of the Code.[100] These recommendations have been implemented in the corresponding revision of the Code.

Consequently, the Code's emphasis on effective consumer information is the achievement of a thorough process that focused on the critical success factors to increase transparency. It is exactly in this regard that the Code and the Regulation differ. While they do not differ significantly in terms of topics[101] to be addressed, they do so primarily in the choice of how consumer information regarding traffic management shall be provided: the Regulation foresees consumer information mainly being presented in terms of contractual information, as outlined in Article 4(1). It is a well-known phenomenon,[102] especially in the context of online services, that consumers on average do not read, understand or act upon terms and conditions. The information a provider is supposed to compile in accordance with Article 4(1) is very likely to constitute relevant information for consumers to make informed choices,[103] but integrating the information in contractual agreements might defeat the purpose of increasing transparency.

In light of conforming motivations for and topics of consumer information, and in consideration of differing ways to present consumer information, the Code is deemed compliant with the Regulation – and highly relevant in order to effectively inform consumers. The Code and the KFI table[104] remain fully relevant as a further developed instrument, which has been optimised for consumer information purposes. The Code and the KFI table provide information that is significantly more likely to reach the attention of consumers than by the Regulation's approach of focusing on contractual information.

---

98 See http://stakeholders.ofcom.org.uk/binaries/research/broadband-research/1145655/traffic-research.pdf.

99 See http://consumers.ofcom.org.uk/internet/internet-traffic-management/.

100 "Provide an introduction to the KFIs that summarises the relevance of the policy and outline how it affects the ISP's product set; Ensure that technical terms are explained in clear and simple (non-technical) language; Provide specific and meaningful measurement criteria for when high usage or 'fair usage' policies are applied (e.g. 'Hours' of streaming as opposed to 'MB'); Use clear symbols to designate 'yes', 'no' and 'not applicable' responses in the KFI tables." See http://stakeholders.ofcom.org.uk/binaries/research/broadband-research/1145655/traffic-research.pdf.

101 The Code/KFI table and the Regulation both focus on traffic management, volume limitations and managed services, and on how these aspects potentially affect a consumer's internet access service. Articles 4(1)(a) to (c) address these topics in the Regulation. In contrast to the Code, the Regulation also addresses speeds – speeds are the subject of a dedicated code in the UK – and remedies in Articles 4(1)(d) and (e), respectively.

102 See, for instance, http://stakeholders.ofcom.org.uk/internet/personal-data-and-privacy/.

103 Recital 18 holds that "[t]he provisions on safeguarding of open internet access should be complemented by effective end-user provisions which address issues particularly linked to internet access services and enable end-users to make informed choices."

104 Adapted to reflect the compliance analysis results.

It should be noted that the Regulation opens the way to an orderly co-existence of consumer information in terms of contractual information and in the form of the Code/KFI table. The Regulation offers two options: the first relates to Article 4(1), which primarily specifies the contractual information duties of providers, but also includes the duty that they "[…] shall publish the information […]". Thus, the Code and the KFI table could be the model for publishing the respective consumer information on traffic management. The second option relates to Article 4(3),[105] which enables Member States to maintain or introduce "[…] additional monitoring, information and transparency requirements, including those concerning the content, form and manner of the information to be published". On this basis, Member States might impose[106] consumer information duties, for instance along the lines of the Code and the KFI table.

4.4 Monitoring the commitments of the Open Internet Code of Practice

The Code not only holds and explains the three commitments of its signatories, but it also refers to three commitments of Ofcom. These commitments refer to monitoring activities, namely which of the signatories' commitments Ofcom monitors and how. The following overview discusses each of them in turn and assesses their respective compliance with the Regulation:

- "progress in delivering transparent information to consumers about traffic management practices, keeping under review the possibility of intervening more formally": this monitoring commitment relates to the assessment conducted in Section 4.3 on the topics of consumer information and transparency. It falls within the scope which Article 5(1)[107] determines by stating that "[n]ational regulatory authorities shall closely monitor and ensure compliance with Articles 3 and 4". Paragraph 1 of Article 4 is particularly important in the context of the Code's monitoring commitment as it sets out the consumer information which providers need to include in contracts and which they need to publish. Thus, the Code's monitoring commitment may be deemed compliant with the Regulation. Since Ofcom have addressed the monitoring commitment in the annual Communications Infrastructure Report[108] series – while it is still to be seen in

105 See also Recital 18, which assigns the right to Member States to "[…] maintain or adopt more far-reaching measures" on the topic of "[…] effective end-user provisions which […] enable end-users to make informed choices".

106 If Member States made use of this power, the result would obviously not be a voluntary self-commitment but a regulatory requirement.

107 See also Recital 19.

108 For instance, in the 2014 Communications Infrastructure Report, Ofcom provided detailed findings as regards the monitoring commitment in Chapter 9, and summarised them in the Executive Summary as follows: "Having reviewed the operators' summaries of broadband and mobile traffic management practices, we believe they are now being more transparent with consumers over this issue. The most significant development is that all UK mobile operators have now discontinued packages which block access to VoIP services. On top of this, EE, Vodafone and Virgin Media have signed up to the Broadband Stakeholder Group (BSG) Open Internet Code of Practice. This means that all major consumer internet providers are committed to the self-regulatory approach, a key part of the Government's policy on Net Neutrality. We will continue to monitor the market closely to ensure that

which way and level of detail[109] National Regulatory Authorities (NRAs) will "[…] publish reports on an annual basis regarding their monitoring and findings […]" in accordance with Article 5(1) – the Code's monitoring commitment remains relevant.

- "the ongoing quality of best efforts internet access and keeping the possibility of introducing a minimum quality of service under review": this monitoring commitment relates to the assessment conducted in Section 4.2.1 on the topic of managed services. It is within the scope of Article 5(1), in particular with respect to the prerequisites of managed services stipulated in Article 3(5) and the contractual information regarding managed services set out in Article 4(1)(c). The monitoring commitment of the Code is therefore seen to comply with the Regulation. It remains relevant at least until further details will be known about the respective monitoring and reporting duties under the Regulation's provisions.
- "the prevalence and nature of products which block services in order to determine whether this would prompt any further intervention": this monitoring commitment relates to alternative types of products as assessed in Section 4.1.4. Since these alternative products were found to be outside[110] of the Regulation's scope and application, as long as an alternative product does not qualify as an IAS, the Code's monitoring commitment is not a concern of the Regulation and therefore it continues to be relevant. It should be noted that the monitoring of alternative products is intended to "[…] provide a mechanism to benchmark signatories' compliance with the provision set out in Commitment 1 that full products offering full internet access will be the norm […]". Such benchmarking implies that both alternative products and products within the scope of the Regulation are the subject of monitoring activity. This means that the Code's commitment to monitor alternative products shows the potential to interrelate on a practical basis with the Regulation's monitoring duties set out in Article 5(1).

The above monitoring commitments of the Code include the right for Ofcom to further intervene or to impose minimum service quality levels. These rights may be deemed compliant with the Regulation under the provisions of Article 5(1) holding that "[…] national regulatory authorities may impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate and necessary measures […]".

