All Party Parliamentary Communications Group

"Can we keep our hands off the net?"

Report of an Inquiry by the All Party Parliamentary Communications Group

October 2009

apComms

Can we keep our hands off the net?

Report of an Inquiry by the All Party Parliamentary Communications Group

October 2009

Introduction

1. The All Party Parliamentary Communications Group (apComms) is an independent group of MPs and Lords, from all political parties, which seeks to encourage debate on a range of communications issues. It brings together relevant stakeholders including Government, Parliamentarians, industry and consumer groups. The group is open to all Parliamentarians from both the House of Commons and the House of Lords.

2. apComms issued a Press Release (see Appendix A) on 22nd April 2009 to announce its intention to hold an inquiry into Internet traffic to assess regulation of ISPs and consider a range of Internet traffic issues from behavioural advertising and privacy to child abuse images and Internet neutrality – with a view to providing some answers as to what role Government should play when it comes to Internet traffic.

3. Respondents were particularly asked to concentrate on five specific issues:

   #1 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?

   #2 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?

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

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

   #5 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?

4. Written submissions to the inquiry were received from nearly 50 umbrella groups, companies and individuals:

   Alliance Against IP Theft
   British Recorded Music Industry (BPI)
   Broadband Stakeholder Group (BSG)
   Federation Against Software Theft (FAST)
   Internet Advertising Bureau (IAB)
   Incorporated Society of British Advertisers (ISBA)
   International Association of Internet Hotlines (INHOPE)
   Internet Service Providers Association UK (ISPA)
   Mobile Broadband Group (MBG)

Motion Picture Association (MPA)
Periodical Publishers Association (PPA)
Respect for Film (RFF)

AT&T
BBBritain
BT
Child Exploitation & Online Protection Centre (CEOP)
Communication & Media Research Institute, University of Westminster
Consumer Focus
Denton Wilde Sapte LLP
Dephormation.org.uk
Foundation for Information Policy Research (FIPR)
Global Digital Broadcast
Hutchinson 3G UK (3)
Internet Watch Foundation (IWF)
JANET(UK)
Ofcom
Open Rights Group (ORG)
Orange
Phorm
Privacy International (PI)
Skype
T-Mobile
TalkTalk Group
THUS
University of Plymouth & South West Grid for Learning
Virgin Media

Phil Brooke
Leon Clarke
Gill Davison
Jamie Dowling
Miles Golding
Robert M Jones
Neil Maybin
Barbara Moore
Peter White

5. On the 6th and 7th July 2009, the committee heard oral evidence from:

Emma Ascroft, Yahoo! UK & Ireland
James Blessing, Internet Service Providers Association UK
Radha Burgess, Phorm
Chris Dawes, Department of Culture Media & Sport

Adrian Dwyer, International Association of Internet Hotlines
Mike Galvin, BT
Jim Gamble, Child Exploitation & Online Protection Centre
Alexander Hanff, Privacy International
Andrew Heaney, TalkTalk Group
David Hendon, Department for Business Innovation & Skills
Peter John, Dephormation.org.uk
Hamish MacLeod, Mobile Broadband Group
Neil Maybin
Harry Metcalfe, Open Rights Group
Justin Miller, Home Office
Richard Mollett, British Recorded Music Industry
Barbara Moore, Moredial
Xavier Mooyaart, T-Mobile
Jeremy Olivier, Ofcom
Andy Phippen, University of Plymouth
Peter Robbins, Internet Watch Foundation
Sarah Simon, Phorm
Nick Stringer, Internet Advertising Bureau
Ian Walden, Internet Watch Foundation
Linda Weatherhead, Consumer Focus

6. Transcripts of the three oral evidence sessions have been made available on our website:

   http://www.apcomms.org.uk/uploads/090706_apComms_Oral_Evidence1.doc

   http://www.apcomms.org.uk/uploads/090707_apComms_Oral_Evidence2.doc

   http://www.apcomms.org.uk/uploads/090707_apComms_Oral_Evidence3.doc

7. We are grateful for all the written and oral evidence that we received and also for the expert advice and assistance afforded by our specialist adviser, Dr Richard Clayton of the Computer Laboratory, University of Cambridge.

8. The costs associated with this inquiry were paid solely by the All-Party Parliamentary Communications Group from existing funds. This includes the costs of printing the report, providing a transcript of the oral evidence sessions, and granting an honorarium to our specialist adviser. In addition, we are grateful for the support of Political Intelligence Ltd who provide secretariat services to apComms on a non-payment basis.

Structure of this report

9. This report poses each of the questions that we asked in turn, and uses the answers we were given, in written and oral evidence, to explain the different viewpoints around each of these topics. We then make recommendations, as we feel appropriate.

10. A glossary is provided in Appendix B for those unfamiliar with the technical terms and abbreviations that are used throughout the report.

11. Finally, in Appendix C, we provide a short bibliography of relevant documents that can be consulted for further and more detailed information about the issues we discuss.

Question 1: "Bad Traffic"

12. The first of our questions was:

> 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?

Botnets, spam and denial of service

13. When we formulated this question, we had in mind the type of issue that the Foundation for Information Policy Research (FIPR) was concerned about. They argued that:

> *In the case of bad incoming traffic, such as spam, the markets have shown that they can cope; most ISPs now offer spam filtering. The interesting market failure occurs with bad outgoing traffic. For example, when end-user PCs are compromised and used to send spam or distribute malware, medium-sized ISPs often take the trouble to identify them and clean them up, as an ISP that emits a lot of spam can find its peering relationships at risk. But large ISPs are under no such pressure, and thus ignore infected machines; dealing with customers costs money. This failure will not be fixed by technology, and will require regulatory action.*

14. FIPR suggested that there should be either a regime of statutory fines, or a private-action alternative in the form of a statutory scale of damages – similar to the scheme introduced by the EU to enable passengers whose flights are cancelled or overbooked to get compensation. FIPR drew our attention to "Security Economics and European Policy" a report they had written for the European Network and Information Security Agency (ENISA) which set out this approach at greater length.

15. Few other respondents addressed this issue at all. One was Barbara Moore who suggested a system of fines for those ISPs who do nothing to monitor and contain users whose machines are taken over and used in criminal "botnets".

16. In oral evidence she provided us with a number of examples of attacks by botnets, and suggested that ISPs could examine the traffic flowing through their systems to look for this type of bad traffic. If there are no fines, she told us, then there is no incentive for an ISP to examine the traffic.

17. THUS (who provide Internet services under the Demon brand name) told us that:

> *There may be an opportunity for ISPs to do more to prevent spam and infected machines. Such a scheme could lead to less impact from botnets and spam, but could be costly to implement depending on the approach taken. The "walled garden" approach of putting an "infected" user into quarantine and limiting general Internet access takes significant development and resource to manage, but could lead to better network management for the hosting ISP as well as benefits for other networks. However we believe that it should be left to the industry to regulate itself in this matter rather than having prescriptive legislation.*

18. Along these lines, the Australian Internet Industry Association has quite recently (11 September) announced a consultation on a voluntary code of practice for ISPs to follow in detecting and mitigating "e-Security" problems that are caused by their customers. The intention is to provide "a fair and uniform approach" to the problem "with the aim of reducing malware infected systems".

19. A contrary view was put forward by Andrew Cormack from JANET(UK), the operator of the major network used by UK universities, colleges and research organisations. He told us that the distinction between "good" and "bad" traffic was rarely clear – and that

technical measures to make the distinction were likely to suffer from a significant proportion of misclassifications.

> *Determining even which application is being used is difficult or impossible as modern applications rarely use fixed port numbers or other identifiers of the kind that could formerly be used to identify traffic as 'web' or 'e-mail', and an increasing volume of traffic is encrypted so that its content is completely opaque to the transit network.*

20. He did agree that competition does not appear to provide incentives for ISPs to protect other Internet users from their customers – in particular because of the risk of incorrectly blocking perfectly good traffic. However, he suggested, if ISPs were held liable then they might overly restrict the type of traffic that they allowed – which would be at odds with national objectives for an information society.

21. He also suggested that a "notice and take-down" approach, where ISPs would be liable only once they received reports of bad traffic, would not fare much better. ISPs would have a strong incentive to just disconnect their customers, and not perform any check upon the accuracy of the reports they were receiving.

Mere Conduit

22. Andrew Cormack also drew attention to another type of disincentive for ISPs to examine traffic:

> *It has been suggested that a hosting provider that attempts to detect infringing material of any kind immediately acquires liability for all infringing material that may be on their service, on the grounds that they have demonstrated some intent and ability to edit and select content and are therefore no longer merely a hosting provider but an editor. For providers that wish to remove inappropriate material from their own services, but are aware that checking can never guarantee to detect all problems, this potential liability can be a significant deterrent. We therefore consider that the law needs to be clarified to ensure that a hosting service that detects problems on its own service is in the same position as (or at least no worse than) a service that waits to receive notice of the problems from others. Such a change would encourage quicker removal of some types of inappropriate content.*

23. The Motion Picture Association also mentioned this issue, albeit in the context of detecting illegal file-sharing traffic:

> *Another claim made by ISPs is that there are legal impediments that stand in the way of anything but a policy of benign neglect. We have not seen convincing evidence of such impediments. However, to the extent that they can make a convincing case, such impediments should be addressed and tempered to the extent necessary for ISPs to take their responsibilities as much as other communications platform operators have had to abide by certain basic rules.*

24. This is closely related to the "mere conduit", "hosting" and "caching" immunities that ISPs are granted under European Law. As the Internet Service Providers Association UK (ISPA) explained it to us:

> *ISPs are mere conduits, carriers of information somewhat like the postal service without editorial control over content posted on its servers by a third-party. However, the Ecommerce Directive provides for ISPs to act "expeditiously" to remove illegal material which is stored on their own networks (e.g. hosted or cached on them) if they acquire "actual knowledge" that they are doing so in order to avoid any potential legal liability for such material. This legal framework has encouraged the development of a thriving, dynamic industry.*

25. Orange also stressed the importance of these immunities in their eyes:

> *The balance created by the legal defence of "mere conduit" has facilitated the open and exponential growth in Internet usage. With the development of user-generated content and Web 2.0 make the 'mere conduit' principle even more relevant. Orange strongly believes that the "mere conduit" principle remains valid, demonstrated by its adoption in most developed jurisdictions, and it has been influential in encouraging the development of the Internet.*

26. However, Denton Wilde Sapte (a law firm) was concerned about the extent of the protection that is granted:

> *The E-Commerce Directive defences have increasingly come under pressure due the fact that companies relying on them are not pure ISPs in the traditional sense, for example social networking sites, and that even ISPs often offer additional content. An example of this is the e-Bay cases in France, Belgium and Germany. The courts came to different conclusions on e-Bay's liability for content on its auction site based on essentially the same facts. This has created inconsistency and uncertainty as to the scope of the defences in this type of situation. The law would benefit from two points of clarification:*
>
> *(a) whether social networking sites and sites hosting predominantly user generated content, such as YouTube, should be protected by the E-Commerce Directive defences at all. Are their activities somewhere beyond acting as a mere pipe for traffic and should they therefore take more responsibility for the content on their sites? They are in many ways different from the traditional ISPs; and*
>
> *(b) that where ISPs and other service providers include professional and commercial content as part of their services, as has been increasingly the case, the "E-Commerce Directive defences only apply to the activities where the provider is truly acting as a mere conduit or caching or hosting and not for all their activities. ISPs are becoming increasingly multi-purpose and there needs to be a recognition that there is a limit to the extent to which they can rely on the defence.*

27. But to return to the general point that Andrew Cormack was making. The way in which the "mere conduit" immunity is phrased, is that it is lost if the ISP "selects" or "modifies" the information within a transmission. This was clearly intended to distinguish between an organisation who generated traffic (who would not be immune from action over what they generated), and those who just supplied the communication pipes to carry the traffic (who would not be liable for carrying material they knew nothing about).

