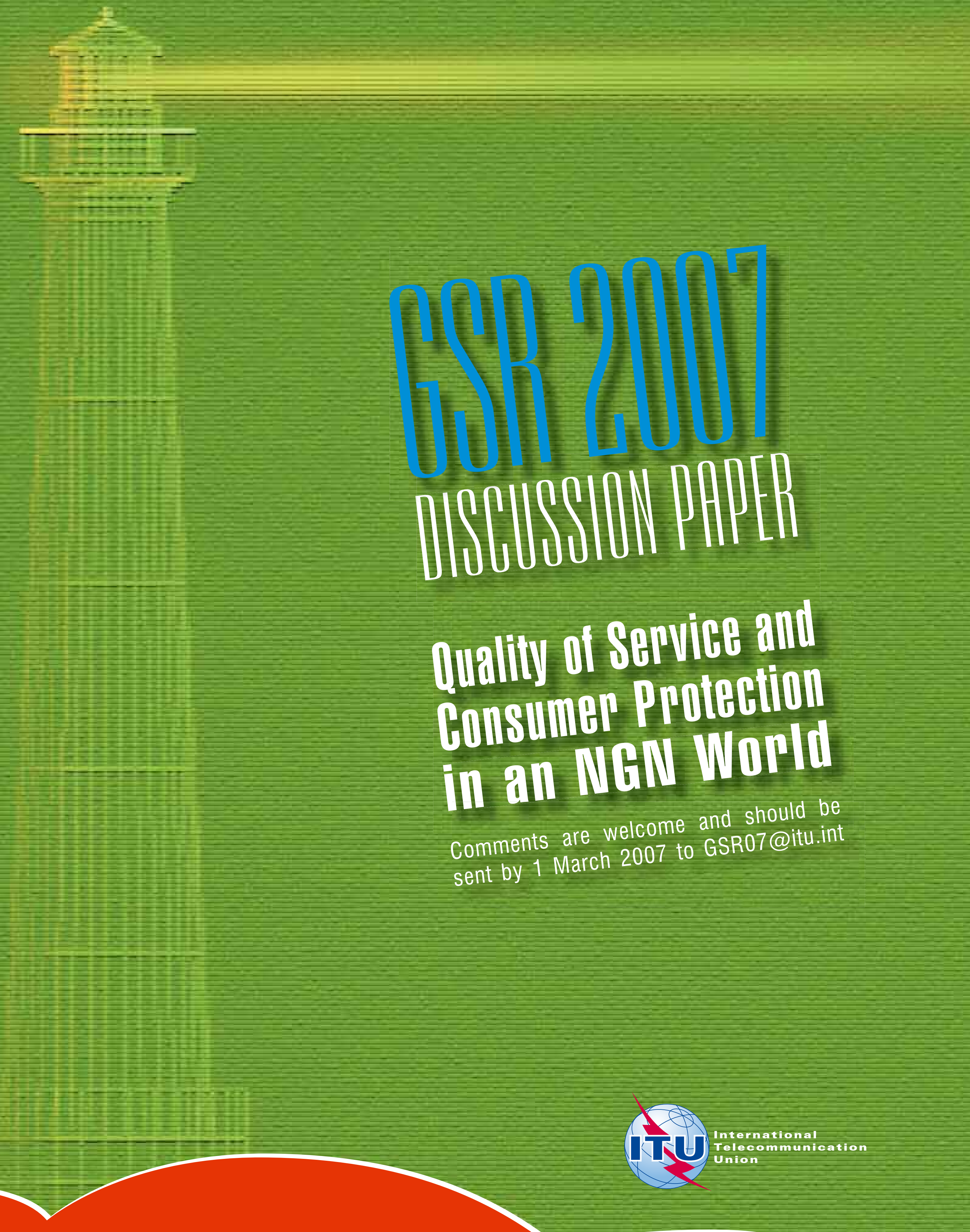
International Telecommunication Union



GSR 2007

DISCUSSION PAPER

Quality of Service and Consumer Protection in an NGN World

Comments are welcome and should be sent by 1 March 2007 to GSR07@itu.int

International Telecommunication Union

GLOBAL SYMPOSIUM FOR REGULATORS

Dubai World Trade Center
Dubai, United Arab Emirates

5-7 February 2007

Work in progress, for discussion purposes

CONSUMER PROTECTION AND QUALITY OF SERVICE (QoS), INCLUDING NETWORK NEUTRALITY AND CYBER-SECURITY ISSUES

Prepared by Rosalind Stevens-Strohmann, Consumer Policy Manager
OFCOM

Comments are welcome and should be sent by 1 March 2007 to
gsr07@itu.int

TABLE OF CONTENTS

GSR DISCUSSION PAPER

CONSUMER PROTECTION AND QUALITY OF SERVICE (QOS), INCLUDING NETWORK NEUTRALITY AND CYBER-SECURITY ISSUES

This paper has been prepared Rosalind Stevens-Strohmann[1]*, Consumer Policy Manager, OFCOM, as an input document for the 2007 Global Symposium for Regulators (GSR), organized by the Telecommunication Development Bureau (BDT). The views expressed in this paper are those of the author and do not necessarily reflect the opinions of the ITU or its membership. Comments are welcome and should be sent to gsr07@itu.int by 1 March 2007.*

1 Introduction

The deployment of Next Generation Networks (NGN, using IP connectivity to support fixed, wireless and mobile voice, video, data, and broadcast TV services, provides new opportunities to increasing consumer choice. It also raises new challenges for Quality of Service (QoS) and for consumer protection.

Consumers have certain expectations of the quality of their communication service, primarily based on their past experience of the well established PSTN voice quality. However the increasing amount of choice of products available to them through NGN may well alter their perceptions of and satisfaction with the overall QoS provided.

In order to take full advantage of the choices on offer, consumers need to be equipped with the necessary skills and information to make fully informed purchasing decisions. They need access to comparable, reliable and independent information about price, quality and service features to empower them to switch with confidence.

The level of regulatory intervention required will depend in part on the structure of the market concerned and the commercial incentives for service providers. Where there is effective competition and commercial incentives for service providers the focus is likely to remain on consumer empowerment, enforced where necessary through transparency requirements. Where competition or commercial incentives are weak, regulators (NRA) may need to take a more interventionist approach, for example through setting and monitoring minimum QoS standards that are appropriate to the NGN environment.

Even the most well informed consumer may still need protection against threats to cyber security, such as identity theft by phishing, malicious virus dissemination via SPAM, the transmission of harmful content, etc. It is probably too early to predict whether these problems will be exacerbated by the deployment of NGN. For example, whereas the increasing sophistication of core NGNs has the potential to improve authentication and tracking procedures, this does not rule out the emergence of new scams and security threats. This chapter also describes the current cyber security issues and considers the options currently available for combating them.

2 Quality of service

2.1 Current QoS practices

From a consumer experience perspective, the regulatory approach to QoS for established PSTN networks is two dimensional[1]:

[1] The author is a Consumer Policy Manager at the Office of Communications (Ofcom). Although she has sought the opinions of her colleagues and referred extensively to Ofcom policy documents when writing this chapter, the opinions expressed are her own and do not necessarily represent Ofcom's views.

- Enforcement approach: whereby the NRA defines the QoS parameters and benchmark standards with which operators must comply.
- Encouragement approach: whereby the NRA relies on competition and publicity to empower consumers to make informed choices and switch providers.

In practice, NRAs are likely to adopt a mixture of the two. Within the European Union, the regulatory framework for QoS reporting is part of consumer protection legislation enacted through the Universal Services Directive.[2] The QoS requirements allow individual NRAs both flexibility and discretion as to whether to impose minimum quality of service standards and the parameters to be measured. This is important as the measures likely to be of most interest consumers are constantly evolving. For example, Annex III of the EU Universal Services Directive[3] did not include a parameter measuring delay before getting a dial tone, as this was no longer considered relevant to digital networks.

Box 1: The evolution of QoS monitoring in the EU

Annex III of the EU Universal Services Directive sets out the quality of service parameters, definitions and measurement methods to be used by NRAs to monitor the performance of designated undertakings with universal service obligations. NRAs may also require all providers of publicly available electronic communications services (PATS) to publish comparable QoS performance indicators for end-users, using Annex III parameters where appropriate.

Annex III Quality of service parameters: in accordance with ETSI EG 201 769-1 version 1.1.1 (April 2000) definition and measurement method.

Supply time for initial connection
Fault rate per access line
Fault repair time
Unsuccessful call ratio*
Call set up time*
Response times for operator services
Response times for directory enquiry services
Proportion of coin and card operated public pay-telephones in working order
Bill correctness complaints

* *Member States may decide not to require that up-to-date information concerning the performance for these two parameters be kept, if evidence is available to show that performance in these two areas is satisfactory.*

In the United Kingdom, for example, Ofcom has directed fixed voice providers to publish QoS parameters covering supply times; fault rates and fault repair; complaints resolution and upheld billing complaints[4]. Ofcom does not set or monitor benchmark standards for the parameters. Instead the results are published on an independent website (www.topcomm.org.uk) which enables consumers to compare QoS across providers and empowers them to switch if dissatisfied. The mobile operators are not directed to publish QoS information but are encouraged to do so. Comparable, independent information on mobile network voice call quality is updated fortnightly on an independent website (www.topnetuk.org). All of the measures are subject to review, with a view to extending the initiatives to include, for example, broadband QoS and mobile customer service.

Beyond the European Framework, NRAs have developed and employed a wide range of service indicators to meet the requirements of different markets[5]. In India for example, the TRAI requires operators to provide information about several categories of QoS indicators, covering[6]:

- Development eg telephony and payphone penetration, or growth in access lines;
- Network performance eg call completion rates;
- Customer service, including quantitative and qualitative aspects.

As well as requiring both fixed and mobile operators to publish the indicators on a quarterly basis, TRAI sets performance targets, which are reviewed annually with a view to encouraging improvements in standards[7].