---

transparency continues to improve." See http://stakeholders.ofcom.org.uk/binaries/research/infrastructure/2014/infrastructure-14.pdf.

109 It is important to note in this context that the Regulation refrains from specifying how exactly the annual reporting shall look and what it shall cover in detail, but the Regulation in Article 5(2) obliges providers to make information available to the national regulatory authority "[…] relevant to the obligations set out in Articles 3 and 4, in particular information concerning the management of their network capacity and traffic, as well as justifications for any traffic management measures applied. Those providers shall provide the requested information in accordance with the time-limits and the level of detail required by the national regulatory authority."

110 Consider the discussion on how connectivity is construed; see footnote 86.

4.5 Voluntary process for raising concerns

Article 4(2) requires providers to establish a process for handling end-user complaints.[111] It states that "[p]roviders of internet access services shall put in place transparent, simple and efficient procedures to address complaints of end-users relating to the rights and obligations laid down in Article 3 and paragraph 1 of […]" Article 4.

The Code incorporates a process for raising concerns in its Annex 1. The Code details the purpose of this process, defines its scope and lays down a straightforward procedure to follow including the responsible persons to contact (with names and email addresses) and the option to escalate the process. By its specification and by practical experience throughout the past few years, the Code's process could arguably be characterised as being transparent, simple and efficient – so that it would satisfy the Regulation's high-level requirements. However, the Code's process cannot act as a direct implementation of Article 4(2) for the following two reasons.

First, the Code's "[…] process is designed to support communication between ISPs and providers of internet-based content, applications or services". In other words, it "[…] is not for consumer complaints". The Code's process refers consumers to their providers of internet access when they want to complain. Second, it has a narrower scope than the complaint process envisioned in the Regulation. The Code's process focuses entirely on concerns with respect to negative discrimination; the Regulation's process focuses on any concern related to topics in Article 3 and Article 4(1). In sum, the Code's process is seen as a relevant instrument that may complement, but cannot replace, the consumer-centric complaint process foreseen by the Regulation.

111 The Regulation not only requires a complaint-handling process, but it also refers to remedies available to end-users in case of non-conformance as well as to the respective penalties. The Code neither addresses remedies nor penalties. Penalties and remedies are handled in the Regulation as follows: Article 6 states that "Member States shall lay down the rules on penalties applicable to infringements of Articles 3, 4 and 5 and shall take all measures necessary to ensure that they are implemented". Article 4(1)(e) holds that the contractual information that providers of internet access services prepare for consumers needs to include "a clear and comprehensible explanation of the remedies available to the consumer in accordance with national law in the event of any continuous or regularly recurring discrepancy between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated in accordance with points (a) to (d)". See also Recital 18. Article 4(4) describes in addition the conditions for non-conformity of performance: "Any significant discrepancy [...] between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated by the provider […], where the relevant facts are established by a monitoring mechanism certified by the national regulatory authority, be deemed to constitute non-conformity of performance for the purposes of triggering the remedies available to the consumer in accordance with national law."

5 The way forward: A strategy for the evolution of the Codes

The expectation that the provisions of the Connected Continent Regulation on an Open Internet will apply from 30 April 2016 has created an opportune moment for reviewing the voluntary Codes of Practice in the UK. It is the right time to consider and assess available options that shape the way forward for the Codes. A strategy for evolving the Codes towards a future within a changed European regulatory framework is needed. This study contributes substantially to the development of that strategy, not least because of the set of recommendations which we identify and present in this concluding section of the study report.

We base these recommendations on the one hand on the key insights obtained throughout the study as presented in previous sections. On the other hand, we derive them from the analysis of relevant market developments. We discuss the latter in Section 5.1, while in previous sections we have established that the voluntary, self-regulatory, open and inclusive approach chosen in the UK continues to be relevant. The approach has proven its value as confirmed by the OIF members, including the Codes' signatories, Ofcom and the UK Government.

This finding extends beyond the approach alone; it also covers the concepts and principles underlining the Codes as well as the Codes themselves. The in-depth compliance analysis conducted in the context of this study (see Section 4) has revealed that the vast majority of concepts and principles of the Codes are compliant with the Regulation. Compliance is a necessary but not a sufficient condition for the relevance of the Codes and their provisions. The compliance analysis, however, suggests that most concepts and principles continue to be relevant, as Table 5-1 documents.

Table 5-1: Compliance assessment and proposals to adapt the Codes

<table>
<tr><th rowspan="2">Concept or principle</th><th colspan="3">Compliance assessment (see Section 4)</th><th rowspan="2">Proposals to adapt the Codes</th></tr>
<tr><th>Codes go further than Regulation</th><th>Regulation goes further than Codes</th><th>Concept not covered in Regulation</th></tr>
<tr><td rowspan="2">Concept of the Open Internet</td><td colspan="3">Compliant
(With minor updates)</td><td rowspan="2">Update the concept to reach compliance</td></tr>
<tr><td>–</td><td>–</td><td>–</td></tr>
<tr><td rowspan="2">General principle that legal content, applications and services, or categories thereof should not be blocked</td><td colspan="3">Compliant</td><td rowspan="2">Address the gaps in the Codes</td></tr>
<tr><td>–</td><td>✓
(Regulation implies additional duties for providers)</td><td>–</td></tr>
</table>

Products that offer full internet access are the norm	**Compliant**			– (Maintain unaltered as the Code adds value to the Regulation)
	✓ (Providers' self-commitment absent in Regulation)	–	–	
Ability to offer alternative types of products	**Compliant** (Assuming that alternative products are outside of Regulation's scope/application)			Develop a clear understanding of these products
	–	–	✓	
Right to develop and offer managed services	**Compliant** (A few detailed aspects need further inspection)			Address the gaps in the Codes; develop principles and voluntary commitments as regards these services
	–	✓ (Regulation imposes additional prerequisites)	–	
Concept of reasonable traffic management and preventing negative discrimination	**Partially compliant** (Some traffic management practices listed in the Codes risk being in conflict with the Regulation)			Develop a set of compliant traffic management good practices
	–	–	–	
Commitment 3 of the Open Internet Code and the commitments of the Traffic Management Transparency Code	**Compliant**			– (Maintain unaltered as the Code adds value to the Regulation)
	✓ (KFIs are superior to contractual information in effectively informing consumers)	–	–	
Monitoring the commitments of the Open Internet Code of Practice	**Compliant**			– (Maintain unaltered)
	–	–	–	
Voluntary process for raising concerns	**Compliant**			– (Maintain unaltered as the Code's process complements the Regulation)
	–	–	–	

As the compliance analysis implies, the ability to offer alternative types of products might turn into a focus area for the evolution of the Codes. This may in particular mean that the Codes need to determine a clear understanding of the characteristics of these products, how they differ from IASs and how they relate to managed services. Similar conclusions may be drawn for the right to develop and offer managed services. In light of the Regulation's many prerequisites for managed services, the Codes could serve as a model to demonstrate how to fill them with meaning in consideration of UK-specific market characteristics and taking account of all stakeholders involved. The Codes might thus be channelled into a set of agreed principles and voluntary commitments as regards the offering of managed services.