28. However, this phrasing means that communication pipe suppliers who are attempting to clean up traffic will lose their "mere conduit" immunity. Of course, this may not immediately open up an ISP to legal action, since they may have other immunities they can rely upon – but in such circumstances, the eCommerce Directive will not be of assistance to them.

29. The Periodical Publishers Association (PPA) are calling for the "mere conduit" immunity to be rescinded once the ISP is put on notice of illegal traffic – much as their "hosting" immunity is only relevant until the ISP has "actual knowledge", after which they must cease to host material or face the legal consequences:

> *PPA supports the "mere conduit" defence. In the circumstances when the mere conduit provisions apply PPA does not believe it is appropriate that ISPs should be required to monitor or filter all traffic to seek out "wicked" or illegal traffic.*
>
> *However, PPA believes it would be useful to identify more clearly the boundaries of this defence and to make it clear that the shield offered by this defence is removed once the ISP takes unilateral action to monitor or has been provided with evidence of*

the "wicked" or illegal traffic (whether criminal or in breach of civil laws such as copyright or defamation) which is sufficient to allow the ISP to prevent access to or remove materials it is hosting or where it has a direct relationship with the source of the "wicked" or illegal material by, for example, providing internet access or hyperlinks to the source.

Illegal sharing of copyrighted material

30. Other "rightsholders", the bodies representing the publishing, music and film industries, had a rather different view of the extent to which "mere conduit" conferred immunity. The Alliance Against IP Theft said:

The Committee, in its introduction to the inquiry, has suggested that ISPs have "almost no legal liability for the traffic that passes across their networks". We do not believe that is strictly true with regards to copyright infringement. While ISPs may point to the E-Commerce Directive, stating they are a "mere conduit", rights holders do not believe this defence is absolute. In addition, the Copyright Directive allows copyright owners to seek injunctions, requiring ISPs to stop illegal activity on their networks.

31. A typical view was that expressed by the British Recorded Music Industry (BPI):

"Bad traffic" could arguably be used to describe the ubiquitous daily online copyright infringement committed by peer to peer users, for two reasons.

First, it is a straightforward breach of the law for a person to upload (i.e. make available) copyright material without the authorisation of the rightsholders. Committing a strict liability offence in this way should not simply be ignored. […]

Secondly, the economic impact of this form of "bad traffic" on the creative sector is highly damaging. Copyright infringement online leads directly to a loss of revenue to the rightsholders, seriously threatening their viability as businesses, and impacting on employment in the sector.

32. The rightsholders had a number of explanations as to why the ISPs were not prepared to deal with what they saw as bad traffic. The Motion Picture Association told us:

One explanation for the current unwillingness of ISPs to cooperate could be a fear of a competitive disadvantage flowing from actions to discourage "bad traffic". This argues for some degree of government intervention to ensure a level playing field, perhaps in the form of a government-sanctioned enforceable Code of Practice establishing a minimum standard of responsible behaviour.

33. The ISPs generally felt that asking them to act as a proxy for the rightsholders was inappropriate. For example, T-Mobile told us:

It is unclear why T-Mobile should be expected or forced to bear the costs of protecting a third-party's rights.

34. TalkTalk drew our attention to other difficulties which occurred when ISPs got involved in trying to prevent unlawful file sharing:

For instance, the current approach to identifying illegal filesharers is unreliable in correctly identifying the perpetrator with the consequence that innocent parties are sometimes identified. It is also easy for individuals illegally filesharing to avoid detection by encrypting their traffic or hijacking someone else's IP address or using their wi-fi network. Similarly, site blocking is relatively simple to get around.

35. There were also concerns expressed about whether identifying people who accessed the Internet via the mobile telephone networks would be possible at all. T-Mobile explained

that the way in which the mobile industry allocated IP addresses to customers caused particular problems:

> *Whilst technical options are often viewed as a panacea the Group should be aware that there are serious practical reasons why the measures proposed in the Digital Britain interim report that work for fixed ISPs will not readily apply in a mobile environment. In particular mobile operators cannot identify individual rights infringers from public IP addresses alone with sufficient degree of confidence to support taking action against customers.*

36. TalkTalk went on to ask (and a great many other respondents made similar points about new business models) if there were better policy options:

> *In many cases there will be other possible approaches to addressing the problem. For instance, in the case of illegal filesharing, education, alternative business models and limited court action make go a long way to addressing the issue. Any consideration of whether an ISP should act must also consider what alternatives exist and whether these would be more appropriate.*
>
> *In principle, we see that there may be circumstances where it is appropriate for ISPs to act [...] However, given the potential issues with other approaches, it is critical to scrutinise and assess any potential initiative against these criteria.*

37. Some people suggested that one way to approach file sharing was to ensure that people paid appropriately for network usage, or – as the rightsholders have proposed – have their traffic artificially slowed down if they use the Internet too "much". As a policy option, this will of course be more attractive to the film industry (where file sizes are very large) rather than publishing, or the music industry, where files are relatively tiny.

The Internet Watch Foundation (IWF) blocking list

38. Most people made the general point to us that we had asked a poor question in our call for evidence. What might or not be "bad traffic" would be a matter of opinion or perspective, and that ISPs were not particularly suited to making such decisions on behalf of society. As ISPA put it:

> *Industry has generally been unwilling to second guess the will of Parliament on freedom of speech issues.*

and T-Mobile had a specific example:

> *Asking ISPs to block content that is offensive to some people (such as anorexia sites), but is clearly legal, places them as arbiters in deciding what their customers can access.*

39. However, as everyone pointed out, there is already a "bad traffic" blocking system that has been deployed by the largest ISPs. The Internet Watch Foundation (IWF) collates a list of child sexual abuse image websites, and then a number of ISPs prevent access to these websites. The technical methods vary, but the intent is that attempts to view these websites will fail.

40. As Skype put it:

> *In a democracy, telephone companies should not eavesdrop on the conversations that go through their networks, for privacy reasons there is indeed a strong argument for those entities transporting or handling Internet traffic not to know the nature and detail of its content. This is true whether or not they have the technical abilities to do so. The risks posed by such new technologies as 'Deep Packet Inspection' in this respect are worthy of examination. The only exception to this rule has been, and should remain, when truly necessary for society and security, in well-defined areas*

like child pornography, and respecting due process, judicial authority when relevant, and fundamental freedoms.

41. The Internet Service Providers Association UK (ISPA) explained further:

Mere conduits are also asked to take action at a network level on certain occasions. ISPs work alongside the Internet Watch Foundation (IWF) […] As the vast majority of illegal content is hosted outside the UK, the IWF provides a list of URLs that are hosted outside of the UK that it has assessed as containing images of child sexual abuse. This list is voluntarily deployed in network-level filters by UK ISPs, representing the majority of consumers, to prevent users from inadvertently stumbling across these websites.

It is widely agreed that images of child sexual abuse constitute a unique category of illegal material, which is why it is considered appropriate by these ISPs to deploy a network-level blocking solution. While public and political consensus in support for blocking this kind of material is high, this has not always been the case. It has taken 10 years for confidence in the work of IWF and industry to make blocking an appropriate tool.

42. The ISPs felt that it was necessary to justify why they went along with the blocking of child sexual abuse websites, but were not prepared to consider blocking other content or other types of activity. For example Virgin Media told us:

Equally, however, questions about when and how ISPs should act to deal with different types of traffic are as much to do with ensuring that we maintain customer confidence and opinion. The public's attitude towards management of their on-line behaviour is far from consistent. When it comes to issues of child protection, or racist or terrorist websites, there is almost universal agreement that ISPs should take action. However in a number of other areas, there is far from unanimous agreement on the lengths to which ISPs should act.

43. Similarly, Orange said:

Orange's decision to implement such a system was based on the fact that (i) it was a criminal offence for its customers to view such images; and (ii) the content in question – child abuse images – was unique in that behind every picture was a human victim and because it is such an emotive subject, the Orange executive board decided it was appropriate to intervene.

44. The Mobile Broadband Group (MBG) viewed this blocking as a success for self-regulation and cautioned against putting it on a statutory basis:

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.

45. The MBG also felt that blocking based on the IWF list was likely to be a "one off".

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.

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.

46. The Open Rights Group (ORG) took a similar view of this being a special case:

We would also wish to state that dealing with sex abuse images separately from other sorts of content seems useful to us, to prevent concerns around freedom of speech, the limits to which, including hate speech and libel, are better defined through the courts.

47. Conversely, the rightsholders clearly felt that this blocking should be seen as creating some sort of precedent. Respect for Film put it this way:

It is clear, however, that ISPs themselves accept responsibility for tackling certain forms of illegal content being transmitted over their networks, demonstrated by their funding of the Internet Watch Foundation. What is unclear, though, is the decision-making process that lies behind such decisions and whether such action is taken out of a sense of moral or legal responsibility. When the state has agreed that something is illegal, we believe that should be sufficient for ISPs to accept a share of the responsibility in bringing such activity to an end when it is brought to their attention, the means for doing so are at their disposal and the illegal activity is conducted over their networks.

48. In particular, it might well be felt that the deployment of a system to block selected web content might cause ISPs to lose their "mere conduit" immunities, at least for some aspects of their operations. Apparently the Home Office do not believe this to be the case, for Orange told us:

Orange consulted the Home Office to ensure that the voluntary implementation of this solution would not endanger Orange's reliance on the "mere conduit" defence. Without such an assurance it is unlikely that Orange would have implemented such a solution.

It is unclear how significant this assurance might be, since the Home Office does not make the law of the land, nor does it usually set out to interpret its meaning.