Many countries continue to prescribe minimum standards for basic telephony services. In Brazil, for example, there are 36 different indicators and all licensed operators must comply with minimum QoS standards. Fines remain the most common way to enforce compliance. In Brazil, the NRA may impose a fine of up to USD $40 million for failure to comply.

In some countries the minimum QoS standards may be linked to price cap regulation. For example in the U.S. a QoS variable "Q" is included in the price cap formula. A similar approach has been adopted by the Colombian regulator. If service quality erodes, this will be reflected in lower prices for consumers, whereas if quality improves higher prices may be allowed. The NRAs are likely to consider imposing minimum QoS standards should quality fall to an unacceptable level.

Box 2: ITU QoS Indicators

The ITU includes QoS indicators for up to 206 economies it its annual World Telecommunication Report. It has also established a set of measures, which are published in the ITU Telecommunication Indicators Handbook[8]. These include:

- The length of waiting lists for main lines
- The percentage of telephone service faults cleared by the next working day.
- The percentage of failed calls.
- The number of telephone main line faults.
- The percentage of calls for operator service answered within 15 seconds.
- The number of complaints per 1,000 bills.

The customer satisfaction rate.

This chapter focuses on the "encouragement" approach which Ofcom has taken. This is because in order for QoS initiatives to be meaningful to consumers the information must keep pace with changing technological and market developments. The communication providers are best placed to provide the relevant QoS indicators in a timely fashion.

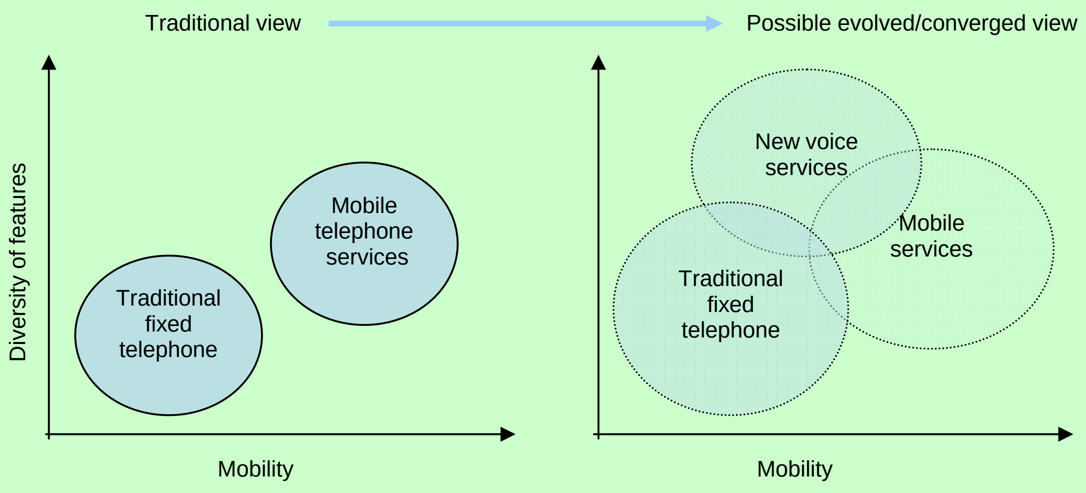
However, the ability to provide meaningful data does not necessarily mean that communication providers will be willing to provide it without regulatory intervention. As competition increases, there are clear incentives for providers with a high quality of service to produce and promote timely and accessible QoS information for consumers. Conversely there is no economic incentive for those providers offering a low quality of service to do the same[9]. In the United Kingdom, this issue is addressed by targeting enforcement action on a provider which fails to comply with the QoS Direction. A company that fails to publish QoS information as prescribed risks a fine of up to 10% of turnover.

For those readers who wish to learn more about various enforcement approaches taken on more global scale, there are a number of detailed studies, together with further information about QoS parameters, benchmarks and measurements[10]. There is also a comprehensive ITU website available, the Global Regulators Exchange (www.itu.int/grex), where NRAs exchange information about their practices with regard to setting parameters, measuring compliance and handling enforcement.

2.2 Quality of Service: Issues for NGN

NGNs support a converged communication framework using internet protocol (IP) based packet technologies on top of various transport technologies eg cable television (CATV), wireless and mobile technologies, etc. This facilitates the provision of multiple services to consumers, including voice, data and multimedia. The associated disaggregation of the service or application layer from the transport layer reduces the barriers for consumers wishing to access services provided by competing service providers.

Fig. 1: Evolution and convergence of new voice services


Traditional view
Possible evolved/converged view
Diversity of features
Traditional fixed telephone
Mobile telephone services
Mobility
New voice services
Mobile services
Traditional fixed telephone
Mobility

Source: Robert Milne (Antelope Consulting)

There are a number of QoS-related aspects that need to be addressed as NGN is deployed. These include:

- Service disruption during the migration from PSTN to NGN.
- Management of end-to-end voice quality of service.
- Access to emergency services and emergency call location.
- Number portability.
- Feasibility of alternative text relay services.
- Differentiation of QoS.
- Network integrity.
- Network security.

From a customer perspective, quality of service may relate to the communication service itself eg voice quality, picture quality, delay, speed, etc. It may also describe the quality of customer experience when interacting with the communication provider eg whether the bills received are accurate, how quickly a service is provided, how likely it is that there will be a fault with the service and how long the provider takes to repair it, how long it takes the call centre staff to answer the telephone and how helpful they are, etc. To avoid disappointment and complaints later on, customers need to be aware of the service levels they can expect before signing a contract for a product or service. This is especially important where a bundle of services is provided under the same contract.

However in order to identify the parameters most likely to satisfy and/or improve the customer experience, a technical perspective is required. In relation to NGN, it may be useful to differentiate between real-time interactive services, eg voice and video telephony; real-time non-interactive services, eg television transmission; and near real-time interactive services, eg instant messaging. For voice telephony it will always be important to control delay, jitter, error rate and packet loss, otherwise the consumer experience is likely to suffer. This is also true for video telephony, which also demands a higher guaranteed bandwidth to maintain a certain quality of service. Delay is less important for delivering quality in “streaming” services like television and for instant messaging only a minimum level of service quality across the parameters is needed to satisfy consumers.

2.3 Migration from PSTN to NGN

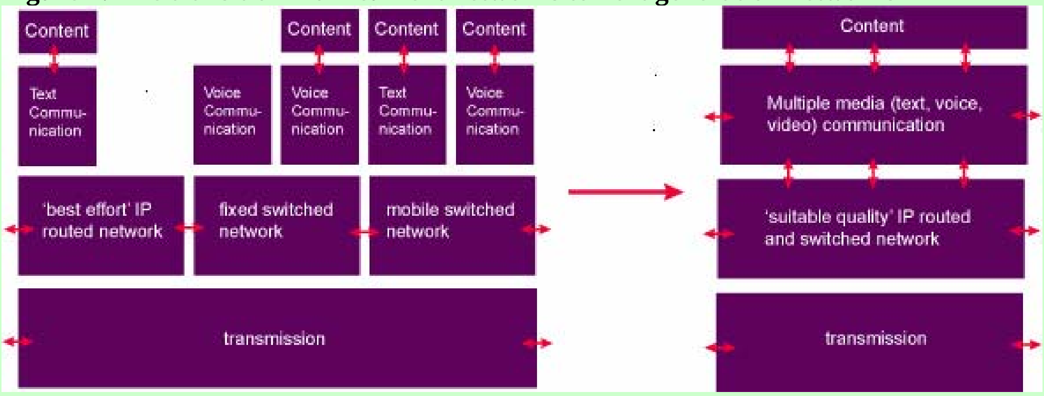
A key consideration for NRAs is to ensure that consumers do not suffer any loss or degradation of service during the migration to an NGN. It is also essential that consumers are fully informed about the transition and know what to expect. In the United Kingdom, BT recently began rolling out its 21CN network on an area by area basis. It has launched a special consumer information website, http://www.switchedonuk.org/home/, which helps consumers find out when the migration in their area is likely to happen, and how it is likely to affect them.

2.4 Management of end-to-end Voice QoS

The voice planning process in traditional telephony, whilst complex, is relatively straightforward. Environment, transmission, switching and voice communication services are provided by dedicated networks. It is possible to ensure voice quality by allocating dedicated bandwidth for the duration of each call.

In the NGN environment, a single network supports multiple service types (as illustrated in Figure 2 below). In order for NGNs to achieve the same grade voice quality, there needs to be either a system of network protocol prioritization or allocation of additional capacity. If not, voice calls may fail due to lengthy queuing delays, which happen during periods of congestion.

Figure 2: The transition from current networks to next generation networks



Source: Robert Milne (Antelope Consulting)

The emergence of NGNs is already driving much of the change in the way voice services are delivered. For example, whereas some of the new voice services such as Voice over IP (VoIP) have the potential to 'look and feel' like traditional telephone services, they may not be able to deliver over the Internet the same features or standards consumers have come to expect from a PSTN-grade voice service

The reliability and performance of a VoIP service depends on a number of elements. VoIP traffic will typically include signalling and media data, which take diverse routes through an IP network. For example, for a VoIP service running over an xDSL network, reliability will be affected by the quality and reliability of the PC, software and adaptor; the local access; the broadband access network (including the Digital subscriber line access multiplexer (DSLAM), Asynchronous transfer mode (ATM) and IP network); the core IP network and Internet peering arrangements; the service and application layers (e.g. home subscriber server, call server and media gateways) and interconnection into other networks.

A VoIP provider can only guarantee technical QoS standards to the extent that it is possible to control the end-to-end parameters of the network employed. In respect of the service/application and network layers there are a number of steps a VoIP service provider (including those offering nomadic services) can take in respect of those elements over which they have control:

- Engineer the VoIP service to minimise latency (which is the consumer's experience of network delay) and specify minimum requirements for use of the service, e.g., bandwidth and traffic control[11]. (However if the public Internet is used, the QoS is not guaranteed and the user experience will be variable.)