An additional focus area to develop the Codes further may be reasonable traffic management practices. Given that the Regulation and the Codes build upon the same principle to establish the concept of reasonable traffic management and in consideration of the room that the Regulation opens for traffic management practices that are based on national legislation, the Code may provide value to all affected stakeholders by developing the current list of practices into an agreed (and obviously compliant) set of traffic management good practices.

5.1 Analysis of relevant market developments

In this section, we set out to understand the key market developments that may have an impact on traffic management. From desk research and exchange with experts from the UK market, we have identified the following trends that are likely to have an impact on traffic management practices in the UK:

- Internet of Things (IoT) and demand for alternative products (other than IASs)
- innovative plans for consumers
- innovative modes of cooperation between ISPs and CAPs
- shifting focus in the net neutrality debate from the access to the core network

The IoT is certainly one of the most important trends of the foreseeable future. Ofcom state that there are already 40 million connected devices in the UK. By 2022, it is expected that there will be hundreds of millions of devices connected to the internet.[112] Experts concur that this trend will have a substantial and sustained economic impact around the world. Estimates on the size of this impact differ though. They range between US$1.9 trillion (Gartner) and US$14.4 trillion (Cisco).[113] A specific estimate for the economic impact in the UK was not found by the authors of this report. It is expected, however, that the major economic impact will happen in the developed countries first. The internet connections of such devices are unlikely to be full internet

112 Ofcom (2015): Promoting investment and innovation in the Internet of Things.
113 UK Government Chief Economic Advisor (2014): The Internet of Things: Making the most of the second digital revolution.

access products as many of them will only ever communicate with a limited number of IP addresses. Consequently, the IoT has large potential to establish various services other than full internet access for ISPs.

With more and more consumers connecting to the internet,[114] variation in consumer preferences/expectations as regards their IAS is likely to increase. In line with the concept of innovation diffusion,[115] one would expect that the remaining 15% of the population who are still without an internet connection in the UK can be described as very late majority or laggard consumers. Often, these consumers have lower expectations and can be expected to have low usage of internet-based services. However, such consumers may be quite price-sensitive, which may merit specifically targeted plans for them that include certain access limitations in order to offer them the services at a lower price. On the other end of the spectrum, the so-called innovators commonly comprise consumers with a strong involvement in technology, who also want to adopt the latest services offered on the internet. These consumers may be interested in receiving prioritised services and are likely to have a higher willingness to pay for such offers. Again, ISPs may intend to meet this demand by targeted offers. In sum, there needs to be some flexibility for ISPs to develop and market innovative services.

With the ongoing convergence of business models along the data value circle,[116] it appears relevant for ISPs' sustained economic success to be able to also enter into agreements and partnerships with OTTs that may or may not have implications for traffic management. In fact, some of the experts we interviewed for the present report thought that we are going to see much closer cooperation between ISPs and CAPs (at least the large ones) in terms of interconnection and peering. It was noted, however, that this is a developing market and it is still questionable whether it will actually take off. There are, for instance, doubts about whether such agreements would be commercially attractive for ISPs. Irrespective of the development of this market, regulation should be flexible enough to allow for such innovative business models and partnerships to operate beyond their current nascent state.

The three trends discussed thus far point to continuous innovation in the electronic communications[117] sector. It will be critical that the interpretation of the upcoming Regulation is not too prescriptive and does not rule out ex ante certain business models or partnerships that potentially bear great economic value in the future. In particular, regulators should refrain from limiting business models just because they see potential

114 Ofcom (2015): Communication market report 2015.

115 Rogers, E.M. (1962): Diffusion of innovation. Glencoe: Free Press.

116 Arnold, R. & Waldburger, M. (2014): The impact of data on ICT business models. GSR Discussion Paper. URL: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/GSR14%20Impact_of_dataBusinessModels.pdf.

117 At the same time as safeguarding electronic communications sector innovation, it is important to ensure continuous innovation in the CAP markets too. The above trends could add to the potential gatekeeper power of ISPs. See, for instance, Ofcom (2015): Strategic review of digital communications. Discussion document, clause 9.120: "[…] we are mindful that [technological developments and convergence] may also raise the potential for new online platform gatekeepers to emerge in the future."

for anti-competitive behaviour. Instead, regulation should be drawn up in a way that does not hinder innovation. If there is potential for anti-competitive behaviour, corresponding monitoring tools need to be put in place. As the UK example and the general evidence presented in Section 3.1 have shown, a self-regulatory approach may solve all these issues effectively.

As the Regulation creates a new framework for IASs, it is likely that the focus in the debate on the Open Internet and traffic management practices will be shifting from the access networks more to the centre of the internet. This shift may be expected to be slow and gradual in light of an access-centric Regulation that needs clarification in many areas. Nevertheless, questions about how networks interconnect and how they manage incoming or outgoing traffic at these interconnection points; how operators of Content Distribution Networks (CDNs) handle the traffic of different CAPs competing for delivery of their content; and whether the incentive schemes of CAPs (including cloud providers), CDN operators, internet exchange points and higher tier network operators may lead to cooperation might draw increased attention in the future. This part of the internet is at least as competitive and innovative as internet access, with the UK playing a key role in Europe (e.g. for transatlantic traffic), thus creating the optimal preconditions for an industry-led initiative to develop agreed principles and voluntary commitments as regards interconnection and traffic management in the core networks of the internet.

5.2 A vision for a new Code / new Codes

Finally, based on the insights gathered throughout this review of the self-regulatory Codes, this section provides a strategy for evolving the Codes in accordance with the upcoming European regulatory framework as well as current market developments discussed in the preceding section. Naturally, an update has to take into account the points where the Codes need to address the two minor gaps that exist in comparison to the Regulation. Otherwise, the recommendations given here build actively on the strengths of the Codes that this review identified.

Recommendation 1: Merging of the two Codes

Given that the Regulation addresses both the concept of the Open Internet as well as the requirements for transparency of traffic management measures to consumers, it is sensible to reflect this move in a single merged Code of Practice. One may expect very little if any friction in doing so as the signatories for both Codes of Practice are identical.

Recommendation 2: Provide consistent guidance on how to interpret the Regulation

Our analysis of the Regulation clearly shows that numerous issues still require clarification. Many concepts in the Regulation are vague, inconsistent or omitted completely. The BEREC guidelines are expected to shed some more light on these issues, but they will in particular focus on NRAs' duties and scope of action. The Codes could serve an important function here, namely to provide a consistent interpretation of the Regulation that builds on the insights and requirements of the industry itself.

Within that, the process of drawing up a common Code of Practice that provides such a consistent interpretation of the Regulation may – similar to the first development of the Codes among stakeholders – facilitate a common understanding of the Regulation. In turn, this may mitigate complaints and conflicts down the road. Naturally, such a process has to take the BEREC guidelines into account. In line with the empirical insights on the general characteristics of self-regulatory approaches, one may expect that such a process enables a mutual understanding among relevant stakeholders based on social norms and peer conduct that has thus far been highly effective in various ways.