49. Finally, the Open Rights Group drew our attention to a key difficulty in attempting to use technology to deal with file sharing systems, which is that sharing some content by some people will be lawful, and technical systems cannot by themselves unpick the legal background:

As a principle, the Open Rights Group believes that in all but the most extreme circumstances, illegal content should be dealt with at source. This is by far the most effective way of getting material removed. Methods of 'blocking' or restriction are likely to be fraught and create unintended consequences, including preventing market access.

In our work on copyright enforcement, the Open Rights Group has identified a particular concern over the practicalities of using ISP networks using tools to monitor for copyright material being transferred in order to reduce infringement.

We feel that monitoring networks for copyright material is extremely unlikely to work well. Detection of material may be possible, while creating new expenses for providers and placing strain on networks, but detection cannot hope to understand the licensing agreements that have been made.

Conclusions regarding Question 1

50. We are concerned about the amount of "bad traffic" such as spam and denial of service attacks that emerges from some ISP networks. We have noted the reservations expressed to us about ISPs taking action in this area, but quite clearly a great deal more needs to be done in order to reduce the number of end users whose machines are malware infected. Although it is not necessarily the ISPs "fault" that these problems are occurring, they are uniquely placed to detect problems, to notify users, and to disconnect users who refuse to take remedial action.

51. We believe that voluntary arrangements would be the best way of tackling this issue and note with approval the initiative which is already under way in Australia. Accordingly, **we recommend that UK ISPs, through Ofcom, ISPA or another appropriate organisation, immediately start the process of agreeing a voluntary code for detection of, and effective dealing with, malware infected machines in the UK.**

52. **If this voluntary approach fails to yield results in a timely manner, then we further recommend that Ofcom unilaterally create such a code, and impose it upon the UK ISP industry on a statutory basis.**

53. We agree with the view that was put to us that the current legal protections relating to "hosting" and "mere conduit" are capable of having a counterproductive effect, in that they may discourage some proactive approaches by ISPs.

54. We recognise that tidying up this area risks overlaying significant complexity over some very simple principles. Nevertheless, **we recommend that the Government revise the law to enable ISPs to take proactive steps to detect and remove inappropriate content from their services, without completely losing important legal immunities which fit with their third party role in hosting and distributing content.**

55. This issue is also relevant to the proactive blocking of material on the IWF's list, which some ISPs have voluntarily undertaken as a self-regulatory measure. We particularly agree with the Mobile Broadband Group's comments on self-regulation in paragraph 45 above. **We recommend that the Government does not legislate to enforce the deployment of blocking systems based on the IWF lists. This has the potential to damage future attempts to fix problems through self-regulation, and will thus, in the long term, be counterproductive.**

56. Turning now to the question of "bad" file sharing traffic. We are only too well aware that since we received written responses in May, and heard oral evidence in July, much more has happened. The final version of the Digital Britain Report has been published; the Department for Business Innovation and Skills has published a consultation paper on dealing with illegal file sharing based on the Report's approach; and latterly the Secretary of State has announced a change in the preferred policy to include disconnecting end users – and then slightly extended the consultation period.

57. We are therefore reluctant to make a substantial number of further recommendations based on the evidence we received in the Spring and Summer, since it is self-evidently now incomplete. However, we have reached some conclusions.

58. **We conclude that much of the problem with illegal sharing of copyrighted material has been caused by the rightsholders, and the music industry in particular, being far too slow in getting their act together and making popular legal alternatives available.**

59. **We do not believe that disconnecting end users is in the slightest bit consistent with policies that attempt to promote eGovernment, and we recommend that this approach to dealing with illegal file-sharing should not be further considered.**

60. **We think that it is inappropriate to make policy choices in the UK when policy options are still to be agreed by the EU Commission and EU Parliament in their negotiations over the "Telecoms Package". We recommend that the Government terminate their current policy-making process, and restart it with a new consultation once the EU has made its decisions.**

Question 2: "Behavioural Advertising"

61. The second of our questions was:

> 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?

What is "behavioural advertising"?

62. The Internet Advertising Bureau (IAB), the UK trade body for digital advertising explained the nature of behavioural advertising to us, distinguishing it from contextual or demographic advertising:

> *Behavioural advertising is not a new phenomenon. It occurs in the "offline" world: for example, television programmes "recommendations" on Personal Video Recorders (PVRs) based upon a user's previous viewing habits. On the internet, it is a type of advertising based upon anonymous web browsing activity which is collected and grouped into interest "segments" (such as cars, finance and travel) to provide more targeted and relevant marketing messages. It works using a "cookie" – a small file of random letters and numbers – which is placed on a computer's web browser to ensure the relevant advertising reaches the right "segment" of users. A cookie does not in itself collect any information.*

63. The IAB included some figures with their submission:

> *UK behavioural advertising currently makes up between 10-15% of all online display advertising (in 2008, online display advertising spend was £637m). Enders Analysis predicts that this is likely to grow to 30% by 2013. The IAB believes this may be a conservative estimate. However, we acknowledge the privacy concerns surrounding behavioural advertising and believe that, in order for the sector to continue to grow, transparency and choice is needed to build greater user trust in the practice.*

64. Gill Davison also took a functional view of behavioural advertising. She explained that the use of cookies to recognise visitors who returned to the same website, or to track their behaviour as they visited associated sites, was a technique that had been around for some time. She described it as:

> *A fairly benign type of advertising where users are tracked by advertising networks as the users surf websites that partner with the advertising network. Data is collected via 'cookies' and 'web beacons'. More experienced users generally know how to opt out of this type of tracking.*

65. Industry respondents generally liked the ideas behind behavioural advertising, Jim Deans from Global Digital Broadcast said:

> *Understanding a consumer's habits is big business for advertisers and, in most cases, the information this new software collects is positive. For example, if I have watched 20 fishing programmes and visited 10 fishing websites, you can pretty much assume*

correctly I like fishing, so offering me a new fishing product will not upset me and I might even buy.

66. However, the individuals who responded to us did not seem so enthusiastic, and Consumer Focus viewed the approach as being "profiling" and told us:

Profiling potentially limits the diversity of content, restricting choice and concentrating the market as the tendency to generalise may lead to a diminution of preferences, differences and values. It also collects sensitive information, such as health or medical issues and potentially targets the vulnerability of certain users in a way that is not known in traditional commercial arrangements.

67. However, the individuals who responded to us may not be representative of the population as a whole: The Broadband Stakeholder Group took the view that the prevalence of behavioural advertising was evidence in itself of acceptance:

Whilst there are clearly some consumers who are uncomfortable with the very concept of their online behaviour being monetised, the full range of current products and services in the market (loyalty cards for example) demonstrates that there are a significant set of consumers who understand and are comfortable with the exchange of data in return for products and services which they value. Furthermore, there would appear to be a proportion of consumers predominantly concerned with how they are informed about such services, rather than the operation of such services per se.

68. However, AT&T, put forward some contrary evidence from research:

AT&T has actually conducted focus groups and asked our customers their views on behavioural advertising, and the results have been illuminating. Customers clearly appear to understand and willingly accept that information will be collected in commercial relationships – both offline and online – and will be used to offer goods and services that are of value to them.

But it seems equally clear that these same consumers do not well understand or fully embrace the concept – what we now call "behavioural advertising" or "invisible tracking" – that their online activity associated across unrelated websites, or their overall web-browsing activity, can be and is used to create detailed profiles of them. They can see the benefits of more targeted and relevant advertising, but they want control over their personal information, and they want that control to be individualised.

Phorm

69. So far we've been discussing behavioural advertising in general. Gill Davison, who we mentioned above in paragraph #64 above, went on to describe a new and, in her opinion "disturbing", development in the behavioural advertising space:

This involved the use of interception equipment installed within the ISP's network to snoop upon individuals to collect and examine data packets from their browsing stream. The ISP then earns an additional revenue stream by providing the data, or portions of the data to third parties. Advertising can then be served to the user based upon their browsing habits.

70. She went on to draw attention to the impact of this on the website owners:

So far, 'if' any consent has been asked for this type of interception, it has only been asked from the user and not from the websites that they have browsed. An analogy to this would be for me to be placing an order to "Marks and Spencers" on the phone, and for a third party to be listening in and sending me adverts for John Lewis products based upon our conversation, but for "Marks and Spencers" not to know

that any third party is listening in. I believe that this particular business model should be illegal on the internet, just as it would be on the phone.

71. Phorm have a product that operates roughly as Gill Davison describes. They say:

Phorm is a UK based technology company that has developed, over the course of the last seven years, a solution that allows advertisers to deliver behaviourally and contextually targeted advertising while preserving consumers' personal privacy and data security. We have exclusive agreements with ISPs representing c. 70% of UK broadband subscribers, and are at various stages of engagement with partners in other leading Internet economies around the world.

72. However, their design differs in that raw data does not flow to third parties, and they avoid identifying individual users, but create an anonymised profile of interests linked to a random identifier. In her oral evidence Radha Burgess of Phorm told us:

We have built a system that is predicated on the idea of data minimisation by design, so while other advertising systems spend a lot of time gathering a huge amount of data on users and lots of it is, arguably, personally identifiable, Phorm only stores a very, very small amount of data and, again, this is not personally identifiable. […]

We have a very, very lean system that has been built absolutely from the beginning so as to consciously avoid the storage of any type of personal information. As everyone will know here because I am sure you all know the ins and outs of how various advertising systems work, but that is highly unorthodox. The orthodoxy at the moment is to gather as much information as you can, store it for as long as possible and then mine it as when you, as a commercial company, feel the need to get that information and use it for whatever purpose. Therefore, if we are talking about the Data Protection Act, we have done something that not only complies […] but it far exceeds any of the requirements of the Data Protection Act simply because there is this deliberate, conscious avoidance of any storage of any personal information

73. However a fair bit of the evidence we received related not to the Phorm design per se, but to the way in which Phorm had tested their system towards the end of their seven year development. The comment from Robert M Jones is typical.

I was particularly furious at the discovery that there had been two covert trials of this technology by my ISP, BT, and that BT were unable/unwilling to tell me whether my traffic had been intercepted and profiled. During the trials they also denied what was going on to press and customers. Since that time, my trust in my ISP has been destroyed.

74. What appears to have taken place is that in September 2006 and again in Summer 2007, Phorm and BT ran some secret trials of developmental versions of their traffic inspection system. Side effects from these trials were noticed at the time, but it was not realised quite what was going on. Then in February 2008 Phorm went public about their system, announcing agreements with the three largest UK ISPs, BT, Virgin Media and TalkTalk. Technical descriptions were then published of how the system operated, and doubts began to be expressed about its legality, and the secret trials were remembered.