- Make the VoIP traffic a priority in terms of QoS within an IP network in accordance with an agreed DiffServ or IntServ class of service scheme which is then used between interconnected Ipv4 networks and may be maintained both in IP headers (precedence bits) and interconnected MPLS networks (EXP bits)[12].

- Design their networks to minimise routing hops, providing sufficient redundancy including call servers, gateways and network capacity, to deal with any throughput issues during re-routing or congestion

- Proactively manage any customer premise equipment (CPE) to dynamically alter the properties, such as packet and/or window size[13], to maximise throughput for voice traffic in response to observed network performance.

- Implement deep packet inspection to identify and prioritise voice traffic in those parts of the network over which it has control.

- Implement home subscriber server, gateways and call servers close to significant sources and sinks of traffic to other networks.

- In the case of an xDSL service, use the associated PSTN line for emergency access to ensure that in the event of power failure emergency calls would be routed to the associated PSTN line by use of software or control in the CPE/broadband adaptor.

The distinctions between mobile and fixed services are also likely to become harder to draw in future as new services start to offer some form of mobility and enhanced functionality. For example, in the UK there are already packages available that combine VoIP, mobile search, instant messaging and online auction services with mobile access to home TV content and to music, video and other digital content on users' home PCs.

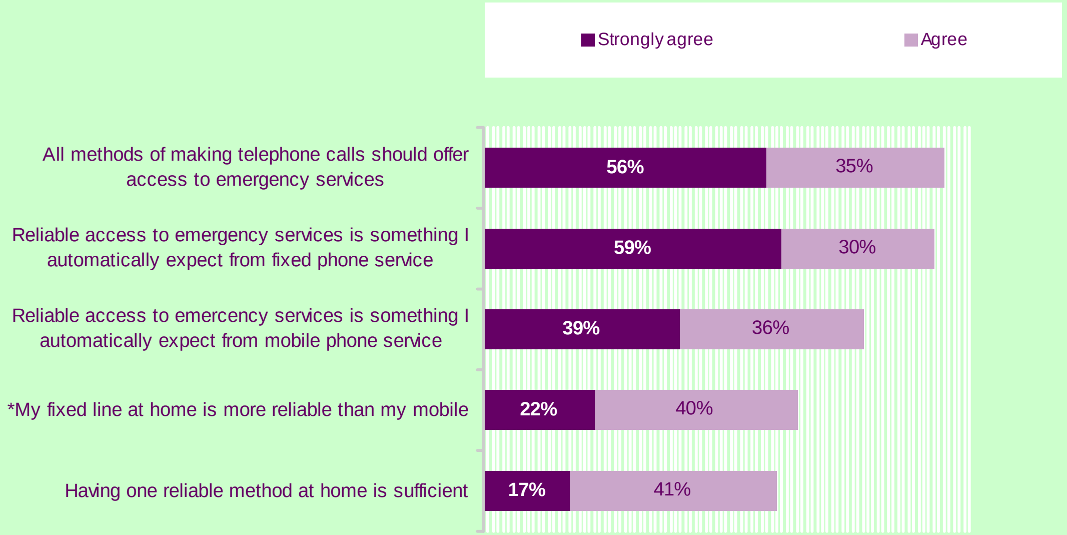
These trends are likely to affect both the type and quality of the services offered in the market. For example, with some routine Internet activities such as web browsing and email all that is normally required is sufficient bandwidth. The IP-protocol should not as rule experience any difficulty with delay, jitter etc. However as consumers demand more interactive functions such as conversations and video-conferencing, a low level of end-to-end delay and jitter, low packet loss, and a guaranteed bandwidth are all needed to ensure standards are maintained.

2.5 Access to emergency services and provision of emergency location information

Whereas traditional PSTN networks are normally line powered, VoIP services are dependent on mains power for their terminal equipment. Some VoIP services may not offer any access to emergency calls or reliability of the access may be affected by a power cut or power failure, or through failure of a broadband connection.

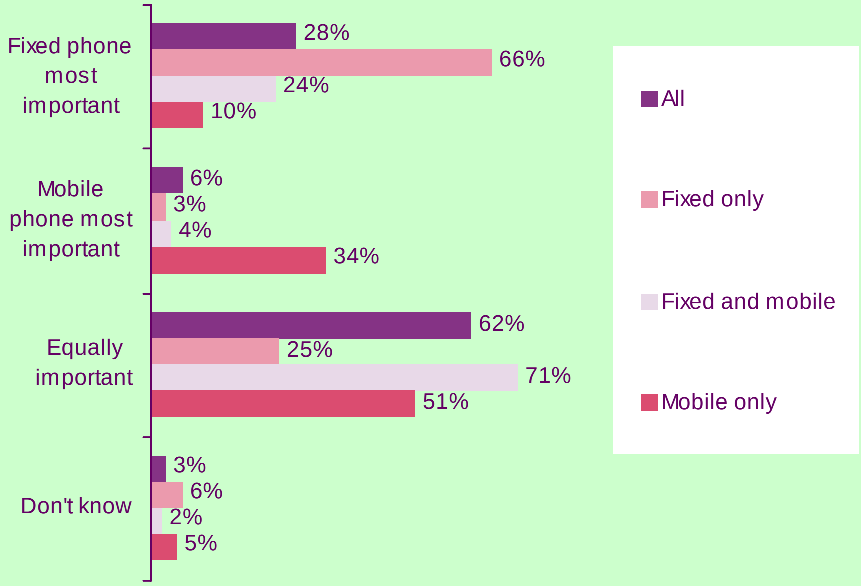
As figures 3 and 4 below illustrate, consumer expectations do not seem to accord with the actual situation, with most expecting access to emergency services through their fixed line phone service.

Fig 3: Consumer attitudes towards accessing emergency services



Source: Ofcom survey UK residents 2006
Base: Adults aged 15+, (Base: 883), with a fixed line at home who also personally use a mobile

Fig 4: Most important device in home for reliable access to emergency services



Source: Ofcom survey conducted by NOP World Base: GB adults aged 15+, May ’2004 (Base: 883)[14]

There have been a number of significant changes in the regulatory arena and wider policy debate in relation to VoIP services. For instance, following high profile incidents in the US in 2005, the FCC changed its relatively liberal regulatory environment to one where VoIP services that interconnect with the PSTN (that is, that allow calls to or from traditional telephone lines/numbers) must provide access to emergency services, in line with the requirements that apply to incumbents[15].

The EU Regulatory Framework[16] requires Member States to put in place arrangements to ensure that calls to emergency services are adequately answered and handled. Caller location information should also be made available to emergency services operators.

The obligation to provide access to emergency services applies to providers of publicly available telephone services ("PATS"), namely if, and only if, all of the following core elements are satisfied:

- The service is 'available to the public';
- 'for originating and receiving national and international calls and access to emergency services';
- 'through a number or numbers in a national or international telephone numbering plan'.

This situation creates a number of inter-linked potential challenges in relation to the regulation of VoIP services.

First, certain PATS obligations eg the requirement to provide uninterrupted access to the emergency services, could impose a burden on VoIP service providers who want to offer PATS services, in that it could discourage market entry and thus service innovation.

Second, the potentially high regulatory burden of meeting certain PATS obligations could create a disincentive for providers to offer access to emergency services, even on a 'best efforts' basis. This disincentive arises since, by not offering emergency access, a VoIP service would not constitute PATS. This raises concerns in relation to consumer protection, particularly where the VoIP service is the only one available to the household.

Third, relates to the provision of consumer information. Both PATS and non-PATS VoIP services may differ from traditional PSTN voice services, eg in terms of availability of emergency access and the reliability of the QoS. This means there is a risk that consumers are insufficiently informed and protected.

Given the wide diversity in regulatory approaches across the EU, the focus has been on consumer information requirements to ensure consumers can make informed choices. This approach is set out in a common statement on VoIP, published by the European Regulators' Group (ERG) in 2005[17] and in a recent report on VoIP and consumer issues.[18]

In the United Kingdom, Ofcom has consulted on a number of proposals[19] designed to encourage providers of VoIP services to help maintain a high level of good quality access to emergency services. The proposals for consideration include:

- a regulatory requirement on all providers of voice public electronic communication services (PECS) to offer access;
- setting more stringent network integrity requirements eg requiring battery back up;
- modifying the consumer information requirements to ensure consumers are aware of the impact of non-availability of access.

Emergency location information is also important to emergency services as the information is used to dispatch and monitor relevant emergency assistance. In the PSTN network a termination point is matched with a caller's location, which can be identified from the caller line identification (CLI). For VoIP providers who do not use or assign an E.164 number (see below) as a user identifier, this is no longer feasible. Industry is therefore being encouraged to develop solutions to overcome any technical limitations to the provision of location information and adequate routing of emergency calls.

The ERG has acknowledged that in future it may be necessary to update emergency service centres and emergency services to accommodate VoIP and other means of communication eg through a SIP address for emergency calls, an SMS number (112) for emergency SMS messages, an e-mail address for emergency messages, etc. Further requirements will be discussed once the technology and standards have matured.

2.6 Number portability

Number portability plays an important role in the promotion of competition and benefits consumers by removing the cost and inconvenience of having to change telephone numbers when switching providers.

The central issue in number portability is how communication providers route calls and messages to numbers that have been ported. In order to route calls correctly, providers need to know the location of the destination number, based on a number range analysis.

Although the regulation of number portability has not changed materially over the past decade, there have been major changes both in the nature of competition and in the way in which services are provided. In particular, there has been increased convergence between services that have traditionally been regarded as "fixed" and "mobile" services, and a rise in the number of services using VoIP. Concerning the latter, according to the EU Universal Services Directive, only subscribers of publicly available telephone services (PATS) have the right to number portability. This may lead to restrictions for the availability of number portability in VoIP services.