Recommendation 3: Proactively address services other than IAS (e.g. managed services)

As the compliance analysis in this report has identified, there are areas that the Regulation does not touch upon. Within that, services other than IAS appear to be particularly relevant especially in light of the market developments outlined in the previous section.

Against this backdrop, it seems relevant that an updated version of the Codes should specify a set of agreed principles and voluntary commitments as regards the offering of managed services, reasonable traffic management practices and services other than (full) IAS. The roll-out of IoT technology underscores the relevance of this point, as the previous section highlighted.

Recommendation 4: Review KFIs with a view to meet latest consumer information best practices

As shown in the above, the KFIs established through the Codes in the UK have already proven to be effective. They provide consumers with consistent, standardised information about traffic management measures. As such, the commitments set up by the Codes outperform the requirements of the Regulation that only refer to presenting technical information in the terms and conditions of IAS products.

The KFIs are substantially more likely to reach consumers' attention than any consumer information included in terms and conditions: As our recent report for Ofcom[118] clearly shows, most consumers do not read, do not understand and do not act upon online terms and conditions. The KFIs on the other hand are focused and consistent, which makes them relatively easy to compare for consumers. Technical and legal jargon has been reduced as compared to typical contractual agreements, and the information is made available upfront to consumers by most ISPs.

Nonetheless, recent research conducted by us on behalf of BEREC[119] indicates that consumers' understanding of information traffic management can be significantly improved by providing them with easy-to-comprehend, vivid and figurative information, for example in the form of an animated video. Our experiment has shown that such a video, when representing both positive and negative effects of traffic management, can educate consumers without immediately biasing their opinions in one way or another. In light of continuous advances in consumer information, we recommend to periodically review the KFIs in order to ensure that they continue to adhere to the relevant best practices.

Recommendation 5: Maintain Ofcom's position and the complaint process

In the primary research conducted as part of this review with individual stakeholders, it became clear that both the role that the Codes envision for Ofcom as well as the voluntary process for raising concerns will remain relevant for signatories and should be sustained.

118 Arnold, R.; Hillebrand, A. & Waldburger, M. (2015): Personal data and privacy. A report for Ofcom. http://stakeholders.ofcom.org.uk/internet/personal-data-and-privacy/.

119 Arnold, R.; Waldburger, M.; Morasch, B.; Schmid, F.; Schneider; A.; Cilli, V.; van der Peijl, S. & Wauters, P. (2015): The value of network neutrality to European consumers. A study commissioned by BEREC. http://berec.europa.eu/eng/document_register/subject_matter/berec/download/2/5024-berec-report-on-how-consumers-value-net-_2.pdf

Annex A – Open Internet Code of Practice

OPEN INTERNET CODE OF PRACTICE:

VOLUNTARY CODE OF PRACTICE SUPPORTING ACCESS TO LEGAL SERVICES AND SAFEGUARDING AGAINST NEGATIVE DISCRIMINATION ON THE OPEN INTERNET

Introduction

This voluntary code of practice puts forward a set of commitments agreed by signatories in support of the open internet. They were developed by signatories following discussions with government, the regulator, industry and broader stakeholders and building on Communications Minister Ed Vaizey MP's statement in 2011 that the concept of an open internet should be guided by three principles:

- users should be able to access all legal content
- there should be no discrimination against content providers on the basis of commercial rivalry; and
- traffic management policies should be clear and transparent.

This voluntary code of practice should be read in conjunction with the existing voluntary code of practice on traffic management transparency[120] and the November 2011 Ofcom statement on its approach to net neutrality[121].

Background

The way we use the internet is changing. The internet is increasingly being used by consumers as a means to access video based services and the uptake of these relatively high bandwidth services is in turn driving the rapid growth in overall traffic levels. Meanwhile significant investments are being made in new fixed and mobile high speed access networks which will, in turn, continue to drive traffic volumes across the internet.

The potential to provide managed services that would enable a specific piece of content, service or application to be delivered without risk of degradation from network congestion is one option open for consideration by Internet Service Providers (ISPs). Such services are still at a very early stage and it is difficult to predict how widely they will be offered or used. These services could provide real consumer benefit in terms of improved experience however the emergence of managed services does raise questions about what their impact will be on best efforts internet access and whether their emergence could lead to additional unintended outcomes that would be less welcome.

Concern about these issues has led to increased focus on the traffic management policies employed by ISPs to help meet and manage demand on their networks. Traffic management is not a new phenomenon but refers to a range of practices that have long been employed by ISPs to make efficient use of their networks and help provide a good experience for customers.

---

120 www.broadbanduk.org/trafficmanagementtransparency
121 http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf

In this context, several issues have been raised, including:

- the importance of providing clear information to consumers about traffic management practices that could be relevant to the service choices they make
- the continued ability of consumers to be able to access legal content, applications and services of their choice through products offered by ISPs
- the risk that any negative discrimination undertaken by ISPs could have harmful impacts on providers of content, applications and services available over the internet
- the potential overall impact of a new managed services market on "best efforts" internet access and the ability of the internet to remain as an open platform for innovation

In November 2011 Ofcom published a document setting out its views on these issues. In this document Ofcom recognised the positive role that traffic management can play in the internet's success, increasing the efficiency with which operators manage network capacity. It also acknowledged that traffic management could be used to support new innovative managed services that will be of benefit to consumers, such as high quality IPTV services, prioritised over other traffic.

Ofcom however also recognised that certain uses of traffic management could potentially lead to some undesirable outcomes. For example, the use of traffic management to target and degrade specific and alternative services and to prevent consumers from being able to access the legal services, content and applications of their choice over the internet.

Ofcom further highlighted the importance of best efforts access to the internet in supporting innovation and would be concerned if ISPs were to prioritise managed services in a manner that left insufficient capacity for best-efforts access to the open internet. Ofcom nevertheless argued that its approach would be to seek for the benefits of both best efforts access and managed services to co-exist. However it acknowledged that ensuring the on-going ability of best efforts access to support innovation would need to be kept under review as managed services may evolve in the market.

Throughout Ofcom's discussion, the importance of being transparent about the nature and elements of an ISP's traffic management policy and the level of competition in the market were also underlined as essential to supporting positive outcomes.

Ofcom did not recommend the need for any regulatory intervention to ensure any specific outcomes in November 2011. Indeed the next steps Ofcom outlined all involve continual monitoring of activity in the market to ensure any issues that need to be addressed are identified.

Ofcom committed to monitoring:

- progress in delivering transparent information to consumers about traffic management practices, keeping under review the possibility of intervening more formally
- the ongoing quality of best efforts internet access and keeping the possibility of introducing a minimum quality of service under review
- the prevalence and nature of products which block services in order to determine whether this would prompt any further intervention

Signatories to this voluntary code of practice believe that the approach set out by Ofcom is broadly correct. The evolution of the managed services market is at a very early stage and the collective impact of potential innovation is impossible to predict and evaluate. Moving at this stage to define specific rules surrounding the evolution of unknown services would be premature and would be likely to chill innovation in services that could deliver significant consumer benefits; restrict consumer choice; inhibit efficiency; and possibly distort the commercial position between ISPs and content, service and application providers. Nevertheless some proactive steps can be taken at this stage to help ensure that innovation leads to positive market outcomes and the positive coexistence of managed services with best efforts internet access.

