



The Mobile Broadband Group

London SE15 5YA

www.mobilebroadbandgroup.com

Can we keep our hands off the net? The All Party Parliamentary Group on Communications' investigation into the role for Government over Internet traffic

Response from the Mobile Broadband Group

1. The Mobile Broadband Group ("MBG", whose members are the UK mobile businesses of O2, Orange, T-Mobile, Virgin Mobile, Vodafone and 3), welcomes the opportunity to contribute to the All Party Group on Communications' inquiry into the role of Government over Internet traffic.
2. In a continuously changing environment, it is appropriate to review regularly principles, policies and practices to ensure that they are affording the best possible environment in which to promote innovation and investment in new services and protect consumers and businesses appropriately.
3. Customers in the UK have access to some of the most sophisticated, innovative and competitively priced mobile services in the world delivered by five mobile networks. In addition, mobile virtual network operators (MVNOs, such as Virgin Mobile), utilising the infrastructure of the mobile networks, provide further customer choice, innovation and specialised services.
4. MBG members are strong proponents of self-regulation. For the Committee's information, we have set out in an annex a summary of the Code of Practice for the self regulation of content on mobile published in 2004. In addition, MBG members are all subscribers to the Internet Watch Foundation, all are members of the UK

Council for Child Internet Safety and, through the MBG, all are represented on the Committee for Advertising Practice.

5. Issues presented by the Internet are diverse and complex. Mobile operators have been demonstrably successful in implementing protective strategies that are proportionate, principled and effective. Our responses to the Committee are informed by these experiences. The MBG would only support measures that would be similarly proportionate, principled and capable of being effective.

Can we distinguish circumstances when ISPs should be forced to act to deal with some type of bad traffic? When should we insist that ISPs should not be forced into dealing with a problem, and that the solution must be found elsewhere?

6. It is common ground that the Internet has had an overwhelmingly positive effect on peoples' personal and work lives.
7. The success of the Internet has been built on a few fundamental principles. One of these principles is that users should be able to communicate without being 'listened into', as is the case with users of telephones and postal services (subject to lawful intercept regulations). Just because it may be technically possible for an ISP to observe the type of content passing across its network, that does not always make it right to do so. The mere conduit status of the Internet Service Provider has been and remains one of the fundamental building blocks of the Internet's success.
8. While ISPs do scan, for example, incoming mail for potential viruses and spam and, if appropriate, place material in quarantine for the customer's inspection, there is a world of difference between an ISP doing something for its customer's benefit (and with their consent) and an ISP monitoring traffic as a matter of course at the behest of the state for the benefit of the state and other third parties. There is no economic model to justify the expense of routine monitoring nor is there a moral justification for such intrusion. By way of comparison, no one objects to the mail service being scanned for letter bombs but it would not be acceptable for the mail service to routinely open and inspect the contents of mail.
9. The MBG does not believe, bearing in mind the wide choice in the market for ISPs and filtering solutions, it would be appropriate or proportionate to require ISPs to filter spam and viruses. This may entail a far more intensive examination of the content of private communications than is currently the case, and it is not at all clear whether ISPs would wish to be held liable for the consequences of their failure to detect spam

and viruses. It should be up to the customer to choose the provision that suits their needs best. There are several sources of information that can guide the consumer in how to protect themselves properly (e.g Get Safe Online).

10. There appears to be broad consensus from Government, ISPs and consumers that protecting customers from inadvertent exposure to child sexual abuse images, which are both illegal to distribute from the country of origin and illegal to view in the country of consumption, is a good thing too. It is understood that about 95% of UK Internet consumers are now protected in this way. This is a great success for self-regulation. It would not be proportionate or sensible to introduce complex and potentially intrusive legislation to cover the balance. If successful self-regulation is always seen to be replaced by formal regulation, it is a significant disincentive to industry to expend the considerable time, effort and expense that self-regulation entails.
11. While blocking has been successful for child sexual abuse images, it should be emphasised that the technique is primarily intended to protect the innocent from inadvertent exposure rather than block someone deliberately seeking the content. The MBG does not believe that using the blocking technique would be suitable for other types of content. There have been discussions with the Home Office, for example, about the use of blocking for radicalisation sites. It was concluded that such an approach would be just too contentious and actually counter-productive, when there is no consensus among the wider population as to the legitimacy of blocking.
12. By way of illustration, the IWF has had recent experience of the public objecting to the blocking of an image (albeit Level 1 illegal) that had been in the public domain for 30 years. The IWF's action led to the image being posted many many times, perhaps thousands of times, more. Whatever the rights and wrongs of that particular incident, it was a very clear demonstration of how power has shifted from government and corporations to the individual. It is very easy for actions taken for the best of motives to be completely counterproductive. The MBG does not support the extension of the use of blocking to content other than child sexual abuse images.
13. Furthermore, while ISPs can protect their customers from viruses and SPAM, there must be no requirement for the ISP to monitor the behaviour of its customer to protect the interests of third parties. ISPs should not be trying to detect whether their customer intends to commit a crime, commit adultery, drive dangerously or any other infringement or illegal activity.