Increasingly therefore the distinction between the geographic location of a fixed number and between fixed and mobile numbers is being eroded and the deployment of NGN architectures will further erode the association of area number codes with a fixed location.

Many NRAs have already established a technology neutral numbering plan to allow for technological innovations and number portability, in accordance with the ITU-T E.164 recommended international public telecommunication numbering plan. At present E-164 is still required for the origination and receiving of VoIP calls from traditional voice services and is likely to remain important for VoIP services in the foreseeable future. Moving forward it may prove necessary to modify numbering plans and open up new number ranges, for example, to distinguish between general purpose, nomadic and ENUM-based services[20].

In the United Kingdom, Ofcom is considering the implementation of number portability within the context of the development of NGNs in UK[21]. The present analysis seems to favour transition of the current onward routing solution for routing of calls to ported numbers to an all-call query of a common database of numbers ("ACQ/CDB") solution, both for fixed networks in transition to NGN and or mobile networks. Implementation would require timely agreement by industry of technical standards as well as the commercial framework for design, build and in-life management of the database

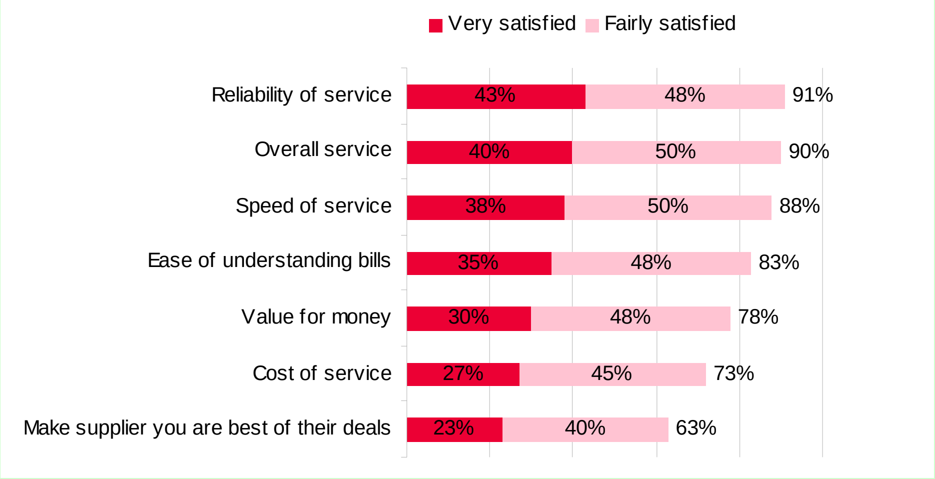
2.7 Feasibility of alternative text relay services

For people with disabilities, the deployment of IP based technologies may present new difficulties. For example, some text phone services may not work on a VoIP connection or may fail mid-conversation. Hearing aid wearers may experience feedback when using a VoIP phone or find that their hearing aid is incompatible. In the longer term however there is plenty of potential for VoIP to make telephone communication easier for people with a hearing loss, because with VoIP there is the theoretical possibility of transmitting frequency ranges that are more readily heard by individuals with a hearing loss.

2.8 QoS: What matters for consumers?

Consumers have certain expectations about the quality of service of a communication services, based on previous experience of the well-established PSTN, mobile and Internet services. Consumers are highly unlikely to consider QoS from a technical perspective. Rather, they tend to focus on customer-related aspects of the service they receive from providers eg reliability, speed, etc. This is illustrated in Figure 5 below, which shows the results of an independent consumer survey undertaken for Ofcom, in which consumers are asked to express their satisfaction with different elements of their internet service.\

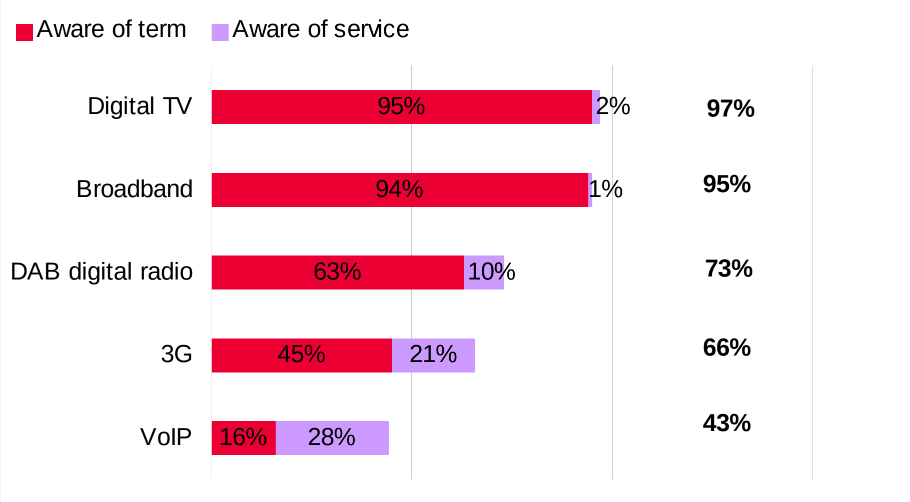
Fig 5: Satisfaction with internet service providers



Source: Ofcom Communications Tracking Survey Q3 2006. Base: All adults with the internet at home n=1116

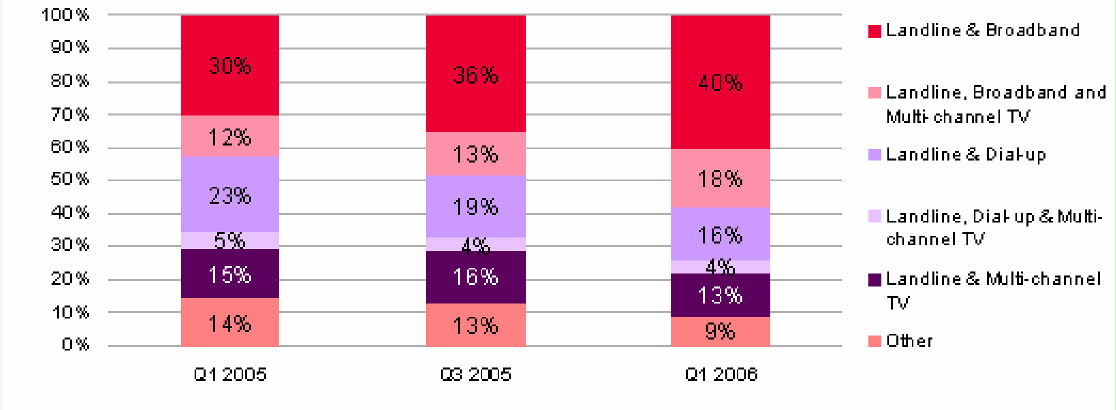
Independent research commissioned by Ofcom during 2006 found that UK consumer awareness of the products and services available through new technologies is high, and take up is increasing. The starting point for comparison is a high level of overall satisfaction with fixed and mobile services. Increasingly consumers are buying a bundle of services from one provider and they are likely to expect, at least initially, a similar quality of service for each element of the bundle.

Fig 6: Awareness of technology and the services this technology makes available



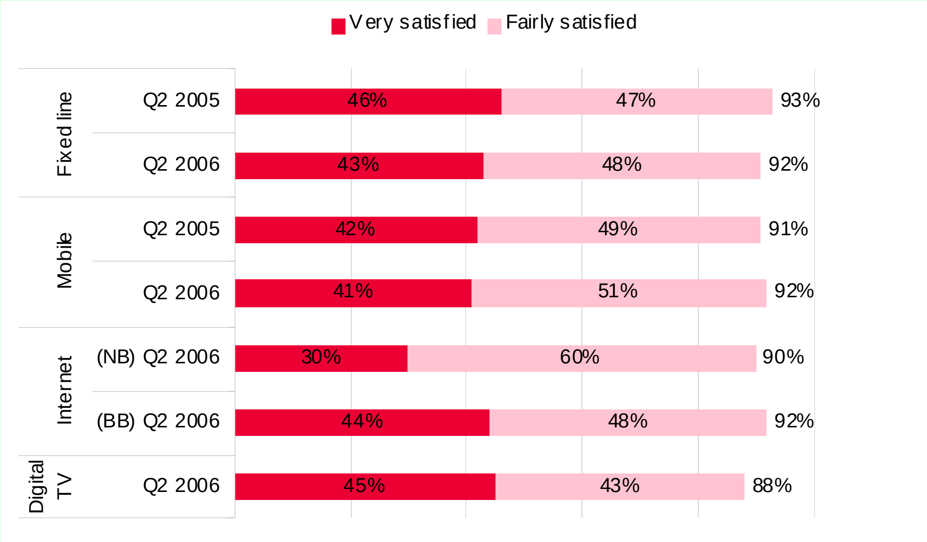
Source: Ofcom Consumer Panel survey, conducted by Saville Rossiter-base during October-November 2005. Base 2689 UK adults

Figure 7: Trend in purchasing multiple communications services from a single supplier



Source: Ofcom Communications Tracking Survey, conduced by IPSOS-MORI Bases Q1 2005(640), Q3 2005 (681) and Q1 2006 (686) UK adults who bundle at least two services