Ensuring robust competition and providing effective transparent information about traffic management practices to users are viewed by signatories of this code as the key elements of an effective approach to these issues. However the signatories also believe it is important to set out at this stage their commitments with regard to ensuring access to legal services and safeguarding against negative discrimination towards the content or application(s) of specific providers.

The Code of Practice

Signatories to this code agree to make the following commitments regarding access to legal services, safeguarding against negative discrimination and supporting traffic management transparency. These are rooted in practical commitments that individual ISPs are able to make. These commitments should be read in accordance with the following explanatory section regarding their application in practice.

1. **Signatories to this code support the concept of the open internet and the general principle that legal content, applications and services, or categories thereof should not be blocked.**

   Whilst products that offer full internet access will be the norm, in order to support product differentiation and consumer choice, ISPs retain the ability to offer alternative types of products. In instances where certain classes of legal content, applications and/or services are unavailable on a product signatories to this code will:

   i. **Not use the term "internet access" to describe or market such products; and**
   ii. **Ensure that any restrictions are effectively communicated to consumers, building on the commitments made in the transparency code of practice.**

2. **Signatories to this code realise the positive impact some forms of discrimination could have in supporting innovation and choice and retain the right to develop and offer managed services. In recognising however that some forms of discrimination may be harmful, signatories undertake that traffic management will not be deployed in a manner that targets and degrades the content or application(s) of specific providers. Signatories also recognise the importance of best efforts internet access being a viable choice for consumers alongside any managed services that might be developed and offered.**

3. **Signatories support the provision of clear and transparent traffic management policies as outlined in the voluntary code of practice for traffic management transparency.**

What these commitments mean in practice

Commitment 1 means that all signatories to this code will ensure that products that support full internet access, i.e. services that permit a consumer to access any content, applications and/or service(s) that are lawfully available on the internet are the norm within their portfolio of products.

In order to support product differentiation and consumer choice, ISPs retain the ability to offer alternative products. However, in instances where a product does not support full internet access, i.e. where certain classes of content, applications and/or services are blocked, the term "internet access" will not be used to describe or market such products. ISPs also commit to effectively communicating any restrictions on such products.

In setting out **Commitment 2**, ISPs retain the ability to deploy reasonable traffic management practices over their networks. Such practices might include:

- managing congestion on its network
- blocking services it is required to do so by law or a court order
- blocking sites and services included on the Internet Watch Foundation list
- deploying age verification/child protection/parental control tools for its consumers
- deploying content filtering or make available content filtering tools where appropriate for public wi-fi access
- supporting the delivery of managed services
- ensuring elements of a consumer's contract are observed (e.g. data caps, download limits, heavy user policy)
- safeguarding the security and integrity of its network

Commitment 2 aims to prevent negative discrimination whereby an ISP targets and degrades the content or application of a specific provider(s). Commitment 2 was developed to address this potential type of negative behaviour espoused by the Minister when he articulated the principle of "no discrimination against content providers on the basis of commercial rivalry".

As set out in **Commitment 3** and the voluntary code of practice on traffic management transparency, ISPs remain committed to supporting the provision of clear and transparent information about their traffic management practices.

How the commitments will be monitored

Signatories believe that this set of voluntary commitments complement the approach set out by Ofcom and the ongoing work and next steps it set out in November 2011.

Ofcom has stated that one of its ongoing pieces of work will be to monitor the prevalence and nature of products which block certain classes of legal content, applications and/or services. This process will provide a mechanism to benchmark signatories' compliance with the provision set out in Commitment 1 that products offering full internet access will be the norm, coupled by the ability to offer alternative products that may not support access to all forms of content, services and applications.

Ofcom's intention to monitor the provision of transparent traffic management information and to investigate the nature of traffic management practices as part of its communications infrastructure report will play a useful role in benchmarking signatories'

success in communicating the nature of its traffic management policies to consumers as per voluntary Commitments 1 and 3.

Commitment 2 covers potential individual cases of negative and targeted discrimination and accordingly signatories to this code recognise that it would be helpful for a process to be put in place that would enable potential concerns about possible instances of negative discrimination to be raised with relevant parties. This process is set out in Annex 1.

Ofcom's stated intent to monitor the on-going ability of best efforts internet access to support innovation and to keep this under review as managed services may evolve in the market is also an important component of the wider context in which these commitments are being made.

Signatories recognise the importance of best efforts internet access being a viable choice for consumers alongside any innovation that may occur in the managed services market.

The signatories to this code therefore believe that it is right that Ofcom take ownership of this issue and also believe that the new proposed process will be a useful input to Ofcom as it continues its work in monitoring the nature and impact of traffic management practices in the market and the effective co-existence of managed services and best efforts internet access.

It is clear that the voluntary commitments being made in this code closely relate to ongoing monitoring work Ofcom has said that it will conduct. Signatories to this code are happy to discuss with Ofcom how its future work plans regarding open internet issues could support or input into a review of these voluntary commitments.

SIGNATORIES:

BE

BT

BSkyB

EE

giffgaff

KCOM

O2

Plusnet

TalkTalk

Tesco Mobile

Three

Vodafone

Virgin

July 2012 (agreed and launched)
May 2013 (minor amendments and clarifications)
November 2014 (additional signatories)

Glossary

- **Full internet access**: as articulated in Ofcom's document, such a service permits a consumer to access any service lawfully available on the internet.

  Providing such a service does not impinge on an ISP's ability to deploy reasonable traffic management practices over their networks. Such practices might include:

  - managing congestion on its network
  - blocking services it is required to do so by law or a court order
  - blocking sites and services included on the Internet Watch Foundation list
  - deploying age verification/child protection/parental control tools for its consumers
  - deploying content filtering or make available content filtering tools where appropriate for public wi-fi access
  - supporting the delivery of managed services
  - ensuring elements of a consumer's contract are observed (e.g. data caps, download limits, heavy user policy)
  - safeguarding the security and integrity of its network

- **Legal services**: this definition excludes any service, content, application or protocol that an ISP is required to block by UK law or a court order and child abuse images as informed by the list provided by the Internet Watch Foundation.

- **Blocked/blocking**: this definition relates to products where certain services are always unavailable as a consequence of an ISP's policy to block access to or contractually restrict access to a certain set of services on a particular product.

- **Managed services**: as articulated in Ofcom's document, such services are delivered when ISPs prioritise certain traffic according to the value they ascribe to it. Managed services can involve an ISP offering a quality of service that can guarantee a certain level of performance, so that the content, service or application can be delivered without risk of degradation from network congestion. Such a quality of service arrangement can be made between an ISP and a content, application or service provider or directly between an ISP and a consumer. An example could be the prioritisation of an IPTV service.

- **'Best-efforts' internet access:** as articulated in Ofcom's document, best efforts operates on the principle by which ISPs attempt to convey all traffic on more or less equal terms. The results in an 'open internet' with no specific services being hindered or blocked, although some may need to be managed during times of congestion.