14. We recognise that some rights owners, such as the record industry establishment (as opposed to the artists, who are learning to cut out the record companies through direct access to customers), are seeking that their commercial interests be more actively protected by ISPs but this is completely inadequate justification for ISPs to be interfering in their customers' privacy and personal communications.
15. The solution to the 'rights' problem lies in more innovative business models, not a 'graduated response' that ultimately relies on suing large numbers of teenagers. Transferring the costs of policing rights to ISPs does little to incentivise the records companies and others to address the business model issues at the heart of the problem.
16. Furthermore the technical measures being considered by Government for dealing with serious infringers of copyright rely on operators having sufficient public IP addresses for each customer device. This is not necessarily the case for mobile networks.

Should the Government be intervening over behavioural advertising services, either to encourage or discourage their deployment; or is this entirely a matter for individual users, ISPs and websites?

17. As with many new services, there is an initial flurry of interest and even disquiet until the nature and implications of the service have been understood by the stakeholders. Behavioural targeting is perhaps in such a phase and we feel that it would be premature for the Government to be either encouraging or discouraging the use of behavioural targeting techniques. Its role is to ensure that there is clarity over the application of the law in this area.
18. The Internet Advertising Bureau has done the right thing in bringing together the major players in the field to prepare guidelines, which we understand have been well received by consumer bodies and regulators.
19. Providing this initiative is successful and, bearing in mind the sponsors, the MBG expects it to be, the MBG believes that this is the only action that is needed at present.

Is there a need for new initiatives to deal with online privacy, and if so, what should be done?

20. The MBG understands that research carried out for Digital Britain has revealed that citizens' major concerns around the Internet mostly relate to viruses (including spyware) and identity theft, as opposed to perhaps more emotive aspects such as pornography and inappropriate content generally.
21. As these concerns appear to be one of the significant barriers to people going on-line, the MBG would certainly agree that overcoming these fears is a high priority and may merit more concentrated and focused policy development. Whether this would need a 'new initiative' is harder to judge. It may be better to re-weight the balance of existing activities and put more behind projects such as 'Get Safe Online' and the Media Literacy strategy generally.
22. A consistent theme behind Ofcom's work in recent years is that, as power over the media shifts towards individual producer/consumers, people will have to take greater responsibility for their own actions and behaviour on-line. This is not a convenient way of releasing Government from its regulatory responsibilities but rather the *quid pro quo* for individuals gaining power and influence at the expense of media companies and the state.
23. This transfer of power is happening quickly and people need to be properly prepared, through increased emphasis on educational programmes and initiatives.
24. For information, the MBG draws the Committee's attention to the Home Office's current consultation on the extent to which law enforcement investigators can impose requirements on CSPs and ISPs to limit privacy.¹

Is the current global approach to dealing with child sexual abuse images working effectively? If not, then how should it be improved?

25. The MBG fully supports the IWF and the work it does. We do, however, believe that it is time to consider how illegal child abuse images could be removed from the web more quickly. The IWF estimates that there are around 3,000 sites hosting illegal content (on a multiplicity of individual URLs) and yet many of them remain live for considerable periods of time.

¹ "Protecting the public in a changing communications environment", a consultation document published by the Home Office in March 2009.

26. In reducing illegal content from 18% hosted in the UK to less than 1%, the IWF has shown that direct action in partnership with the web hosting companies can be effective. The MBG understands that country hotlines are constrained by international protocols from informing overseas companies directly that they are hosting illegal content on their servers and that this information has to be conveyed via the local LEA.
27. Taking account of how ineffective this approach has been in some countries, we believe the Government should explore with other countries a different international settlement on 'notice and take down' for child sexual abuse images, whereby hosters can be notified directly by country hotlines across international borders in circumstances where the local LEA has failed to take action promptly.