75. Phorm maintain that their system is entirely legal, and they particularly draw our attention to opinions from the Home Office and the Department for Business, Enterprise & Regulatory Reform (BERR) as it was then called:

While Phorm has attracted considerable attention as a result of its partnership with ISPs, BERR has stated that our service is capable of being deployed legally. Further, the Home Office has indicated that Phorm's service does not fall foul of RIPA, which law is not intended to inhibit legitimate user-based applications with no harm to individuals. Such services include Phorm, spam filters and Gmail. In an environment when technological change is incessant, what matters is not which specific

technology is deployed, but the most important issue of whether or not consumers' personal data and privacy are protected,

76. Various campaigners did not accept the accuracy of the Home Office's legal opinion and went to the police to complain that the Phorm system performed illegal interception of their traffic contrary to the Regulation of Investigatory Powers Act 2000 (RIPA). Several forces refused to investigate the matter at all, with the sole exception being the City of London force. They came to the conclusion that no crime had been committed. Following further complaints, that decision is currently being reviewed by the Crown Prosecution Service.

77. Some suggested that RIPA complaints should be made to the Interception of Communications Commissioner, but his role is to investigate complaints about interception by public bodies, and so he would not be an appropriate person to contact.

78. The campaigners also approached the Information Commissioner's Office (ICO), who took the view that to conform to Data Protection laws, permission had to be sought from ISP customers before traffic was monitored, viz: that the system had to be "opt in". This was at odds with the indicated plans for the system, which was apparently to have been run (by some of the ISPs at least) on an "opt out" basis.

79. A further trial by BT and Phorm took place in Autumn 2008. This trial was only for a small number of volunteers – that is they all opted in, so the ICO's view had been acceded to. A recent trial at a Korean ISP has also been operated on an opt-in basis.

80. However, since no permission at all had been sought from users affected by the secret trials (and there had not even been the opportunity to "opt out") this caused further complaints to be made to the ICO. The ICO have decided to take no action on these complaints – apparently on the basis that they do not expect any similar trials to take place in the future, so they do not feel it would be useful to examine what may or may not have occurred in the past.

81. Complaints were then made to Vivian Reding, the EU Commissioner for Information Society and Media, pointing out that the police and regulators in the UK had failed to deliver satisfaction to the complainants. The Commission seems to have taken this matter seriously, and has expressed some concerns to the effect that there may be some flaws in the transposition of relevant EU Directives within the UK. They have started a legal process to determine whether or not this might be correct – potentially ending in legal proceedings to get UK statutes changed.

82. Over the summer it has become clear that none of the three large ISPs will be deploying a Phorm system in the near future, if at all. The company continues to work with ISPs in other countries, and in particular Korea.

83. The events surrounding the Phorm trials have clearly coloured a number of the recommendations made to us. The Open Rights Group said:

Government should insist that all interceptions require the informed consent of all participants, as expected under RIPA. In the case of Phorm and BT, this would mean that web services / sites should agree to partner with Phorm and BT, and be required to inform their users that Phorm and BT will be able to intercept their traffic.

The Phorm interception case also showed that the UK does not have sufficient protections for commercial or domestic surveillance or interception of communication.

The government should amend RIPA to extend the duties of the Intercept Commissioner to nongovernmental interceptions. The activities of the Interception of Communications Commissioner must also be properly resourced and open to much greater public scrutiny.

84. The Periodical Publishers Association (PPA) said:

> *PPA believes that use of Deep Packet Inspection to intercept and read transmissions and data on the internet without fully informed and express consent of the originator and recipient is unlawful and should be unacceptable.*

85. Neil Maybin expressed his concerns this way:

> *In theory, existing UK laws provide adequate protection of privacy in the Internet. In practice they do not. The Regulation of Investigatory Powers Act 2000 should provide users and websites with protection against the interception and processing of their communications by a third party. Yet the UK Government appears unwilling to enforce it.*
>
> *In the case of BT's secret trials of Phorm in 2006 and 2007 the police appeared to believe that web users generally consented to having their communications intercepted.*

86. Jamie Dowling felt that enforcing the law was important, even for events in the past that might not recur:

> *The failure of government and watchdogs to enforce existing law in relation to the 2006 and 2007 secret testing by BT and Phorm provided a seed from which a very strong campaign has emerged.*
>
> *Government must enforce the law wherever it is broken, regardless of whether an individual or a corporation has broken the law. Government has a duty to respect and enforce European law to which it is a signatory. It has failed to do that and rightly faces legal action for that failure.*

87. The Foundation for Information Policy Research (FIPR), who have published a number of lengthy analyses of the legal position of Phorm was rather more pithy:

> *On the issue of behavioural advertising and Phorm, I will simply reiterate the comment of FIPR's General Counsel, Nicholas Bohm: it is amazing that the Home Office gave out free legal advice and disappointing that it was so inaccurate.*

We once again note that, as we did in paragraph #48 above, the Home Office does not make the law of the land, nor does it usually set out to interpret its meaning.

88. We will however give the last word in this subsection to Phorm (who refer to their system under the brand name of Webwise), and who continue to insist that their system is entirely legal:

> *The anti-Phormers repeatedly allege that Webwise contravenes the Regulation of Investigatory Powers Act (RIPA). This relies on a selective misreading of the legislation and its application outside it intended scope (telephone calls, post and e-mail) to an unintended area – browsing the internet. The term 'communication' implies the mutual transfer of information with an expectation of privacy, which is accurate for telephone calls or email, but not for web browsing, which is much closer to a publishing or broadcast model. [..]*
>
> *In Webwise, communications data is not made available to anyone. It is processed automatically, in real time and deleted as soon as an 'interest match' has been made. Only the interest match is stored, not the data, and this information is not made available to anyone. [..]*
>
> *The ISP provides the Webwise service to the user, and acts as their agent. Webwise processing of the user's web requests therefore occurs before the request is transmitted to the website, and processing of the website response occurs after it has been received at the ISP. Therefore 'interception' does not occur 'in the course of transmission'.*

Possible regulation of behavioural advertising

89. Industry respondents were not generally in favour of new laws in such a novel area as behavioural advertising. T-Mobile's view was typical:

> *Premature regulation on matters that are not fully considered and understood runs the risk of unintended adverse consequences.*

90. The Broadband Stakeholder Group was similarly cautious:

> *It should not be the role of government either to promote or discourage the deployment of such services. It is our view that the correct role for government should principally be to provide legal clarity and ensure that the regulatory framework remains fit for purpose and is effectively enforced to ensure privacy and data protection. At the same time government has a responsibility to recognise the need to enable innovation in the market place when developing policy in this area.*

91. Skype felt that the current legal framework was suitable, although it might need some tweaking:

> *Behavioural advertising represents a potential for innovation and consumer benefit which cannot be neglected. Although there are clearly privacy questions in this area, there is an existing, extensive and long-held legal framework for privacy in the UK which does not need further government intervention. What may be needed from the authorities in this respect is to ensure that enforcement of existing privacy laws is cognizant of, adapted to, and resourced for the Internet age, coupled with awareness raising.*

92. Several industry respondents felt that the main problem was a lack of clarity about what was going on. AT&T said:

> *Yet, the concern here is not necessarily that there will be more or new forms of online advertising. Rather, pitfalls arise because behavioural advertising in its current forms is largely invisible to consumers. Consumers confront an overwhelming amount of online content and advertising without the benefit of a cohesive explanation of the businesses or relationships that underlie that content, the manner in which the consumer's personal information is collected or used, or the control – or lack thereof – that the consumer has over her personal information in the first place.*

93. Virgin Media was also concerned about clarity and simplicity:

> *While the legal framework around privacy and data protection already exists, there is a key role for Government in clarifying and simplifying that framework to ensure that it is capable of being applied to a fast moving digital economy. This clarity is essential if consumers are to be clear about their rights, confident about their privacy and free to enjoy the potential benefits such services could provide.*

94. Consumer Focus also used the "clarity" word:

> *We are not opposed to behavioural advertising but there needs to be clarity around how information provided by a consumer and their online behavioural patterns are being accessed and stored, in addition to positive informed consent by consumers to these practices. We know profiling and targeting go on behind the scenes, which is why if you have recently booked an airfare you will receive hotel ads, or if you watch the football online you seem to be targeted with beer ads. However, the issue of consent to this 'behind the screen' information collection is often brushed aside. Phone tapping or listening devices are not tolerated in a democratic society without extraordinary justification and compliance with legislation, however digital profiling is a daily occurrence.*

95. Phil Brooke saw regulation as important because individual users, on their own, were not capable of making a difference:

> *The government should be intervening to protect the public on this matter. The use of inspection of data traffic, and potential modification to traffic to insert advertising is not appropriate: it is not for advertisers or ISPs to decide that data travelling between a user and an arbitrary web site should be tampered with. The important point here is that individual users are not able to negotiate individual terms.*

96. Miles Golding was concerned about a specific issue – the way in which existing opt-in, opt-out settings often depend on cookies, and preferences are lost when cookies are mass-deleted:

> *The government must formulate and apply robust laws that protect citizens' privacy, and ensure that ISPs respect those laws. Any "value-added" systems must follow a clear once-and-for-all opt-in or opt-out choice for each account-holder – no cookies that get cleared and have to be reset each time.*

97. BBBritain was equally concerned that cookie handling was too complex:

> *The current state of cookie development and particularly third party cookies, will demand that Internet browsers are upgraded to support the right to choose. The right to choose should not be buried in the workings of a hard to find browser setting but be transparent to the user. This is something the Gov can specify and demand as a minimum requirement.*

The Internet Advertising Bureau "Good Practice Principles"

98. Ofcom told us that behavioural advertising was not really their area, but nevertheless they set out some principles. They wanted to see a framework with transparency:

> *Companies deploying these technologies must clearly explain how they work and what is done with the data that is collected;*

with informed consent:

> *Consumers must have a real, prominent and easily understood opportunity to decide about participation. Their consent must be sought using clear, non-technical language and the terms must not be hidden away in the often murky depths of the service providers' privacy policy. And consumers must be able to change their mind at any time, without penalty;*

and they also wanted to see effective processes for handling complaints, along with the exclusion of some specific areas:

> *Behavioural advertising must not target children or be used in potentially sensitive areas like health, sexuality and religion.*

99. The Internet Advertising Bureau (IAB) drew our attention to their "Good Practice Principles" which, in summary are:

#1 Notice: Clear and unambiguous notice must be given when data is collected for behaviour advertising purposes.

#2 User choice: An opt-out mechanism must be provided at the very least; in some circumstances informed consent must be obtained.

#3 Education: Users must be provided with clear and simple information about the use of their data for behavioural advertising, and how they can opt out.