Annex 1

Voluntary process for raising concerns about possible cases of negative discrimination over the open internet (in respect of commitment 2 of the code)

The purpose of this new process is to:

- provide a useful mechanism for various industry players to constructively engage on specific issues and concerns should they emerge;
- provide a useful evidence base on actual market developments that will help inform Ofcom's evaluation of the nature and impact of traffic management practices and the co-existence of managed services alongside best efforts internet access services;
- build on the useful cross-industry discussions that have informed the development of this code to support useful and productive future dialogue on open internet issues.

The following sets out the details of the process and how to engage with it should you have an issue within its scope that you would like to raise:

Who and what falls in scope of the process?

This process deals with alleged issues of negative discrimination, defined as an instance whereby an ISP targets and degrades the content or application of a specific provider(s).

This process is designed to support communication between ISPs and providers of internet-based content, applications or services with the overall aim to support the resolution of legitimate issues of concern in an efficient manner on a bilateral basis.

This process does not apply to more general issues about a signatory's traffic management policy, the price or conditions of a broadband product or how details of traffic management policies are communicated to consumers and service providers.

If you are interested in traffic management transparency please refer to the voluntary code on this issue: www.broadbanduk.org/trafficmanagementtransparency

Please note that this process is not for consumer complaints. If you are a consumer and wish to raise an issue in respect of traffic management, please contact your ISP in the first instance contacting its customer services team and following its published complaints procedure.

How does the process work

1. Raising an issue with the ISP

If you are a provider of internet-based content, applications or services and believe that a signatory ISP to the open internet code of practice has targeted and degraded your content, application or service you should raise this with the named contact below.

In doing so it is recommended that as much evidence and supporting information are provided as possible. It should be stressed that the signatories commit to this voluntary

process in good faith and would expect any third party raising concerns to act accordingly by ensuring that any concerns raised are properly evidenced and supported. Signatories to this code therefore reserve the right to dismiss and/or reject a complaint if it is not properly evidenced or if it does not fall within the scope of this process and commitment 2 of the code.

The provider of internet-based content, applications or services may also wish to look at the signatory ISP's overall traffic management policy to ensure that the issue is not in relation to general and disclosed traffic management policy. A list of hyperlinks to traffic management Key Facts Indicator tables provided by signatory ISPs is provided at: www.broadbanduk.org/trafficmanagementkfis

Named contacts from signatory ISPs:

BE: Ben.Shaw@bskyb.com

BT: mike.cunningham@bt.com

BSkyB: Ben.Shaw@bskyb.com

EE: Anne.hoitink@ee.co.uk

giffgaff: Robin.Vernon@o2.com

KCOM: Christine Roberts – regulatory@kcom.com

O2: Robin.Vernon@o2.com

Plusnet: Kelly Dorset - kdorset@plus.net

TalkTalk: Andrew.Heaney@talktalkplc.com

Tesco Mobile: john.preston@tescomobile.com

Three: trafficmanagement@three.co.uk

Vodafone: justin.hornby@vodafone.com

Virgin: Andrew.Wileman@virginmedia.co.uk

2. Logging an issue with the BSG

Should the issue not be resolved as a result of this bilateral contact the provider of internet-based content, applications or services can log this with the BSG by emailing: openinternet@broadbanduk.org

Please note that the BSG will only accept issues within scope of the process and which have been directly communicated to the ISP in question.

The BSG will not make a judgment of the validity of the claim but will share the log of raised issues with government and Ofcom at regular intervals to help build the evidence base of issues of concern and assist government and Ofcom with any further analysis, action or investigation they may wish to pursue.

3. Update and review of process

The BSG and signatory ISPs will keep this process under review in consultation with other stakeholders. Publically available updates on this issue will appear on the BSG website as they are published.

Annex B – Traffic Management Transparency Code of Practice

Voluntary industry code of practice on traffic management transparency for broadband services

March 2011

Overview

This document sets out a voluntary industry code of practice on traffic management transparency for broadband services.

The code was facilitated by the Broadband Stakeholder Group (BSG) with a number of leading Internet Service Providers (ISPs): BSkyB, BT, Everything Everywhere, O2, TalkTalk, Three, Virgin Media and Vodafone.

Traffic management is the term used to describe a range of technical practices undertaken to manage traffic across networks.

The use of traffic management is not new. It has, and continues to be, a vital tool in supporting the efficient operation of the internet and providing a good experience for the end-user.

Interest in how and why traffic management techniques are used by ISPs has grown in recent years. Whilst it is recognised that the use of traffic management for operational reasons, such as the provision of consistent quality of service at peak times is essential, regulators and policy makers in the EU are agreed that more information should be provided about how and why traffic management practices are employed by ISPs.

This code marks a step-change in the provision of such information and, while it is based on the way traffic management is employed today, it is also designed to adapt to developments that may emerge in the future such as managed services[122]. The commitments made in this code also go significantly beyond any statutory requirements in regards to transparency.

Whilst ISPs already provide information about traffic management practices, this initiative recognises that given growing interest in traffic management it is important to build upon information currently available and crucially give consumers and policy makers access to comparable information for the first time.

The code has been developed to support meaningful, useful and comparable information for consumers about the traffic management practices employed by their ISP.

The code has three elements.

122 Please see glossary on page 9 *[page 64 of this report]*

Firstly, an explicit commitment to provide more information to consumers about what practices are used in networks to (a) help maximise capacity for everyone's benefit and (b) to support adherence by customers to terms and conditions.

Secondly, an agreed set of good practice principles that will inform how ISPs communicate that information to consumers. Signatories agree that the information they provide about traffic management to their current and prospective customers will be:

- Understandable
- Appropriate
- Accessible
- Current
- Comparable
- Verifiable

Thirdly, to deliver on the comparability principle, signatories commit to publishing a consistent Key Facts Indicator (KFI) table, summarising the traffic management practices they use for each broadband product they currently market.

The introduction of the KFI will put information about the traffic management practices employed by these ISPs into the public domain in a consistent format. This information will be accessible to consumers and for third parties, such as price comparison websites, to be able to compile this information for consumers.

The development of this code by ISPs provides a key building block to delivering enhanced transparency to consumers about traffic management practices. The joint commitment to provide information in a common format should significantly assist in ensuring that information is made available in a way that enables comparisons to be made.

Furthermore, the code creates a framework for traffic management transparency that can be built on in the future. It commits ISPs to update consumers on any changes in the use of traffic management practices that would have a significant impact on their broadband product.

This is a new approach to providing information to consumers and refinements will likely need to be made over time to ensure this code delivers on its objectives. Therefore BSkyB, BT, Everything Everywhere, O2, TalkTalk, Three, Virgin Media and Vodafone intend to pilot this initiative throughout 2011 and review it in early 2012.

Feedback and comments are welcome on this approach from interested stakeholders throughout the pilot stage. Please send feedback to trafficmanagement@broadbanduk.org by 31 December 2011.

During this pilot stage, the founding signatories of this voluntary code also hope that other ISPs will sign up in order that comparable information about traffic management practices can be made available for all ISPs offering broadband products in the UK.