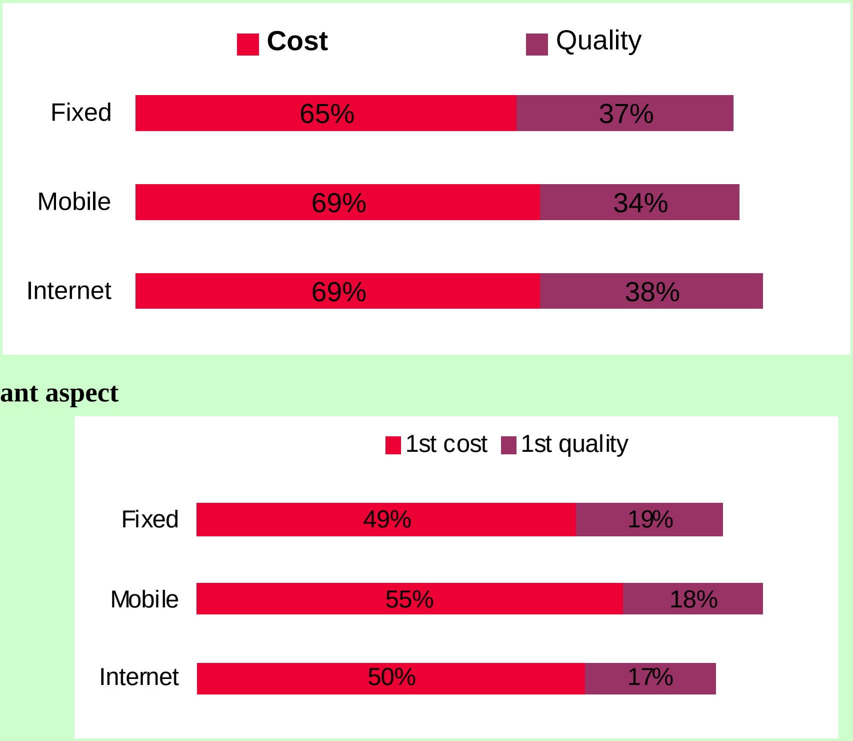
Fig. 8: Satisfaction with overall services over time



Source: Ofcom Communications Tracking survey, conducted by Ipsos- MORI Q2 2005 and Q2 2006 Bases: UK adults 2439. Don't knows have been excluded.

Quality of service is consistently mentioned by consumers as the most important factor after price when choosing a new supplier. However, around a third of consumers find it difficult to make quality of service comparisons, with only 43% of fixed line customers and 51% of mobile customers finding it easy. Most consumers say they find it easier to compare costs than to compare quality of service.

Figure 9: Importance placed on cost and quality when choosing a new supplier



Total mentions of cost and quality

Most important aspect

Source: Ofcom Strategic Review of Telecommunications., Research Annex. Base: 1586 UK fixed decision makers, 1303 mobile decision makers, 715 Internet decision makers, May-June 2004, MORI

The deployment of NGN adds a new dimension and increased complexity to the consumer purchasing decision and satisfaction levels, namely choice of services available and the differential quality of service they may experience. Consumers are increasingly likely to have experienced degraded quality or loss of service eg on international calls over satellite and/or Digital Circuit Multiplication Equipment (DCME) compression, mobile to mobile calls with low signal strength and "free" VoIP services. These may alter their perception of and satisfaction with the overall QoS provided.

Some consumers may demand a higher quality of service than they currently experience, which could be provided, for example, through wide-band speech [22], or expect the same level of service from a different technology, for example IPTV.

Consumer may be prepared to pay more for faster Internet speeds and access to new content and applications. In turn, this may lead to a more transparent quality of service-related pricing mechanisms, provided consumers demand the relevant QoS information needed to differentiate between the products and services on offer. What is not clear is whether consumers will be prepared to "trade" quality for the more choice of products, services and features.

The challenge for regulators going forward will be to ensure that consumers have access to transparent, comparable, reliable and up to date price and quality of service information that helps them to make increasingly complex choices and the potential for differential product and service offerings. Such initiatives are most likely to succeed if provided through independent, industry led initiatives as these are more flexible and capable of keeping pace with the dynamics of the marketplace.
In order to achieve this it is essential that consumers are aware of the availability and importance of comparative QoS indicators. Ofcom is considering various ways to achieve this objective. For example, in

December 2006, Ofcom launched its consumer advice portal http://www.ofcom.org.uk/consumeradvice/. This provides advice on the most useful questions asked by consumers and is designed to help them choose the best product and service for them. The portal includes links to price and QoS comparator sites.

3 Net neutrality

The expression "net neutrality" usually refers to the debate around whether there should be an overarching principle of non-discrimination regarding different forms of internet traffic carried across networks. At the extreme this would imply:

- No prioritisation of applications or one application provider's traffic over another.
- No deliberate degradation of applications or an application provider's traffic.
- No charging application providers for a higher quality of service.
- No deliberate blocking of any one application or an application provider's traffic.

The debate originated in the U.S. triggered by changes made to the way in which broadband networks were regulated, namely as information services and not telecommunication services. This has led to an increase of market power at the retail ISP level.

Those in favour of net neutrality argue that to date the Internet has treated different types of traffic equally and has been free. However, the Internet has never really been neutral. Operators, content providers and consumers all have to make payment to access content in various ways. A number of business models have evolved which require inter-operator payments for the delivery of content to end customers. Examples include content provider payments to backbone network providers to host content, either with or without quality of service level agreements (SLA's) or with or without content caching close to the customer.

Box 3: Service Level Agreements (SLAs)

An SLA provides a way of quantifying service definitions by specifying what the end user wants and what the provider is committed to provide. The definitions vary at business, application or network level.
Business SLAs typically cover pricing and contract terms.
Application level SLAs relate to server availability (eg 99% during working hours)
Network SLAs relates to service level specifications such as throughput, latency, packet loss[23].

The net neutrality debate is most typically argued from a supply-side perspective ie whether network operators should be allowed to block, or charge for prioritizing and application provider's traffic. However there is clearly a consumer dimension to net neutrality. Customers have always paid differential amounts for different quality of service from service providers. This can take the form of higher prices for higher bandwidth services, guaranteed quality of service, greater usage caps or managed services. The prioritisation of different types of traffic has clear benefits for consumers. For example, it allows them to pay to access products that are more tailored to their individual needs. They are also likely to benefit from improved network efficiency. If all applications were delivered at a uniform level of service, irrespective of the application's tolerance to say, jitter and delay, all consumers would be paying for QoS requirements that are only relevant for some of the services.

In reality, net neutrality is best thought of as a continuum, with a range of approaches that network operators may adopt to prioritise certain types of traffic and/or traffic from particular providers. It is relevant to QoS because of the potential to change the nature of delivery of traffic from a "best efforts" basis to one of prioritisation according to certain criteria.

The current interest in the topic arises for a number of reasons:

- The majority of internet access in developed economies is now through broadband, mainly priced with flat rate tariffs.

- The availability and increasing popularity of heavy usage applications, such as HDTV, has generated a rapid increase in the volume of traffic on the Internet, which had led to substantial congestion in some parts.
- Some applications are more time sensitive than others eg VoIP services, as compared to music downloads.
- Network routers are more intelligent and therefore capable of identifying and prioritising the packets associated with different applications.

The debate is most controversial where it relates to differentiation between application providers. For example, network operators in the US have argued that they need to be able to charge application providers for high priority traffic in order to support the business case for investment in higher capacity networks that such applications require. The counter argument by those who favour net neutrality is that end users have already paid the operators for access such that prioritisation by the ISPs effectively constitutes charging twice for the same network.

Innovation is also a key consideration. Those who favour net neutrality would argue that some of the most innovative internet applications have been developed through start-up companies who would be either unwilling or unable to pay ISPs to allow end users to access their applications at the required quality of service. If they were made to do so, innovation would effectively cease. Network operators, on the other hand, argue that differential QoS may increase the scope for product and service innovation as it allows new emerging products and services to be supported through prioritisation.

In essence the issue of net neutrality is all about the future of commercial relationships, payment flows and access to markets. Concerns about net neutrality are greatest where an operator with SMP in the relevant market undertakes to prioritize delivery of its own services over those of its competitors for anti-competitive purposes.

Under the European Framework, most incumbents have requirements to unbundle and/or offer wholesale broadband access, facilitating competition in the retail broadband market. The EU's position on net neutrality is that the EU is not at risk of problems in the same way as in the U.S. Provided that an operator with SMP does not discriminate between customers in similar circumstances, the EU does not object in principle to operators offering different services to different customer groups. Where discriminatory behaviour by an operator with SMP is demonstrated to be anti-competitive there are sufficient powers available under the Framework Directive and competition law to deal with any arising issues.

In relation to consumers, the European Commission is concerned that some operators may degrade the QoS of some services offered to consumers (eg "free" broadband) to unacceptably low levels. In its Review of the EU Framework, it makes proposals for amendments that would allow NRAs to mandate a common set of minimum QoS standards for network transmission services. The proposed standards would apply across the EU to all operators, not just those with SMP.

The UK's favoured approach is not to impose uniform minimum QoS standards but to agree a fully transparent set of service level definitions which allow for the ready comparison of services from different providers. Whether or not SMP is an issue, it is essential that service levels and traffic prioritisation, degradation or blocking policies applied by the ISP are fully transparent to operators and consumers. This approach is equally valid where the level of competition in the retail market is weak or non-existent.

There are therefore a number of possible remedies that NRAs may apply as an alternative (or possibly in addition to) net neutrality rules. These could include, for example, obligations to supply, charge caps, minimum quality of service standards and mandating ISPs to provide consumers with information as to whether they block access to certain ports or websites.

3.1 Reducing barriers to consumer switching

For those operators without SMP in the relevant market, the efficient working of a competitive market should address the risks posed to consumers from non-network neutral approaches. An effectively competitive market at the retail level, with relatively low barriers to entry, means that customers have a range of choice in their ISP.

Therefore, if a single operator without SMP were to introduce charging for the delivery of third party content services, or to block specific services, consumers would be able to move supplier. This reduces the incentives for operators to charge consumers excessively high prices or block specific services.

In order for this to function effectively:

- Consumers need to be well-informed and have accurate, comparable and easy to understand information about the nature, price and quality of services as well as complete and accurate information about the transfer process, at the point of purchase.
- There must be no artificial barriers to consumer empowerment, reducing their ability to switch service providers e.g. where a process is not seamless and subjects consumers to a level of unnecessary hassle.
- The migration process from one service provider to another must not unduly influence consumers' decision to switch service provider e.g. where the process is unpredictable and unreliable this may be a factor in stopping consumers engaging in the competitive process.