100. These Good Practice Principles were welcomed by the Mobile Broadband Group:

> *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.*

101. Virgin Media was in favour of self-regulation, of which the Good Practice Principles are just one part, telling us:

> *Some good work has been undertaken by the Internet Advertising Bureau in developing good practice principles in this area, and we believe that UKCISS provides another forum in which such principles could be developed.*
>
> *On a pan-European level we are pleased to see the European Consumer Commissioner, Meglena Kuneva, taking an active interest in this issue and believe that her principles of transparency, clear information, choice, fair commercial communications and fair contract terms are key to ensuring that consumers can feel confident about being online.*

Opt-in/Opt-out

102. It will be noted that the Internet Advertising Bureau Good Practice Principles specify the default to be an "opt-out" regime: people have to actively request that their data is not used for behavioural advertising, and if they say nothing then they are deemed to have acquiesced. The alternative approach is "opt-in", where people have to actively request behavioural advertising, and saying nothing means that their data will not be processed.

103. It might be though that businesses and business umbrella groups would be entirely in favour of "opt-out", but this was not always the case. For example, Hutchinson 3G UK ("3") told us:

> *3 do not use behavioural advertising, and have no plans to introduce advertising based on a users' online activities or usage. We continue to work with the MBG and Internet Advertising Bureau in order to establish strong guidelines which protect the consumer and are understood by stakeholders. It is our belief that any behavioural advertising service should be an opt-in rather than opt-out service.*

104. However, in some circumstances they do collect data (albeit anonymised data) without offering any choice at all:

> *3 do however support the GSMA's Mobile Metrics project to collect anonymised mobile browsing statistics so that advertisers and websites have audited data to base their payments and charges on. We believe that this will encourage investment in mobile websites which will be a benefit to customers.*

105. The individuals who responded to us mainly favoured "opt in", The Open Rights Group, who describe themselves as a "grassroots digital advocacy group" were in favour of "opt-in":

> *Under current IAB guidelines, users can if they are aware of behavioural advertising make a choice to 'opt out'. Unfortunately, because many of these systems are 'cookie based', it is harder to stay opted out than become opted back in.*
>
> *'Opting in' should happen without duress. Data sharing or profiling should not be mandatory in order to take up a commercial service.*

106. Privacy International wanted behavioural advertising to be treated the same way as location-based services (the sort of advertising that can be done over short-range Bluetooth connections to mobile phones, or over normal channels when the phone's location is known):

Privacy International believes that all behavioural advertising models (irrespective of the technology) should only be permitted to be deployed on a basis of explicit informed consent and that such models should be required to be Opt-In as opposed to the industry's preference of Opt-Out. In this respect, the rules that apply to Bluetooth mobile advertising should apply to online advertising.

107. Privacy International also made explicit the sub-text to this debate, that the public were not so convinced of the merits of behavioural advertising that they will actively seek it out – so the industry must rely on inertia to ensure a reasonable audience size;

It is clear that the commercial sector are committed to an Opt-Out model based on their fear that the public are cautious and concerned about behavioural advertising and what this means for their privacy.

Behavioural advertising to children

108. The Internet Advertising Bureau Good Practice Principles also contain specific rules concerning children:

No business that collects and uses information for behavioural advertising (and has agreed to the Principles) will create an "interest segment" intended for the sole purpose of targeting children under the age of 13 years of age.

109. This was an area of concern for Consumer Focus:

Almost every website used by young people is commercial. The content is funded by three methods: selling advertising space to third parties who want to target children; selling merchandise direct from the site; and/or collecting children's data to sell to other organisations. Self-regulation and best practice guidelines do exist to protect children but are not standard between nations and often are confusing and misleading in their interpretation

110. The Child Exploitation and Online Protection Centre (CEOP) also addressed this issue:

Children are very often not able to distinguish what is and what is not an advert on the websites that they frequently use. This is epitomised by hidden product placement where advertising is subtly blended into content.

We would argue that greater regulation would give advertisers an obligation to ensure transparency in their marketing strategies. Children and their parents/carers would then be able to more easily understand how they are targeted by commercial messages when online.

111. CEOP's recommendation was to bring websites under the wing of the Advertising Standards Authority:

CEOP supports the position of Ed Mayo, Chief Executive Officer of Consumer Focus, in that children's websites should be regulated through the Committee of Advertising Practice (CAP) codes. Bringing children's websites under the supervision of the Advertising Standards Authority (ASA) would thus give greater protection to children's rights.

Conclusions regarding Question 2

112. We believe that the construction of the Phorm system, and the efforts that the company has made to explain its design, and the comparison they have made with other systems, has made a significant contribution to the debate around what sort of information it is appropriate for advertisers to obtain and how long they should keep it.

113. Phorm has not emerged unscathed from this debate, and we note that during the period of our inquiry it has become clear that their system will not be deployed by any UK ISPs, at least in the near future.

114. Although this issue didn't feature much in the evidence we received in this inquiry, we are particularly aware of comparisons between Phorm's data processing and that done by search engines, and particularly by Google. The Phorm system does not appear to retain personal data for long periods – whereas Google has been specifically criticised by European Data Protection Authorities for the long periods it keeps personal data.

115. We were deeply disappointed that Google, the clear market leader in online advertising, and the operator of a rather different type of behavioural advertising system, did not submit any evidence to this inquiry, despite a specific request from us to do so.

116. We do not believe that it is at all appropriate to consider the deployment of any type of behavioural advertising system without explicit, informed, "opt-in" by everyone whose data is to be processed, and whose behaviour is to be monitored and whose interests are to be deduced. We do not believe that "opt-out", however commercially convenient, is the way that these systems should be run. To that extent, the Good Practice Principles promoted by the Internet Advertising Bureau are insufficient to protect people.

117. **We recommend that the Government review the existing legislation applying to behavioural advertising, and bring forward new rules as needed, to ensure that these systems are only operated on an explicit, informed, opt-in basis.**

118. We are particularly concerned that behavioural advertising systems may be being deployed without sufficient consideration being given to protecting the interests of children and young people. We did not receive sufficient evidence to form a view as to the way forward, but it is a matter that requires urgent consideration. **We recommend the UK Council for Child Internet Safety (UKCCIS) consider how behavioural advertising that is aimed at children and young people should be regulated.**

Question 3: "Online Privacy"

119. The third of our questions was:

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

120. A handful of responders read this question as referring to "online piracy". We have considered their answers as being further responses to the "bad traffic" question above.

121. There was consensus that people were entitled to privacy online, and concerns that they were not currently experiencing it. Suggestions as to how to deal with it fell into two main camps: those who thought user education was the key, and those who wanted to see more and better regulation. We will deal with these approaches in turn.

Education

122. Privacy International provided a list of recommendations for addressing online privacy concerns, and the first item on their list was:

> *Educate the public to make them more aware of why their privacy is important, how online activities pose a threat to their privacy and how to be more responsible for their own privacy.*

123. However, this was not just a view taken by NGOs. Skype believed that online privacy should be addressed by an education approach:

> *A global culture of cybersecurity needs to emerge, whereby citizens will not only be more careful about their personal data, but they will have a better understanding of*

which pitfalls to avoid. Therefore, we would submit that initiatives on online privacy should focus on building citizens' awareness, and on building increased IT skills more generally.

124. The Mobile Broadband Group also believed that individual responsibility was essential:

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.

125. The Child Exploitation & Online Protection Centre (CEOP) told us about their Thinkuknow (TUK) education programme aimed at 5-16 year olds. Since April 2006, 4.2 million have engaged with the programme. One of the key focuses of TUK is to raise awareness of online privacy settings, but CEOP felt that other parties also had a role to play:

There is an issue around children and young people self-generating risk by posting personal information on social networking sites and other applications.

Whilst the TUK programme seeks to highlight the dangers of this, ISPs should also have some corporate social responsibility to raise awareness of potential dangers and to ensure that default privacy settings give maximum user-privacy protection.

126. CEOP also called for auditing of the uptake of Best Practice recommendations:

Guidance developed in partnership with industry and other stakeholders already exists and we would welcome an independent audit of its adoption amongst relevant service providers to help maximise the impact it could have in better protecting our young people.

127. Dr Andy Phippen from the University of Plymouth and his colleagues told us about the work done in conjunction with the South West Grid for Learning (SWGfL):

It is clear from our research that one cannot enforce online privacy via technology. Many privacy technologies have existed for years, yet online privacy and information abuse remains a growing problem. An often quoted statement by IT security experts is that the weakest link in any secure system is the human element. Within the social context this is exacerbated as the traditional controls for information abuse (organisational policy, threats of disciplinary action, etc.) do not exist. The experience of SWGfL in their filtering work bears this out – no matter how effective a filtering technology is, there will always be ways around it, especially with a determined user. In focus group work with young people, it can be astounding to see how many 14 years olds are aware of IP routing, proxying, etc. as ways of getting around filtering technology.

128. They had three main recommendations for improvement:

***# School curriculum:** The curriculum, from Key Stage 1 through to Key Stage 4, should cover eSafety as a core part of learning, and it should be appropriately monitored and assessed by local authorities and OFSTED. The current school's Self Evaluation Framework pays lip service to Internet protection but there is little follow up if it is not addressed.*

***# Media Responsibility:** Parental awareness develops on the whole from media stories or, less frequently, from communications from schools and local authorities. We should stress the responsibility of the media in this context – while scaremongering might sell newspapers and increase viewing figures, it is not constructive to effective public education.*

 # National co-ordination on eSafety education and practice: *National co-ordination, informed by a strong evidence base, is needed to inform the curriculum and ensure it is up to date, relevant, monitored and evaluated appropriately. Teachers are aware that eSafety needs to be addressed in schools, they just require centralised support to ensure they are confident that what they are delivering is relevant and will be appropriately acknowledged.*

Regulation

129. Our question had been whether new initiatives were needed, but many felt that there were plenty of applicable laws already, but they just needed to be enforced. For example Phil Brooke told us:

> *The new initiative needed here is better enforcement of existing data protection legislation.*

a sentiment echoed by BT:

> *We are not convinced that any new initiatives are necessary – rather, existing requirements should be properly applied and enforced.*

130. There was specific criticism of the powers available to the Information Commissioner's Office (ICO). Peter White told us:

> *Currently the ICO does not appear to have sufficient powers to effectively enforce the current legislation due to several statutory instruments not yet having been passed into law and is effectively left with the option of requesting people and companies to comply with the legislation. This needs to be rectified without delay and is part of the reason for the latest EU infraction proceedings.*

and Miles Golding said:

> *It is incomprehensible that the ICO, on their own admission, has no IT expert on their staff, and apparently lacked the resources to call on experts when they received complaints relating to BT's trials of Phorm's Webwise system.*

131. Jamie Dowling had a list of other examples:

> *I contend that the failure of the ICO to protect citizens' rights over DPI, Google StreetView and ID cards is symptomatic of the lack of understanding that government has about technical issues. It is vital that the Committee realises this and takes action to ensure that all future governmental deliberations and dealings with these issues are done so with a sizeable presence of and critical input from independent experts who are clearly seen to have no connections with companies or bodies involved in those issues.*

132. Other areas of Government were also felt to be short of expertise. The Open Rights Group recommended the hiring of Privacy Officers within all government departments along with technically able staff to help them.