Voluntary industry code of practice on traffic management transparency for broadband services

Traffic management: what is it and why is it used?

In its broadest sense, traffic management is a component of an ISP's overall approach to network management. Network management includes elements such as capacity planning and network dimensioning to provide a quality of experience for consumers. Traffic management practices are subsequently used to deliver and maintain that experience for consumers.

In the face of rapidly growing traffic volumes, traffic management techniques help to make efficient use of networks and improve customer experience. The internet, including the networks over which it runs, is a shared resource and it is therefore right and important that access to it is allocated appropriately between users.

There is also the potential for traffic management practices to be used to support the delivery of managed services as part of a consumer's individual contract. This would allow ISPs to meet the varying needs of different consumers by offering them a range of differentiated services.

Accordingly, there are broadly two scenarios under which traffic management practices are being used or could be used in the future:

1. Traffic management to manage the operation of the overall network

This type of traffic management relates to practices applied to ensure the most efficient use of the network.

This can involve deploying techniques to prioritise time-critical applications (e.g. video streaming) so that they work effectively even in busy periods or congested locations. Conversely, ISPs can limit the throughput of non-time critical applications to provide a better experience for consumers accessing other types of traffic.

Traffic management is also subject to all applicable UK law and ISPs block child abuse images as informed by the list provided by the Internet Watch Foundation.

2. Traffic management in relation to a customer's contract

This type of traffic management is used to ensure that the particular services and content that the customer has contracted to are provided and that data caps and fair usage policies are observed. As such traffic management can or could be used to:

- apply restrictions or limitations to applications and protocols as per the terms and conditions of the consumer's contract
- invoke data usage caps or fair usage policies
- deliver managed services, offering a guaranteed quality of service for specified content, services or applications

How can traffic management best be explained to the consumer?

Traffic management is not a straightforward issue to explain to consumers, particularly as the impact of traffic management practices is only one component of the various factors that can impact on a consumer's experience of their broadband service. Other issues such as contention ratios (the number of consumers sharing the available bandwidth within a given area), the technology or type of network used to deliver the service, bottlenecks in other parts of the network, network elements in the consumer's home such as domestic wiring or the processing power of the end-user device can all impact on the consumer's experience.

Furthermore, even when the consumer's ISP is providing un-contended capacity, it may be that the content, service or application they are seeking to access is itself congested, or subject to restrictions, or otherwise managed by the content owner. Consequently traffic management practices by the consumer's ISP are far from being the sole determinant of the broadband experience.

In light of this, it is important that ISPs are allowed to put traffic management into context for consumers and provide information about it alongside other relevant information about their service that can impact on the consumer experience. As services naturally vary between ISPs, it makes sense that ISPs can speak to their current and prospective consumers in "their own voice".

Whilst ISPs already provide information about traffic management practices, this initiative recognises that it is important to build upon information currently available and crucially give consumers access to comparable information for the first time.

As such, the signatories of this voluntary code agree to:

1. Provide specific information to consumers

ISPs will make available the following information to consumers:

- description of traffic management practices
- how traffic management can affect a user's internet experience for different types of internet services
- changes made to traffic management practices that could have a significant impact on their broadband product for example access to services
- information on usage caps or upload/download limits

2. Good practice principles on transparency

In order that this information is useful and clear to consumers, ISPs will ensure that the following good practice principles inform the way they communicate with their current and prospective consumers.

Good Practice Principles on Traffic Management Transparency

Understandable	ISPs will use non-technical and clear language that consumers can understand to describe the traffic management practices they use.
Appropriate	ISPs will ensure the level of detail of the information provided will be adequate to meet the varying needs of different consumers. This could involve providing headline information about traffic management practices and supplementing this with additional information for consumers who may wish to access more detailed information.
Accessible	ISPs will ensure that this information is easy to find and access.
Current	ISPs will keep customers up to date about changes to traffic management practices that have a significant impact on their broadband product as quickly as reasonably possible using the most appropriate method. ISPs also endeavour to offer real-time information where appropriate and practicable.
Comparable	ISPs agree to publish a consistent key facts indicator table on their respective websites to summarise the traffic management practices used on the broadband products they currently market. This information will be available to third parties to present this information collectively for consumers to compare the practices of different ISPs.
Verifiable	ISPs will support a credible and independent assessment of their traffic management practices to give consumers assurance that the information provided about traffic management is robust.

How the good practice principles will work in practice

The principles[123] will inform the way in which individual ISPs communicate with current and prospective customers about the traffic management practices they employ.

Naturally, ISPs will want to talk to customers in their own language and put traffic management into context for consumers as it relates to the broadband products they currently market.

Yet what will be consistent across ISPs is a commitment to making sure this information is understandable, appropriate to the needs of different consumers and accessible and easy to find.

Furthermore, the code creates a framework for traffic management transparency that can be built on in the future. It commits ISPs to update consumers on any changes in the use of traffic management practices that would have a significant impact on their broadband product.

Enclosed overleaf is the key facts indicator table that ISPs who have signed up to this voluntary code will make available on their websites in relation to each broadband product they currently market. This information is sufficiently detailed to provide comparable information and will be available for third parties, for example price-comparison websites, to compile comparative information about ISPs' practices for the benefit of consumers.

In order that the principles of "understandable" and "appropriate" are applicable, ISPs may choose to provide other, more top-line, discursive and contextual information about their approach to traffic management in line with the products they offer. However a link to the more detailed KFI will be clearly available to those consumers who would like further information and to third parties who may want to utilise it in order to innovate ways of presenting comparative information about ISPs' traffic management practices.

Finally, ISPs acknowledge that appropriate independent verification of the information they provide about the traffic management practices they use will assure consumers and stakeholders that the information provided is robust. Verifying traffic management practices is a technical process and it will be important to thoroughly explore how such an exercise could take place. During the pilot period, ISPs look forward to discussing with Ofcom any potential approaches that could be taken towards third party verification.

BSkyB, BT, Everything Everywhere, O2, TalkTalk, Three, Virgin Media and Vodafone intend to pilot this initiative throughout 2011 and review it in early 2012.

Feedback and comments are welcome on this approach from interested stakeholders throughout the pilot stage. Please send feedback to trafficmanagement@broadbanduk.org by 31 December 2011.

123 These principles are separate from, but build on, the requirements relating to traffic management set out in the Voluntary Code of Practice on Broadband Speeds.