Who should be paying for the transmission of Internet traffic? Would it be appropriate to enshrine any of the various notions of Network Neutrality in statute?

28. The interim Digital Britain report recorded that *"Ofcom has stated that provided consumers are properly informed, such new business models could be an important part of the investment case for Next Generation Access, provided consumers are properly informed [sic]. On the same basis, the Government has yet to see a case for legislation in favour of net neutrality."*
29. The MBG agrees with both the Government's and Ofcom's conclusion on this point. If Government were to intervene in this area it would preclude all manner of potential investment models. A command and control approach would carry significant regulatory risk and should be avoided.
30. Demand for Internet bandwidth from consumers and producers is expanding exponentially and it is self-evidently necessary to align the interests of consumers, content providers and network providers to ensure that the incentives are in place to enable more bandwidth to be brought on stream in line with demand.
31. This is more complex than in the past because, for example, consumers have a strong preference for flat tariffs and budgetary certainty when it comes to paying for Internet access and content. Although far less prevalent now, with traditional voice networks, customers rationed their usage because they could understand a charge of so many pence per minute and differentiated pricing at peak traffic times. Understandably, it is much harder to grasp what so many pence per kilobyte means in real life and to judge what sort of utility can be derived from such a pricing structure. That is why flat data rate tariffs are so popular.

32. As a consequence, the ISP's ability to ration usage through price is very much diminished. It is thus very important that providers have other traffic management tools at their disposal to help allocate resources fairly and economically and to enable them to invest in new network resources as demand increases.

33. In conclusion, the MBG believes that the Government are broadly taking the right approach to the regulation of matters around the Internet and strongly believe that the 'mere conduit' status of the ISP should remain as fundamental building block of success and to protect consumers' privacy. Following the Digital Britain strategy, we would expect the Government to place considerably more emphasis on media literacy.

34. Even though Ofcom's media literacy audits reveal that consumers' ability to create, use and understand content on line is relatively high, it is still important that there is continuous improvement in this area so that the Internet can be safely navigated without the need for further regulation that is potentially complex, expensive and intrusive on people's personal lives.

ANNEX

Supplementary information about the mobile operators' code of practice for the self regulation of new forms of content on mobile.²

1. There are roughly 1.2 mobile subscriptions per head of population in the UK, with about 85% of the population owning a mobile device. A very fast going segment of this market is mobile broadband, whereby a laptop or home PC is connected to a mobile network via a subscriber using a 3G modem. Beyond mobile, customers with devices that have both 3G and Wi-Fi connectivity can access Internet based services such as Web browsing and voice over IP, through a network of public and private Wi-fi hotspots.

² <http://www.mobilebroadbandgroup.com/social.htm>

2. The consequence of the customer's wide choice of connectivity is that the mobile operator is no longer needs to be the sole provider of the customer experience while on the move. Nevertheless, where the mobile operator is providing connectivity, MBG members have, since, 2005, operated a self-regulatory Code of Practice that governs the way in which Internet connectivity on a mobile handset and commercial content services are provided.
3. With commercial content (i.e. where the content is provided by the mobile operator or a commercial partner), content that is classified as 18 (as determined against a framework provided by the Independent Mobile Classification Body) is not made available until a customer has demonstrated, through robust age verification, that he or she is at least 18 years old.
4. For Internet access on a mobile handset (i.e. where the mobile operator is just providing connectivity to the Internet), customers can invoke a filter that is designed to block content that is unsuitable for customers under the age of 18. Many operators apply the filter by default for the 3G device connection. For mobile broadband connectivity, the customer is able to install software or apply their own settings via their chosen Internet browser on the laptop or PC.
5. Filters are an extremely effective way of providing a service that is appropriate for children without the need to engage in heavy handed intrusions over the content that adults may wish to view.
6. All the UK mobile operators are in receipt of the Internet Watch Foundation's list of child sexual abuse images that are illegal to distribute and possess in the UK and thus mobile customers are protected from inadvertently committing an offence by viewing such images on their mobile device. It should be noted that the primary purpose of using the blocking list is to protect customers not prevent a determined user from viewing content they shouldn't.