If this is not the case, then there may be a role for regulatory intervention to protect consumer interests. However, any intervention would be best focused on addressing the lack of consumer information, empowerment or migration processes. Addressing any issues within these three areas would then allow the efficient working of the market and consumer choice.

However, for this to be an effective constraint of the potential for consumer harm, it is essential that there are no unnecessary barriers to switching and that migration processes are efficient and of a high quality. Customers must be able to switch seamlessly between providers and/or products regardless of the nature of the service migration or the underlying technologies involved. This becomes more critical of an issue as more consumers increasingly look to 'bundle' their products and services together.

Competition will only be effective if consumers are confident in the switching and transfer process. Where this is not the case, customers will be unwilling to engage effectively in the competitive process. In order for this to be achieved, there are a number of characteristics that need to be met:

- The customer should control the process and be well-informed throughout
- Where possible, a consistent approach should be used across products and/or services – to make switching easier for customers and competitive providers.
- The customer should be subject to minimal hassle;
- The switching process should be predictable and reliable.
- There should be adequate opportunity for the customer to change their mind.
- The switchover period should be as quick as possible (albeit will need to ensure adequate protection from the risks of mis-selling/slamming).
- There should be minimal customer disruption, including no interruption to service.
- Consumers should be protected against dishonest sales and marketing activity.
- Consumers should have access to essential information including the identity of the company, its address, telephone, fax and e-mail contact details, as appropriate.
- The description of the services to be provided should be sufficient to enable the customer to understand the option that they have chosen, and how it works.
- Consumers should have access to information about the major contractual elements of the service, including the cost of any standing charges, the payment terms, line rental, key call types and details of "protected or special support" arrangements.

- Consumers should understand what the impact of switching will be upon services currently being used, including a clear understanding of which services will be affected/unaffected.
- Consumers should be informed about the arrangements for the provision of the service, including the order process and, as accurately as possible, the likely date of provision. Where there may be significant delay in the likely date of provision, the customer should be informed:
  - the existence of a right of cancellation and the process for exercising it;
  - the period for which the charges remain valid; and
  - the minimum period of contract and minimum contract charges, if any.

In addition it is essential that competition in retail markets is supported by ensuring that switching costs are kept to the minimum necessary. This objective is dependent on many factors. These include the following:

- avoiding ‘unnecessary’ switching barriers for customers;
- ensuring that providers, including prospective new entrants, can access efficient, symmetrical and high quality migration processes to support migration of customers, through efficient back office operations; and
- avoiding distortion to the competitive process through preventing unfair behaviour by providers during the transfer process.

4 Consumer Protection and cyber security

Over the past decade, the internet has grown to become a central part of the cultural and economic life of many people around the world. The internet is a powerful platform for the distribution of services to their intended audiences. It spans the world and connects a global audience with a globally provided set of content and services. The internet’s flexibility means it has been an engine for innovation, enabling the development of new businesses and new business models, new content and new communications services; and its openness has allowed operators of every scale, from multinationals to individuals, to create and offer content and services as well as benefit from them. Alongside global reach, openness and flexibility, many observers attribute the success and importance of the internet to the limited extent of internet service regulation.

The international nature of the internet has generated new opportunities for consumers but it has also put them within easier reach of those seeking to take advantage of them. The internet has given rise to many new types of crime – for example, identity theft by phishing, malicious virus dissemination via SPAM, and online grooming of children. It has also made it easier for criminals to circumvent the law by taking advantage of the impersonal nature of the internet to misrepresent or disguise their true identity. With the advent of NGN and its potential for higher speeds of connectivity, the Internet is likely to play a much greater role in citizens’ lives, increasing the potential for harm.

In response to both the growing role the internet plays in delivering services to consumers and the risks it exposes them to, there has been an immense amount of activity at national and international levels in developing legislative and regulatory frameworks to deal with internet-specific issues. While some of these efforts have sought to achieve international cooperation and harmonisation of laws, many have also been tailored to suit the particular circumstances, and cultural and political norms of local markets.

Box 4: Stemming the tide of international spam

ITU 2004 Global Symposium for Regulators (GSR): proposals for a multi-pronged approach for dealing with spam:

- Anti-spam legislation eg US 2003 CAN-SPAM Act
- Enforceable codes of conduct for ISPs
- Voluntary codes of conduct approved by NRAs
- End-user initiatives eg spam filters

Box 5: ITU Thematic Workshop of Countering Spam 2004: proposals for a five-part approach combining

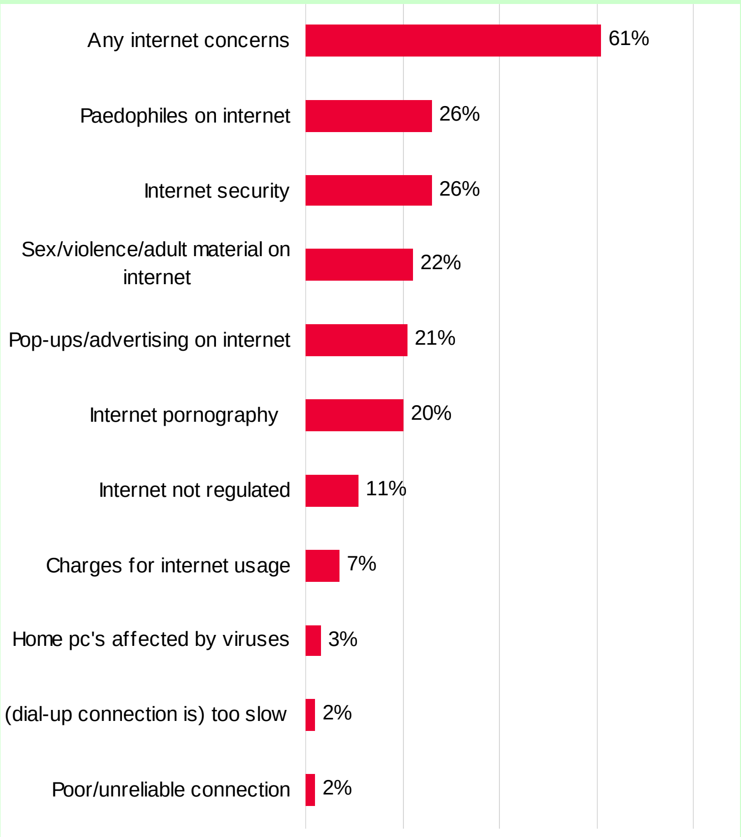
- Strong-enforceable legislation.
- Continued development of technical measures.
- Establishment of meaningful industry partnerships, especially among ISPs, mobile carriers and direct marketing associations.
- Consumer and industry education about anti-spam measures and Internet security practices;
- International co-operation among government, industry, consumer, business and anti-spam groups for a global and co-ordinated approach to the problem.

Independent research undertaken for the UK regulator has identified a number of internet security issues that cause concern for consumers. These include:

- access to personal data
- scams and fraud
- Internet spam
- children and the internet
- inappropriate/harmful content
- unauthorised access to personal data, which may or may not be malicious

The results of the survey are illustrated in Figure 10 below. Security and content are common themes.

Figure 10: Spontaneous concerns about Internet services



Source: Ad hoc survey conducted by BMRB on behalf of Ofcom, during August 2006 Base 612 UK adults using Internet at home

Despite an increasing number of national and international laws and agreements, internet-related issues remain a serious and growing concern. For example, the Information Commissioner's Office, the regulator charged with oversight of data protection regulation in the UK, received over 19,000 data protection complaints from the general public in 2004[24]. Phishing incidents are becoming increasingly common. Globally, the Anti Phishing Working Group reported 16,882 unique attacks in November 2005, up from 8,975 unique attacks launched in November 2004[25]. BT reported in December 2005 that its "cleanfeed" technology blocks an average of 45,000 attempted hits onto illegal child pornography sites each day[26].

The attempts to translate traditional direct regulatory structures onto the internet have for the main part been ineffective at achieving their desired goals. Where action has been effective, both nationally and internationally, it has often involved co- or self-regulatory measures developed with participation from the industry.

The Internet Watch Foundation (IWF) in the UK is one such example of self-regulation. The IWF operates a hotline for reporting illegal content on the internet. Once content is ascertained by the IWF to be illegal, it issues take-down notices to hosting service providers, when these are based in the UK. Additionally, it supplies ISPs with details of websites containing internationally hosted illegal content, and of online user groups dedicated to disseminating illegal and offensive material. Most UK ISPs have already voluntarily agreed to block those sites and user groups. The IWF has been a successful self-regulatory strategy – in 2005, only 0.4% of potentially illegal child abuse images reported to the IWF were hosted in the UK[27]. However, the international problem remains.

At international level, industry-led measures have played a significant part in increasing consumer confidence in e-commerce and hence making the internet a more secure place for commercial transactions. For example, data encryption through the https protocol[28] has been widely adopted by online banking and commercial sites, although there remains a need for on-going investments to ensure adequate levels of security. Furthermore, significant efforts have been invested by the industry in marketing its benefits to consumers – today, for example, the padlock symbol is displayed on many browser windows. Though further efforts are needed to ensure that the padlock symbol guarantees adequate levels of consumer protection, its use by e-traders can serve to give consumers the peace of mind necessary to decide to engage in e-commerce.

Within the context of NGN, the problems to be addressed are likely to be similar to those that already exist for Internet service, for example:

- Misuse of NGN that causes harm to consumers, for example ‘SPAM over Internet telephony’ (SPIT).
- Potential for fraud and identity theft.
- Privacy concerns and potential for misuse of personal information (eg through the greater personalisation capability provided by NGN.

To protect the integrity of the network, operators need to take account of potential security threats at every level of their network infrastructure as well as at the customer level e.g., laptops, personal digital assistants and mobile phones. High quality and network security management is therefore likely to become an increasingly important aspect of brand reputation and the associated customer satisfaction.