133. Other initiatives proposed by ORG were:

> *# Procurement policies for government services should take a much higher regard for both security concerns, and privacy concerns.*
>
> *# No procurement should take place without a Privacy Impact Assessment.*
>
> *# The government should work internationally to promote much more comprehensible standardised privacy agreements, for voluntary use.*
>
> *# The government itself needs to scale back its own schemes for data retention and online 'black box' surveillance which themselves are undermining privacy rights.*

134. Peter John of deformation.org.uk was concerned about Ofcom:

> *The Government should review whether Ofcom can combine the roles of regulating communications, regulating the media, and encouraging investment in infrastructure without unacceptable conflicts of interest arising. The Government should consider whether Ofcom should be split into a telecommunication regulator and a media regulator.*

135. Privacy International saw a need for new laws. Their list of recommendations included:

> *# Legislate effectively to regulate commercial and public sector activities in order to make privacy a primary consideration instead of an after thought.*
>
> *# Empower regulators such as the Information Commissioner in order for them to enforce regulations regarding the use of private data. Giving them powers to initiate criminal prosecutions for unlawful use of private data is critical to the effectiveness of these reforms.*

136. However, all this complexity as to what was or was not covered by existing laws did not impress Leon Clarke. He felt that what was needed was some clear principles backed up by legislation:

> *The recent controversy over Phorm has seen several respected think tanks (and the EU) disagreeing with the government about whether or not BT's trials of Phorm were legal. Since experts so massively disagree about what the law currently says, it's quite hard to defend the status quo.*
>
> *I don't have any precise answers here but I would suggest that there should be a wide-ranging national debate, leading to a bill outlining the fundamental principles of privacy we can expect. This bill needs to lay down principles that are clearly understandable, so that what privacy rights people have don't depend on obscure technicalities.*

137. Consumer Focus came to much the same conclusion:

> *Digital connectivity means that Britain is moving towards increasing informational transparency that is not necessarily top-down, but to some extent democratised, giving rise to citizen surveillance and the inability to establish which personal information is held by who. We renew the National Consumer Council's call for consumer involvement in decision-making on information risks otherwise a consumer backlash will arise against new developments*
>
> *Consumer Focus has asked the Government to clarify and simplify the legal framework governing data sharing in the public and private sector, as well as enhancing the role of the Information Commissioner's Office in policing data sharing. Private and public bodies should be required to provide information to consumers about how to protect and control their own data and provide information about the form, collection and processing of data held. Consumers' continuous willingness to provide personal data will depend on whether or not they have confidence in the way data sharing and use is regulated.*

138. The Foundation for Information Policy Research (FIPR) was also looking for a new legal regime, but was specifically concerned about "regulatory capture", where over time, decisions are made more in favour of the sector being regulated, rather than in the general public interest. They felt that this could be addressed through legal action, but only if it was realistic for people to consider going to court:

> *To stop the erosion of privacy, we need a legal regime in which individuals can sue search engines, credit reference agencies, behavioural marketers and banks, without risking bankruptcy if they lose.*

Other issues

139. A few other relevant issues were raised with us, under this heading, which we feel are worth mentioning in our report.

140. The Periodical Publishers Association told us:

> *Special mention needs to be made of the current moves in Europe to treat "cookies" as a special type of information from which consumers need protection. PPA has been lobbying with others in the European Parliament on the benefits of behavioural advertising to consumers and business in the face of threats to restrict use of cookies and particularly in relation to the European Commission's Telecommunications Package threat to treat all use of cookies as if they were personal information even when they are not.*

141. Gill Davison was concerned about the ineffectiveness of privacy policies:

> *Many companies have privacy policies that state that they share data with partner companies, and that the privacy policy of the partner company covers the data when they process it, but they don't tell you who the partner company is. The partner company may then share your details with more partner companies, and so on. It is difficult (impossible) to know which companies hold data on you, never mind if it is correct or not.*

142. Barbara Moore was concerned about website visitor tracking by the Government:

> *The Government's own websites host 3rd party scripts that are used to track visitors from one website to another and to monitor the effectiveness of advertising campaigns. The privacy policies published on the sites do not mention these 3rd party tracking scripts nor provide a means for visitors to the site to either opt in or opt out of the tracking. There is no need for any such scripts to be hosted by any website: all reporting is available from the website's server log records.*

Conclusions regarding Question 3

143. We are very impressed by the excellent work being done by CEOP in educating very large numbers of children. This is particularly notable because this programme is being operated on very tight budgets indeed.

144. The three recommendations put forward by Dr Andy Phippen and his colleagues (see paragraph #128 above) struck us as extremely sensible. We would of course like to see the media doing less scaremongering and more public education; however the other two recommendations are far more straightforward to adopt as explicit recommendations of this inquiry.

145. **We recommend that eSafety should be included in the core school curriculum, with appropriate topics being taught at Key Stages 1 through 4.**

146. **We recommend that the Government establish a national coordinating body to ensure that eSafety messages and teaching remain up-to-date.**

147. We feel that considerably more could be done to promote eSafety for the users of mobile phones that permit Internet access. As more and more children and young people use these as their way to get online, there is a much to be gained from even modest attempts to educate the about safety issues. **We recommend that network operators and retail outlets cooperate in providing point-of-sale literature on eSafety messages for mobile phones.**

148. Our conclusions on this question have thus far concentrated on the "education" strand of the responses. We now consider whether further regulation of online privacy is required.

149. We agree with the views expressed to us that what online privacy we have comes from a hodgepodge of laws and the side-effects of complex regulations, and that this is not an ideal way of providing a legal basis for privacy.

150. In 1968 a whole raft of complex laws about offences such as larceny, burglary and housebreaking were codified into a single, simple Theft Act. Just a few years ago, another intricate array of provisions covering fraud was converted into just three simple concepts in the Fraud Act 2006. The time has now come, we believe, for the Government to create an effective and easy-to-understand Privacy Act to provide the clarity, and security, that everyone needs.

151. **We recommend that the Government bring forward a Green Paper on Privacy, with a view to bringing forward a Privacy Bill in the next Parliament that sets out simply expressed, but far-reaching, protection for everyone's privacy, in both the offline and online worlds.**

Question 4: "Child Sexual Abuse Images"

152. The fourth of our questions was:

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

How child sexual abuse images are currently dealt with

153. The Internet Watch Foundation (IWF) was set up in 1996 to provide a "hotline" to receive reports of illegal material on the Internet. Although initially it was much concerned with images posted to Usenet, in recent years it has been almost solely dealing with reports of child sexual abuse images hosted on websites.

154. When the material is hosted in the UK, a "notice and take-down" scheme is operated. As ISPA told us:

> *Users can report to the IWF potentially illegal content and if identified on a UK server, it issues a notification to the relevant ISP advising that the item be removed. ISPA has made it a requirement of membership that such notifications be acted upon. These self-regulatory processes, which are widely recognised as an example of best practice, have resulted in less than 1 per cent of child abuse content being hosted in the UK since 2003.*

155. However, for the 99% of material that is not hosted in the UK, the process is different. The IWF passes a report to CEOP, who then pass it on to the relevant overseas police force. In parallel with this, if there is an equivalent hotline in the foreign country (a member of INHOPE, the international association of hotlines), then they will pass the report to the local hotline as well.

156. However, in many countries the local hotline is not able to issue "take-down" notices to ISPs, leaving that to the local police. The local police may take some time to deal with the report, and may wish to leave the material up whilst they investigate whether they can catch the criminals responsible.

157. In some cases, the local police may decide that no crime has been committed – laws vary as to the age of children who can be legally photographed, standards of indecency may be different, and computer generated images may be lawful in the jurisdiction. Hence in these cases the ISP will never be asked to remove the material.

Critiques

158. There was considerable criticism of the current arrangements, whose limitations were well-understood. BT, the first major ISP to roll out a blocking system, told us:

> *Cleanfeed-type solutions stop accidental exposure to such images but represent no obstacle to the determined criminal.*

159. And similarly, THUS said:

> *ISPs having to block or filter content will not stop the availability of the material outside the UK, nor will it stop the most determined of users from trying to access it.*

160. The Foundation for Information Policy Research (FIPR) drew our attention to an academic paper "The Impact of Incentive on Notice and Take-down" (Moore & Clayton, 2008) which studied the take-down time for various type of content. Whilst bank "phishing" websites were taken down within a few hours, child sexual abuse websites persist for a median of 288 hours and a mean of 719 hours. FIPR told us:

> *This is because the Internet Watch Foundation takes a police approach to dealing with offending websites that are overseas (as most of them are): it contacts the abuse line, or the police, in the hosting country. Many of these are ineffective. By contrast, the companies that remove phishing websites on behalf of banks are vigorous at asking foreign ISPs politely to remove offending material – which ISPs are usually happy to do.*

161. FIPR also believed that individuals and non-police organisations might assist in getting phishing websites removed, but were less likely to be involved with child sexual abuse image websites:

> *A secondary factor is that absent "necessity" the possession of child abuse images is a crime, and the police take an unduly strict view of necessity – as a consequence of which private action is excluded.*

162. The Open Rights Group was also concerned that the lists of illegal sites were created in a reactive rather than a proactive manner:

> *Our conversations with the IWF have led us to understand that their own view is that their role is limited, and the part of their role which involves 'blocking' is simply a service to users, so they do not [actively seek out] such material, which is both offensive and illegal to view.*

163. The Open Rights Group pointed out that it was often arranged that the blocking of an illegal site was made to look like a communication failure, rather than being specifically flagged to the user:

> *Recent events with the blocking of Wikipedia for an illegal child image showed weaknesses in the approach that the IWF had, as Wikipedia appears not have been fully aware of the threat of blocking initially, and unwanted confusion. A very basic step would be for ISPs to give a '403' (Forbidden) error rather than a '404' (Not found) error.*

Proposals going forward

164. There was a consensus that removal of illegal material was much to be preferred to blocking it and there were many calls for more action on an international stage. THUS's analysis was fairly typical:

> *The failings globally are the continued availability of child abuse content outside the UK. This has resulted in the UK ISP industry having to finance web blocking systems with no immediate evidence that the images are being tackled at the source.*

There does not appear to be a universal approach for the takedown of the content in some countries. The IWF have regularly reported the areas across the world where the material is hosted, yet it continues to be available. The UK government and law enforcement should be tackling the countries that are hosting the content to ensure more effective takedown mechanisms exist worldwide.