TIMETABLE

Launch: March 2011

Publication of KFIs: June 2011

Deadline for comments and feedback on approach: 31 December 2011

Review: Early 2012

TRAFFIC MANAGEMENT KEY FACTS INDICATOR*

Section 1: Traffic management in relation to your broadband product (not including during busy times and places to manage network congestion see Section 2)			
Name of broadband product			
Use and availability of services, content, application and protocols on this product			
Are any services, content, applications or protocols always blocked on this product?**			Y/N
If so what?	*List*		
Are any services, content, applications or protocols always prioritised?			Y/N
If so what?	*List*		
Are any managed services delivered on this product?			Y/N
If so what? What impact?	*This would highlight prioritisation of specific content or service and explanation on impact on any other traffic*		
Data caps and download limits			
What are the download/upload limits or data usage caps on this product?			Insert
Is traffic management used to manage compliance with data caps and download limits?			Y/N
Under what circumstances?			
Level of speed reduction?			
Duration of speed reduction?			
Is traffic management used in relation to heavy users?			Y/N
Under what circumstances?			
Level of speed reduction?			
Duration of speed reduction?			
Section 2: Traffic management to optimise network utilisation (what happens during busy times and places in addition to traffic management as described in section 1)			
Is traffic management used during peak hours?			Y/N
When are typical peak hours?	Weekdays:		Weekends:
What type of traffic is managed during these periods?***			
Traffic Type	*Blocked*	*Slowed down*	*Prioritised*
Peer to Peer (P2P)			
Newsgroups			
Browsing/email			
VOIP (Voice over IP)			
Gaming			
Audio streaming			
Video streaming			
Music downloads			
Video downloads			
Instant messaging			
Software updates			
Is traffic management used to manage congestion in particular locations?			Y/N
If so how?	The same practices are applied as during peak hours		

*This KFI gives an overview of typical traffic management practices undertaken on this product; it does not cover circumstances where exceptional external events may impact on network congestion levels.

**This excludes any service, content, application or protocol that an ISP is required to block by UK law and child abuse images as informed by the list provided by the Internet Watch Foundation.

***If no entry is shown against a particular traffic type, no traffic management is typically applied to it.

Glossary

Traffic management:

Traffic management is the term used to describe a range of technical practices undertaken to manage traffic across networks.

The different outcomes achieved by the use of technical practices can include:

- the prioritisation of certain types of traffic in busy times or busy areas to ensure that it is of an adequate quality
- the slowing down of certain traffic types that are not time-critical at busy times or busy places
- ensuring compliance with a consumer's contract, for example slowing down of traffic for the heaviest users
- supporting the delivery of managed services, for example to ensure a guaranteed quality of service for a specific piece of content

Managed services: The majority of internet traffic is delivered on a "best efforts" basis. A managed service, on the other hand is one whereby an ISP offers "quality of service" that can guarantee a certain level of performance, so that the content, service or application can be delivered without risk of degradation from network congestion. Such a quality of service arrangement can be made between an ISP and a content or service provider or directly between an ISP and the consumer.

Best Efforts: This phrase relates to the delivery of internet traffic where traffic management is applied without distinctions based on the source of that traffic.

Slowed down: This outcome is achieved by the deployment of technologies that can decrease the priority of traffic types deemed to be non-time critical on the network e.g. slowing down traffic such as downloads during busy times and busy periods.

Prioritised: This outcome is achieved by the deployment of technologies that increase the priority given to certain traffic types, e.g. time-critical traffic such as video. This outcome can also be achieved as a consequence of slowing down other selected traffic which reduces the overall data flow on the network.

Heavy users: Heavy users can cause peak traffic volumes to exceed the engineered maximum load. In practice this refers to a very small proportion of users of a network whose use is excessive to the extent that it impacts on other users.

Signatories

Update as per May 2013:

In addition to the founding signatories of the code:

BSkyB

BT

EE

O2

TalkTalk

Three

Virgin Media

Vodafone

The following additional ISPs have subsequently signed up to the code since its launch in March 2011:

BE

giffgaff

KCOM

PlusNet

TescoMobile

Annex C – Open letter to Ed Vaizey

Dear Minister,

The Open Internet

We welcome your recent statement that the UK Government supports access to the open Internet. In particular we support your call for adherence to the openness principle both for fixed and mobile access to the Internet, whereby

- "*consumers should always have the ability to access any legal content or service,"*
- *"content and service providers should have the ability to innovate and reach end users*."

This is the first time that such a clear political commitment has been made in the UK to preserve the end-to-end principle that underpins the Internet, and the benefits it brings to citizens, consumers, businesses and economic growth.

In order to safeguard these benefits for all stakeholders in the future, five key principles are important complements to this political commitment:

- The Internet should remain open so that everyone is able to send and receive the content, use the services and run the applications of their choice, on the device of their choice, within the law.
- Traffic management should be kept to a minimum, and deployed for purely technical, security or legal reasons. There should be no discrimination in the treatment of Internet traffic, based on device, or the origin and/or destination of the content, service or application.
- Meaningful information about any traffic management practices must be made available to all stakeholders, end users and businesses who rely on broadband infrastructure to reach their customers.
- Future investment in network capacity and underlying infrastructure must take place in a way that is consistent with the end-to-end principle and where new models of Internet access do not compromise openness.
- For competitive markets to function effectively, the regulatory framework must be fit for purpose and able to respond to abuses by network providers.

End-users' choice of which applications, content, and services to view, use or run is already restricted in the UK today, especially when accessing the Internet on mobile. The Government's commitment to the open Internet must be reflected in action on the ground to remove any such arbitrary restrictions to the open Internet. We also recommend the Government's policies on the open Internet and traffic management take account of citizens' access to public services online in the future.

In conclusion, we call on the UK Government to add more detail to its position in support of the open internet by:

- Protecting the open internet through a judicious implementation of the new EU legislation for electronic communications.

- Requiring Ofcom to closely monitor the market and demonstrate that effective and timely enforcement processes are in place to respond to complaints about unfair discrimination from any affected stakeholder.

- Pressing UK Internet service providers to urgently develop meaningful self-regulation to ensure fair principles around traffic management to serve as a benchmark for assessing what is or is not acceptable practice, as has been done in other countries. Ofcom should step in if ISPs do not deliver this in a timely way.

- Ensuring that Ofcom's forthcoming review on switching delivers real benefits to broadband subscribers in terms of their ability to change providers and drive meaningful choice between broadband Internet packages.

- Conducting a wide-ranging policy debate about this crucial subject for the future competitiveness of the UK's economy and well-being of UK society, and adopting a joined-up approach in policy making, by assessing long-term implications of traffic management practices and the maintenance of an open Internet for the economy, for consumers and citizen's interests, including freedom of expression, access to public services and digital inclusion.

The letter was signed by: Coadec, Ariadne Capiral, Consumer Focus, eBay, Eden Ventures, IMRG, the NUJ, the Open Rights Group, the Oxford Internet Institute, Reevoo, Skype, Techhub, Truphone, The Filter, We7, Which, XIX, and Yahoo Europe.

Imprint

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany
Phone: +49 2224 9225-0
Fax: +49 2224 9225-63
eMail: info(at)wik.org
www.wik.org

Person authorised to sign on behalf of the organisation

General Manager and Director	Dr Iris Henseler-Unger
Director Head of Department Postal Services, Logistics, and Transport	Alex Kalevi Dieke
Authorized Signatory Head of Department Cost Modelling and Internet Economics	Dr Thomas Plückebaum
Director Head of Department Regulation and Competition	Dr Ulrich Stumpf
Authorized Signatory Head of Administration	Karl-Hubert Strüver
Chairman of the Supervisory Board	Winfried Ulmen
Registered at	Amtsgericht Siegburg, HRB 7225
Tax No.	222/5751/0722
VAT-ID	DE 123 383 795