Box 6: Effects of spam in developing countries

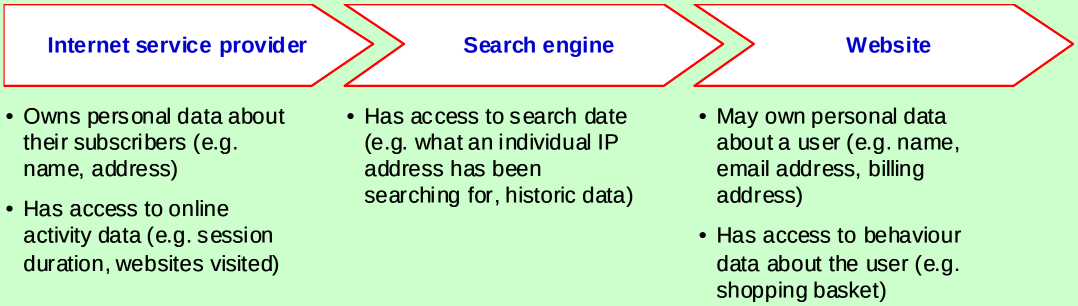
Spam is arguably a bigger problem in developing countries, many of whom do not yet have anti-spam laws. For those that do, many do not have the resources to enforce them, although the law may still be useful in providing the basis for regional and multinational enforcement. The impact of spam may also be more costly where ISPs are frequently deluged by spikes in spam that lead to network slowdowns and breakdowns. Moreover many people send e-mails from shared Internet connections and equipment, such as cybercafés or other public access centres. These services normally rely on hosted e-mail services with limits on in-box sizes. Accessing e-mail become too expensive if per-minute charges to cybercafé owners are consumed by cleaning spam from their inboxes.

Source: John G Palfrey, *Trends in Telecommunication Reform, 2006*, chapter 7

4.1 Protection of personal data and monitoring of users’ online activities

There are many ways in which an internet user provides personal data, as illustrated in one example below.

Figure 11: Data collection and retention across an example internet lifecycle



- Owns personal data about their subscribers (e.g. name, address)
- Has access to online activity data (e.g. session duration, websites visited)

- Has access to search date (e.g. what an individual IP address has been searching for, historic data)

- May own personal data about a user (e.g. name, email address, billing address)
- Has access to behaviour data about the user (e.g. shopping basket)

There has been increasing concern about how aware consumers actually are about the disclosure of their data online, especially when data is collected unknowingly. For example, a common method by which personal data can be collected from an individual without their knowledge is through the use of 'spy ware' - software installed on an individual's computer which covertly transmits information about the user's activities to a remote host.

There is no conclusive definition of the term spyware, although for the purposes of this report we define spyware as comprising of two types: 'malware' and 'adware'. Malware includes viruses, worms and trojans and its defining characteristic is that it is intended to cause harm to the computer or be otherwise used for criminal purposes.

Adware is distinct from malware in that it does not have a malicious intent, but rather is designed to enhance the effectiveness of advertising targeted at the user or otherwise provide marketing information to a third party. Examples of this are applications that facilitate pop-up browser windows, redirect browser home pages and add favourite sites to browser lists. In addition, data tags referred to as cookies can be used by websites to identify users. On their first visit to a specific website, users may have a cookie downloaded onto their computer, which allows the website to recognise that user and their preferences when they return.
However, in the majority of cases users are not aware a) what spyware is and b) that it has been installed on their computer, creating potential privacy issues as personal data about them is being collected and distributed without their knowledge. The user's ability to manage these issues happens at the local level ie dependent on their choice of browser technology and/or the configuration of their browser. This example demonstrates the importance of promoting media literacy.

Users who rely on cybercafés for internet access should in principle be able to rely on security procedures being in place to deal with key loggers, filters and data theft. However this may be open to compromise and NRAs need to take a pragmatic approach eg by providing information and guidance.

When considering the protection of personal information, the starting point for most analyses lies with rights to privacy. The right to privacy is a basic human right enshrined in the 1948 United Nation's Universal Declaration of Human Rights and the 1981 European Convention on Human Rights (Article 8). Since the 1970s, many developed countries have responded to concerns about privacy risks arising from the collection and use of personal data by relying on "fair information principles" to govern the appropriate use of personal data. For example, such principles were laid out in the 1981 European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, following the development of the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980.

According to these principles, personal data can be collected lawfully for specific and limited purposes only, and can be stored only for as long as necessary to fulfil the purpose. Data must be accurate and adequate for the intended purposes, and individuals have a right of access to and correction of their personal data. The Convention also established special protection for data of sensitive nature, such as, for example, data on the individual's religious and political beliefs or medical records. Many of these principles have been formally adopted through data protection legislation.

4.2 International framework

The growth of the internet has exacerbated many issues concerning the protection of personal data, particularly across national borders. In response, the EU and APEC (Asia Pacific Economic Cooperation) have developed agreements to harmonize their Members' approach to legislation regarding internet data protection. Of the international organisations developing data protection laws relating to the internet, the EU has been the most active, developing both legislative instruments and guidance that aim to protect data and underpin the free flow of goods and services within the EU.

There are three EU directives that relate to the protection of personal data. The first is the Directive of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. The 1995 Directive lays out six conditions of legitimate date processing one which is unambiguous consent before data may be collected, with limited exceptional cases, for example, if it is in the vital interests of the subject, to ensure legal compliance, or in the interests of national security. The 1995 Directive prohibits the collection of specific types of data (e.g. race, ethnicity, religious beliefs, political opinions, health), unless under exceptional circumstances, and requires those collecting, processing and retaining data to institute technical and organisational security measures to protect the data.

The second is the Directive 97/66/EC of 15/12/1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The 1997 Directive aims to harmonize and provide an equivalent level of privacy and data protection as provided by the 1995 Directive but specifically within the telecommunications environment. It includes responsibilities on telecoms providers to maintain security of the network and traffic/billing data, and the right of individuals not to appear in publicised directories.

The third is the Directive of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. The 2002 Directive updates and replaces the 1997 Directive (97/66/EC) and deals specifically with internet related issues. It includes the legal protection of new internet data, such as traffic data (e.g. routing information, session duration) and focuses on the confidentiality of electronic communications, data retention of users' online activities, spamming and inclusion of personal data in public directories.

Other international agreements include the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28/01/1981 . The 1981 Convention aims to strengthen the legal protection of individuals with regard to automatic processing of personal information relating to them. It includes basic provisions requiring the lawful collection of data, secure and confidential retention of data, maintenance of accurate data and the right to access data by the subject, effectively harmonising signing Member States' legislation. It also includes provisions on the cross-border flow of data and international collaboration in the implementation of the treaty. The convention has been ratified by 35 Council of Europe Member States.

The OECD has published guidelines, signed by 30 OECD Member States, setting out data protection and privacy principles to be observed by signing States. These include limits on how personal data is collected and used and requirements on signatories to secure information flows across borders and cooperate in areas related to data protection. The OECD continues to be active in this field, especially through the work of its Working Party on Information Security and Privacy.

Finally, the Asian-Pacific Economic Cooperation (APEC) Privacy Framework promotes a consistent approach to information privacy protection across APEC member economies, including the development of appropriate privacy protections for personal information, and the prevention of unnecessary barriers to information flows.

4.3 Inappropriate content and consumer protection

The definition of what constitutes inappropriate content varies by country and even region. Whilst in one country certain types of content are deemed perfectly legal and acceptable for consumption, in others, production or consumption of the same content may be frowned upon or even be a criminal offence. These variations in attitudes occur for many reasons, including local political, cultural and religious differences, and result in different stances on how best to tackle the distribution of what is considered inappropriate content within each individual territory.

There are, however, certain types of content for which there exists a widespread consensus amongst different countries of what is deemed to be "decent" or "legal". The best example of such content where there is a general consensus is child pornography. In such cases, a cross-border approach to tackling the distribution of such content is possible. For other types of content, national differences in attitudes make it difficult to achieve cross-border cooperation, forcing national markets to adopt solutions tailored to their specific circumstances and prevailing cultural norms.

The extent and nature of international and national legislation and regulation differ across content types, with certain types of content being targeted more actively than others. Broadly speaking, inappropriate content can cover the following types of content:

- Child pornography.
- Content and communications which facilitate acts of terrorism.
- Racist or xenophobic material or material which incites racism or xenophobia.
- Other content (includes adult pornography, violent material, defamatory content and other content which may be deemed to be illegal or inappropriate under a nation's laws).

4.3.1 *Inappropriate content*

Child pornography is the clearest example of content that is considered not only inappropriate but also illegal in most countries. At an international level, both the Council of Europe and the United Nations have taken action against dissemination of child pornography, and have encouraged collaboration between nations in combating the problem.

The 2000 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, mandates signing parties to prohibit the sale of children, child prostitution and child pornography within their nation's law, including via the internet. It also provides a framework for increased international cooperation in prosecuting perpetrators in these areas. The Protocol has entered into force following 12 ratifications by signing nations.

The 2001 European Convention of Cybercrime mandates signing parties to prohibit the production, distribution and buying of child pornography over the internet. It was the first international treaty to criminalise offending behaviour directed against computer systems, networks or data in addition to content related crimes such as child pornography. The Convention creates a legislative framework for investigating and prosecuting violations of law with respect to child pornography, and mandates cooperation between national agencies in combating child pornography. It entered into force in July 2004 following 5 ratifications. To date, it has been signed by 38 countries and ratified by 12 countries, though not including the UK.

The substantive criminal law measures of the European Convention of Cybercrime include offences on:

- Intentional illegal access of computer systems
- Intentional illegal interception of non-public transmissions of computer data
- Intentional interference with computer data including deletion or alteration
- Intentional interference with a computer system.

Additionally, the Convention includes crimes such as computer related forgery and fraud, and content related offences such as child pornography. Offences related to infringements of copyright and related rights are also included within the Convention.