Clearly, the major problems behind the distribution of child sex abuse images are to do with international criminality, but this is not our specialism, nor that of the IWF.

165. JANET(UK) was also in favour of improvements to take-down regimes, but was also of the opinion that filtering, to prevent inadvertent access, was best done on end user machines rather than in the network:

We consider that the first priority should be to improve the removal of internationally-hosted material at source, and second that tools and advice to PC owners on using content filters should be improved. Filtering in the core network is likely to be less effective than either of these.

166. The Mobile Broadband Group (MBG) drew attention to the IWF's success in the UK:

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.

167. But they then pointed out that the IWF's current approach of notifying local hotlines of the content was in practice ineffective:

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.

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.

168. The IWF told us that they were considering changes in this area:

The 2009/10 work programme for the IWF includes consideration of whether the IWF could directly give notices to providers hosting child sexual abuse content in countries which do not have INHOPE-partner hotlines and for issuing advisory notices to international ISPs.

The scoping exercise will consider the legal risks of issuing notices in other countries, the potential impact on law enforcement activities in those countries, the impact on the complex network of relationships on which international co-operation rests, as well as the financial implications of a primarily UK-funded membership organisation carrying the costs of activity taking place outside the UK.

169. However, they told us that there were limitations to this in that:

Extending take-down procedures to INHOPE-partner countries would be contrary to the IWF's funding agreement with the EU.

and this would mean that take-down notices would not be issued to ISPs in the United States or Russia; with these countries, historically, hosting a very high proportion of all illegal websites.

170. CEOP also had a relevant view:

> *The current strategic focus is on the product (i.e. images and content) rather than behaviour. Consequently 'blocking' is a tool rather than a solution to child sexual abuse and exploitation where technology is a factor, as it does not take into account developments in how offenders use technology and the fact that websites are no longer the primary mechanism for the distribution of child abuse material.*

171. They saw the way forward as being on the international stage:

> *By shifting the focus onto behaviour, ISPs and law enforcement agencies can work together to get a better understanding of how to make the converged environment as safe as possible for children and as hostile as possible for offenders and to reduce the opportunities for offenders to misuse technology in pursuit of their deviant sexual desires.. It may be argued that there is a role for the United Nations here in establishing and agreeing international protocols and legislation on issues such as international law enforcement cooperation, blocking, notice and takedown and sanctions against international companies or countries that do not comply.*

172. CEOP also argued for take-down to be put on a statutory basis, and for reporting to be made mandatory:

> *ISPs should be obligated under legislation to report illegal and/or harmful content to the Internet Watch Foundation (IWF) and comply with notice and takedown procedures as defined by consensus agreement.*

173. Dr Andy Phippen and his colleagues had a rather different viewpoint:

> *Our research with young people suggests that they are far more likely to be a victim of cyber bullying or "sexting" than stalking and grooming. In some recent research, 75% of schools surveyed reported incidents of cyberbullying and our discussions with young people show this is a serious, yet common, problem with little control or protection from technology providers.*

174. They saw a bigger role for telecommunications providers:

> *ISPs and mobile telcos have a responsibility to act on these less high profile threats which have potentially devastating effects on their victims. At present, providers will tend to absolve themselves of accountability by being perceived merely as technology providers, with no control over the content distributed by their infrastructure. However, given that providers have full details of their consumers (such as age), we would suggest that it is entirely possible for them to provide tighter controls on issues such as bullying via SMS, peer to peer distribution of personal images, etc. yet without tighter control, they will not accept responsibility.*

175. Although we agree with Dr Phippen and his colleagues about the importance of cyber bullying, we regretfully feel that it is outside the scope of this inquiry, and so we have not received all that much evidence on the topic. For that reason, although this is a big problem which we would wish to see progress in tackling, we will not make any recommendations on this occasion.

Conclusions regarding Question 4

176. It seems quite clear from the evidence that we received that a great deal more could be done to promptly request ISPs to remove child sexual abuse image websites. The IWF are clearly doing a good job along these lines within the UK, but they tell us that they are unable to extend this activity to key countries such as the US and Russia.

177. In our view, this is an unacceptable situation. If the IWF are unable to perform this important function on a global basis, then some other organisation will need to be given the task. Although there is no particular reason why such a global body should be UK

based, the long history of leadership in this area makes the UK a natural candidate to develop a new approach.

178. **We recommend that the Government, in consultation with the EU Commission, establish whether the Internet Watch Foundation (IWF) should extend its "notice and take-down" mechanisms to the whole world, and if not, work to establish such a global system.**

Question 5: "Network Neutrality"

179. The fifth and last of our questions was:

> 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?

180. Several respondents explained to us, in greater or lesser detail how Internet traffic is currently paid for. For example Skype said:

> *Network operators build and manage the infrastructure necessary to transmit Internet traffic in return for consumer subscriptions to Internet access.*
>
> *Internet content and applications providers invest in innovating and developing these content and applications in return for consumers paying directly or indirectly (e.g. through advertising) for them.*
>
> *Consumers pay for Internet access not because they want to possess a cable or satellite dish or mobile broadband dongle, but because of what they can do with it, what online content, services and applications they can enjoy and benefit from.*

adding:

> *This is a virtuous cycle where all in the Internet value chain can benefit, including consumers. It is high time that it be recognized by the market, and in regulation, so that no actor in the ICT sector can abuse its control over a particular layer of the value chain.*

181. However, this explanation isn't quite sufficient, in that the content providers also need to pay for their connection to the Internet. As the Periodical Publishers Association pointed out:

> *Internet traffic is paid for by those that produce or supply the content by way of both hosting and internet access fees paid to their respective ISP. There are well established means for ISPs to exchange traffic and receive balancing compensation. ISPs receive internet access payments from consumers and businesses who receive and send content usually based on amount of bandwidth made available and totally neutral to the source of content.*

182. At present the expectation is that once a content provider has paid for their Internet connectivity, then their website can be reached by anyone who wishes. Some people believe that this should change, and content providers should also pay something to not only their own network provider, but also to recompense any other networks who carry their traffic.

183. TalkTalk helpfully explained the possibility of different payment models by reference to the television industry:

> *For instance: in the UK cable industry Virgin Media typically pays the TV channels; in Germany, the channels pay the networks for access; in Japan many mobile services are delivered via an iMode model where the content providers bill customers and pay a revenue share to the networks.*

These different models (and there are many others) have each developed through innovation and commercial negotiation to reflect the different dynamics in each market. Content providers and access providers are free to innovate and commercially negotiate terms about who pays that work for both sides. If the businesses don't like the terms they can decline or go elsewhere. If consumers do not like the available content they can change access provider and/or content provider. Through market forces effective and efficient outcomes are delivered for consumers.

184. TalkTalk went on to argue, as did a number of other respondents, that the correct thing to do was to "leave it to the market". However, they did recognise the possibility of market failure:

We do recognise though that there may be certain limited circumstances where the market may fail to deliver and some form of intervention would be appropriate. The main ones are: where a content provider or an ISP has a 'dominant' market position; where there are barriers to switching or lack of transparency; or, where certain essential content may become unavailable.

However, we do not believe that these circumstances exist in the UK communications market today – we have a very competitive ISP and content market, good transparency and ease of migration for consumers, and there is no 'must have' content that is not available through other channels. Furthermore, if any problems did arise we they could be adequately be handled by existing competition and consumer protection regulation.

185. This is essentially the position set out by Ofcom and incorporated in the Digital Britain report – that in the UK there was sufficient competition to ensure that the market would produce the best solution.

186. The Open Rights Group understood this argument but were sceptical:

The EU proposals seem to expect ISPs to be prevented from acting anticompetitively by competition law. This is however in general a long process to use, and in general, it seems that by the time that competition law is enforced, the damage has already been done.

187. Ofcom were reassuring:

We believe that Ofcom currently has sufficient powers to investigate allegations of anti-competitive practices. Effective competition, combined with incentives to promote service transparency and low barriers to consumer switching provides the best balance between rewarding efficient investment, innovation and consumer protection.

188. But the Foundation for Information Policy Research sounded a note of caution:

The question of who should pay for Internet traffic is an old one, and well studied by network economists (such as Odlyzko). The combination of high fixed costs and low marginal costs can make it difficult for communications service providers to recover infrastructure costs if exposed to unlimited price competition. Regulation is thus inevitable and the framework that has emerged in the UK is by no means the worst. But the issues are often thought "too technical" by legislators.

189. In the United States, there is considerably less competition between broadband suppliers than in the UK, and this has led to many calls for "network neutrality". This term has a myriad of meanings, but BT had a stab at defining it for us:

Network neutrality is a concept gaining increasing pace in the US. There is a view that network providers should not prioritise or "size" the types of traffic it delivers over its network and should ensure the network capacity is sufficient to ensure that users can access the capacity they need for the purpose they require it.

190. BT saw it as obvious that content should be carried on "fair and equal terms" but stressed:

> *Network owners should be able to offer and charge for additional capabilities to enable differentiated service levels (such as guaranteed quality of service, dedicated speeds, etc)*

191. Virgin Media was also thinking about different levels of service in the future:

> *In the future, as data demands increase, it is inevitable that ISPs will be forced to make choices on behalf of their customers as to the relative priority of traffic. Given the scale of growth in data and bandwidth consumption and the potential for this to degrade customer experience, it is also logical that network providers and content providers will look at new ways of working together, forging new partnerships to deliver content to consumers; examining the possible development of business models that offer new forms of delivery.*
>
> *Critically, however, it is important that any decisions are made in a transparent fashion. While we recognise the commercial advantages that managing access in this way could bring, we are equally conscious of the need to support the principle that the internet should remain a space that is open to all.*

192. The Mobile Broadband Group said:

> *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.*
>
> *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.*

193. The Internet Service Providers Association UK (ISPA) stressed the need for transparency:

> *When consumers have meaningful information about the nature of their broadband services and the practices of their providers, in a competitive market, they will choose the models that succeed for them in the marketplace according to their own needs and budget. ISPA recommends transparency about how its members manage their network. ISPA advises its members to make clear information available to its customers and users on the nature of any traffic management or filtering that takes place. ISPA has a Best Practice Document on filtering and blocking of Internet traffic, which states that members should "make available to its customers and users in a clear manner the nature of the filtering that takes place".*

194. Ofcom assured us that this should already be occurring:

> *Ofcom's Broadband Speeds Code of Practice will support and enable transparency: it requires ISPs who do not provide the same quality of service to all internet applications to tell their customers that this is the case. Specifically, the Code states: "where ISPs apply traffic management and shaping policies, they should publish on their website, in a clear and easily accessible form, information on the restrictions applied. This should include the types of applications, services and protocols that are affected and specific information on peak traffic periods." The Code has been signed-up to by the majority of ISPs covering more than 90% of UK consumers.*