Attempts to encourage international collaboration for other types of inappropriate content have proved problematic due to national differences in the definition of what is inappropriate. For example, the committee drafting the Cybercrime Convention discussed the possibility of including content related offences other than child pornography (Article 9) within the Convention, for example, the online distribution of racist propaganda. However, the committee could not reach consensus on the inclusion of additional offences within the Convention. Instead, it was recommended that additional protocol to the Convention be developed under the title "Broadening the scope of the convention to include new forms of offence".

The Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems aims to harmonize substantive criminal law in the fight against racism and xenophobia on the internet and, to improve international co-operation in this area. Following five ratifications, it came into force on 1 March 2006. Importantly, however, the UK and the US are currently not signatories to the Additional Protocol.

Though the US had signed the original convention which focused on child pornography, it has not signed the Additional Protocol on the grounds that the Protocol restricts an individual's right to free speech. The First Amendment of the US Constitution guarantees an individual's right to free speech and is broader in scope than the equivalent Article 10 of the European Convention of Human Rights. The First Amendment states that 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances'.

Such differences in national opinion compromise the effectiveness of the treaty. Websites containing offensive content, in this instance racist or xenophobic content, can relocate their hosting to a country which is not a signatory to the treaty thereby avoiding legal sanctions.

4.4 Online advertising

For inappropriate advertising practices on the internet, there is a European coordination manifested through the EU's Television without Frontiers Directive (TWF) and the European Advertising Standards Alliance (EASA).

The EU's Television without Frontiers Directive was first written into EU law in 1989. Since then it has been subject to a number of amendments with a substantive review of the legislation currently underway. The Directive seeks to harmonize Member States' legislation across all aspects of the production and distribution of audiovisual media, including advertising.

When the legislation was first established, it was primarily aimed at linear audiovisual content, that is, transmission of broadcast television via a terrestrial, satellite or cable network. The current review of the Directive seeks to address the increasing role of the internet as a platform for the delivery of audiovisual services. The new Directive has not yet been finalised.

Under the proposed new Directive, the regulations would not apply to:

- Internet services whose primary objective is not the provision of audiovisual services (e.g. contains an audiovisual content clip which is ancillary to the main purpose of the site);
- Electronic versions of newspapers or magazines;
- Private correspondence (e.g. e-mail).

The European Advertising Standards Alliance does not have a Code of Conduct which members agree to comply to. Instead, it works as a forum and lobby group for self-regulatory entities from across Europe and other member countries, and industry players such as advertising federations. Since 1992 it has also had a role in handling and resolving cross-border complaints concerning advertising content and standards between members. Its remit extends into the internet space.

It is important, however, to bear in mind that ways to misuse personal information are constantly evolving. One of the key challenges for government, regulators, enforcers and industry lies in responding swiftly and effectively to new forms of abuse.

5 Conclusions

Next generation networks offer the possibility of delivering real benefits to citizens and consumers in terms of innovative new services and greater choice. However the convergence of different services onto a single network raises important issues around quality of service, consumer awareness and consumer protection.

For example whereas new voice services may seem at first sight to consumers to be identical to traditional voice services, they may not be able to deliver certain features, such as access to emergency services, that consumers have in the past taken for granted. With the growing trend towards bundled products, with new content and applications, consumers may or may not be prepared to accept differential service standards. They are likely to become more aware of the importance of quality of service when choosing a supplier and demand more information which allows them to differentiate between the products and services on offer.

Network neutrality implies there should be minimal differentiation in the traffic management and prioritisation of delivery of services to the consumer. However, provided consumers are well informed and there are no barriers to switching, discrimination between product offerings need not be detrimental and may even increase consumer benefits.

The internet's flexibility makes it an engine for innovation. With the advent of NGN it is likely to play a much greater role in citizens' lives. In relation to cyber security, high quality and network security management will be essential to protect brand reputation and protect consumers from harm.

[1] See Milne, Claire, *Telecom Reform: Principles, Policies and Regulatory Practices*, (Chapter 14 -Regulating Quality of Service, http://lirne.net/2003/resources/tr/chapter14.pdf

[2] Directive 2002/22/EC of the European Parliament and of the Council, 7 March 2002, on universal service and users' rights relating to electronic communications and services (Universal Service Directive) Annex III, pL108/72.

[3] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to the electronic communications networks and services (Universal Services Directive)

[4] http://www.ofcom.org.uk/consult/condocs/qualitystate/statement/

[5] As discussed by Intven, Hans and Miedema , Theresa in *Trends in Telecommunication Reform 2002, chapter 5, Specific Regulatory Function*

[7] For a full discussion of monitoring of QoS standards in India see Milne, Robert, ICT *Quality of Service Regulation: Practices and Proposals. Background Paper*, ITU Global Seminar on Quality of Service and Consumer Protection, Geneva, September 2006

[8] ITU, Telecommunications Indicators Handbook, on line : http://www.itu.int/ITU-D/ict/publications/world/material/handbook.html

[9] See discussion in *Ofcom's Consumer Policy: A consultation*, 8 February 2006 http://www.ofcom.org.uk/consult/condocs/ocp/

[10] See for example, ITU Trends in Telecommunications Reform, 2002; the ITU-T 2004 Handbook on QoS and Network Performance. http://web/pub/T-HDB-QOS.02-2004/en and Milne, Robert, Antelope Consulting, United Kingdom (rem@antelope.org.uk), *ICT Quality of Service Regulation: Practices and Proposals, Background Paper*, ITU, Global Seminar on Quality of Service and Consumer Protection, Geneva, Switzerland, 31 August – 1 September 2006; and Oodan, A.P., Ward, K.E. and Mullee, A. W., *Quality of service in telecommunications.* IEE Telecoms Series No. 39, London, 1997. (especially chapters 14, 15 and 16) http://www.iee.org/Publish/Books/TeleComm/Te039c.cfm#8Customers

[11] The ITU-T Recommendation G.114 (5) establishes a number of time constraints on one-way latency. The upper bound is 150 ms for one way traffic. VoIP calls must achieve the 150 ms bond to successfully emulate the QoS experienced in traditional voice services. This time constraint leaves very little margin for error in packet delivery.

[12] Diffserv and Intserv are methods for controlling priority of Internet protocol packets by encoding priority into some digits reserved for this purpose in each packet. Some routers are able to recognise this information and route the packets with priority over other packets when network nodes are congested. EXP is a similar concept used in networks employing MPLS to provide QoS differentiation between different services).

[13] Window size is a parameter specific to flow control in Transport Control Protocol (TCP), commonly used to transport non real time data reliably over the Internet

[14] http://www.ofcom.org.uk/consult/condocs/new_voice/anew_voice/nvs.pdf

[15] http://ftp.fcc.gov.uk/cgb/voip911order.pdf

[16] Universal Service Directive, Article 26

[17] http://erg.eu.int/doc/publications/erg0512_voip_common_statement.pdf

[18] http://erg.eu.int/doc/publications/erg_06_39_report_voip_cons_aspects.pdf

[19] Ofcom consultation, *Regulation of VoIP Services*, 22 February 2006

[20] ENUM is a standard for converting an ordinary telephone number into a domain name, which can then be converted

into an IP address for use by an NGN or VoIP system to route a telephone call.

[21] see Ofcom, *Review of General Condition 198 – Number Portability*, 16 November 2006

[22] In digital networks (NGN or otherwise) speech is encoded into a digital representation. The most commonly used standard for doing this is known as G.711, which encodes telephone speech at 64,000 digits per second (or bits per second). Wide-band speech is encoded at a higher rate, say 96,000 bits per second for example, to provide better speech quality.

[23] See Chieng, Marshall,Ho and Parr, Agent-Enhanced Dynamic Service Level Agreement in future network environments,

[24] Information Commissioner's Office

[25] Anti-Phishing Working Group Phishing Activity Trends Report, November 2005

[26] [26]BT. See http://www.btplc.com/societyandenvironment/news/showarticle.cfm?articleid=2ab29f02-bd0c-4e0a-952f-60fef2500246

[27] Internet Watch Foundation

[28] HyperText Transfer Protocol (https) is a secure version of HTTP which uses certificates and encryption when sending data to prevent unauthorised interception and receipt of data. It is used for credit card payments and entry of sensitive personal or financial data.

Bibliography

OECD Working Party on Telecommunication and Information Service Policies, *Next Generation Network Development in OECD Countries*, DSTI/CCP/TISP(2004)/FINAL, 18 Jan 2005

Ofcom, *Next Generation Networks: Developing the Regulatory Framework*, 7 March 2006, http://www.ofcom.org.uk/consult/condocs/nxgnfc/statement/

Ofcom, *The Consumer Experience, Research Report*, 16 November 2006, http://www.ofcom.org.uk/research/tce/report/

Ofcom, *Strategic Review of Telecommunications. Phase 2* Consumer Research Annex (M), 18 November 2004

Ofcom, *Ofcom Response to the European Commission Consultation on Content Online in the Single Market*, Consultation, 20 October 2006

Ofcom, *Communications Market: Special Report, Consumer Decision Making in the Telecoms Market*

Ofcom, *New Voice Services, An interim consultation and guidance*, 6 September 2004, http://www.ofcom.org.uk/consult/condocs/new_voice/anew_voice/nvs.pdf

Ofcom, *Next Generation Networks, Further Consultation*, 30 June 2005 http://www.ofcom.org.uk/consult/condocs/nxgnfc/ngnfc1.pdf

Ofcom, Review of General Condition 18, Number Portability, 16 November 2006, http://www.ofcom.org.uk/consult/condocs/gc18/

Ofcom, *Broadband Migrations: Enabling Consumer Choice*, 17 August 2006 http://www.ofcom.org.uk/consult/condocs/migration/

Ofcom, *Regulation of VoIP services*, 22 February 2006 http://www.ofcom.org.uk/consult/condocs/voipregulation/