195. Many of individual responders and NGOs felt that what was necessary was to incorporate some notion of network neutrality in statute. Neil Maybin recommended:

> *The basic principles of Network Neutrality should be enshrined in statute. This would best protect the interests of all parties involved – Websites, Internet Service Providers and Users – and of society overall.*

196. The Communication & Media Research Institute at the University of Westminster said:

> *We believe that network neutrality should be enshrined in statute with a specific reference to abuse of market power. Effectively, the absence of network neutrality is about a provider with significant market power in the broadband access market leveraging power in the neighbouring markets for the provision of content, services, and applications. Whilst competition authorities have a role, we believe that the ex-post character of such interventions may adversely impact upon the market and we are therefore in favour of the network neutrality principle to be enshrined in statute in order that the sectoral regulator Ofcom would be empowered to intervene if and as needed in a timely manner.*

197. They were joined by content providers such as the Periodical Publishers Association (PPA):

> *PPA believes that Net Neutrality is crucial for a fair and level playing field to ensure universal access to information and that government should ensure that Net Neutrality is protected and that a content access class system does not develop. This requires legislation.*
>
> *Without a legal requirement for Net Neutrality, network operators, particularly at the delivery end of the network, will be free to accept payments to give priority to some content over other content, or to slow down or not allow delivery of content for which payment has not been made creating a digital content delivery (and possibly access) class system with increasing prices to consumers. It could also distort and/or limit availability of content. PPA is not suggesting that non-discriminatory traffic management should be prohibited (i.e. where the type and source of content is neutral but the size and timing is the determining factor).*

198. And also by Skype:

> *Abuses such as the undue blocking and degradation of traffic already take place in the current market environment. It will be important to acknowledge the potential for future market structures to incentivise discriminatory behaviour, particularly the abuse of bottleneck control over users' Internet access. It would therefore be appropriate to introduce specific safeguards to ensure openness and transparency.*

who had three specific policy objectives:

> *Enshrining in UK law a presumption of end-to-end connectivity and open access which consumers have come to associate with the Internet;*
>
> *Clarify that traffic management, where it is necessary to manage congestion and is essential to providing a broadband service to end users, is reasonable, justified and transparent to all parties (both end users and those parties whose traffic is being managed);*
>
> *Ensure that the regulators have the legal powers and access to evidence that they require to investigate claims that traffic management is unfair or anti-competitive and to give the timely remedies that are essential to support a fast-moving online market.*

199. Conversely, all of the ISPs and network operators felt that regulating for network neutrality would be a disaster. AT&T put it extremely clearly:

> *There is no market failure that warrants a regulatory intervention in the Internet that would affect the management or pricing of network offerings, whether denominated as "net neutrality" or otherwise. To the contrary, the downside risk of such intervention would be enormous. We should not put investment and affordability at such profound risk by barring network management tools before even seeing their effect in operation or by barring new and creative commercial arrangements before even knowing what these arrangements might be or how they might operate in practice. Governments should continue to allow market forces to do what they have been doing exceedingly well in this industry.*

200. A number of people favourably mentioned what had happened in Norway where a document setting out what was meant by "network neutrality" had been voluntarily adopted by their ISP industry. The Open Rights Group was in favour of this type of approach:

> *Government could encourage ISPs to reassure the public about competition and access concerns by adopting a voluntary agreement. If no such agreement is forthcoming, this may indicate that concerns have more of a possible basis than is currently admitted.*

201. Some respondents saw network neutrality in term of ISP "traffic shaping" (such as the artificial discouragement of peer-to-peer file sharing traffic). The ISPs explained that this approach was necessary in order to maintain a quality of service. For example Virgin Media told us:

> *The architecture of residential broadband networks means that bandwidth capacity is shared among multiple users, meaning that even the most sophisticated networks can get congested at busy times of day. Without proactive management of this traffic by service providers, for example by prioritizing particularly time-sensitive applications such as video-streaming, the performance of an individual customer's broadband can deteriorate significantly.*
>
> *In that sense, we do not believe that there is a credible argument for pure "net neutrality"; in practice, networks will have to prioritise traffic, but by default rather than by design.*

202. The Communication & Media Research Institute explained the law to us:

> *The current legal position is that the prioritisation of content, or discrimination against it (blocking) is neither permitted nor forbidden. The law says nothing about it, because when the current EU framework was drafted in 2002, such practices were not really possible. Now, with new technology known as traffic management systems, broadband providers may selectively block traffic. The Telecoms Package does not change this situation, but it does legitimise it. It says that blocking is fine as long as the operator says so, somewhere in the contract. That is very low legal barrier.*

203. However many people saw traffic shaping as being entirely a matter of ISP network capacity. BBBritain said:

> *Measures to control congestion should not require an ISP to look inside our packets, but the ISP should inform the customer of their peak hour capacity […] ISPs should also make users aware how busy their network is, so they can schedule downloads in off peak periods.*

and Neil Maybin told us:

> *Claims of network speeds are made which are often undeliverable at peak times. Because of a failure to regulate this, no major Internet Service Provider has yet had*

the courage to be first in offering an accurate specification of what consumers will actually experience. Consequently some Internet Service Providers feel the need to inspect data in messages in order to decide how best to prioritise network traffic.

204. Barbara Moore suggested this was a quality issue and suggested a system of fines for overselling available bandwidth:

Net neutrality issues are only a problem when the low quality ISPs oversell and then try to avoid incurring the expense of investing in infrastructure or buying more bandwidth as their customer demands increase.

The quality ISPs currently offer bandwidth packages ranging from pay-as-you-go and from 1 Gb to over 200 Gb per month with excess charge packages if users go over their contractual limits. Overselling is rare with networks having redundant capacity to enable re-routing in the event of congestion or failure in one part of the network.

Mobile phone filtering

205. The whole network neutrality debate can be seen in miniature by looking at Internet access by mobile phones. The Communication & Media Research Institute told us:

Current examples of discriminatory practice are the widely publicised case of T-Mobile blocking Skype on wireless access (note that wireless access from a laptop computer could be a user's main form of Internet access).

206. However, it's not quite as straightforward as the Institute makes out. T-Mobile addressed this issue in their written evidence:

To ensure all customers have the ability to access the Internet equally with no capacity problems, T-Mobile has, for example, consistently and transparently restricted the use of VoIP on many of its tariffs whilst permitting it on one specified tariff and making this information clear in the terms and conditions of each tariff.

207. Although some respondents indicated that in their opinion, this blocking was being done for revenue protection reasons (Skype calls could be much cheaper than using the mobile phone for a normal voice call), T-Mobile told us that was not the reason for their blocking:

Mobile networks have not been designed for "always on" applications like the use of VoIP clients. Thus, we need to be aware of the capacity constraints of our networks regarding the number of users that are "always on". If too many VoIP users are "always on" this will prevent additional users from connecting to our network and thus cut them off from our services entirely.

208. Since other mobile providers permit Skype, indeed one makes a point of its support for Skype in their advertising – it might well be argued that there is not a network neutrality problem of any note here, and the market will determine if T-Mobile needs to redesign their tariffs (or rebuild their networks to support more "always on" clients).

209. The mobile networks also do a fair amount of content filtering to protect children. The Mobile Broadband Group told us that adult content they (or a commercial partner) provided would not be made available "until a customer has demonstrated, through robust age verification, that he or she is at least 18 years old".

210. However, the MBG continued:

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.

211. These differences in approach could be seen in the evidence. For example, T-Mobile told us that the child protection filter was initially set as "on" for all devices including mobile phones, PDAs, Blackberrys and dongles. Whereas their rival 3 told us:

The internet filter is applied as a default for handset customers as currently there is no software that customers can install on their handset to personalise and control their internet access. However, users of mobile broadband internet access – where customers use a 3G modem connected to their PC or laptop – are able to install software or personalise the settings on their internet browser so as to control spam, viruses and apply appropriate restrictions to protect themselves or members of their family.

3 do not believe it is appropriate to seek to apply network level controls on the content which mobile broadband customers may wish to view.

Conclusions regarding Question 5

212. From the evidence we have received we are persuaded that in the UK, at present, "network neutrality" is being delivered by market mechanisms. However, we also believe that the evidence shows that this situation could change. Therefore, **we recommend that Ofcom keep the issue of "network neutrality" under review and include a section in each annual report that indicates whether there are any signs of change.**

213. It is clear from the evidence to this inquiry, from our postbags, and also from our personal experience, that many people are dissatisfied with the speed of their broadband connections. We are unimpressed by the current approach of advertising a maximum speed, which few if any customers will actually achieve.

214. Although we recognise that speeds can be affected by many different variables, we do not consider the current method of advertising broadband speeds to be acceptable. We also believe that ISPs could do more to help consumers with speed problems to address these issues, from improving the phone wiring within their houses, to selecting appropriate ADSL modems. To that end, we believe that the way forward is to promote competition between ISPs on more than just price. Hence **we recommend that Ofcom regulate to require ISPs to advertise a minimum guaranteed speed for broadband connections.**

215. Finally, we are concerned to discover the differences between the default settings for child protection filters on different mobile devices from different companies. This is unnecessarily confusing for parents and quite obviously a consistent approach should be adopted by the whole industry. **We recommend that for reasons of clarity, Ofcom ensure that child protection filters should be enabled by default for every type of mobile Internet access device, whether they be handsets or "dongles".**

Summary of Recommendations

51. We recommend that UK ISPs, through Ofcom, ISPA or another appropriate organisation, immediately start the process of agreeing a voluntary code for detection of, and effective dealing with, malware infected machines in the UK.

52. If this voluntary approach fails to yield results in a timely manner, then we further recommend that Ofcom unilaterally create such a code, and impose it upon the UK ISP industry on a statutory basis.

54. We recommend that the Government revise the law to enable ISPs to take proactive steps to detect and remove inappropriate content from their services, without completely losing important legal immunities which fit with their third party role in hosting and distributing content.

55. We recommend that the Government does not legislate to enforce the deployment of blocking systems based on the IWF lists. This has the potential to damage future attempts to fix problems through self-regulation, and will thus, in the long term, be counterproductive.

58. We conclude that much of the problem with illegal sharing of copyrighted material has been caused by the rightsholders, and the music industry in particular, being far too slow in getting their act together and making popular legal alternatives available.

59. We do not believe that disconnecting end users is in the slightest bit consistent with policies that attempt to promote eGovernment, and we recommend that this approach to dealing with illegal file-sharing should not be further considered.

60. We think that it is inappropriate to make policy choices in the UK when policy options are still to be agreed by the EU Commission and EU Parliament in their negotiations over the "Telecoms Package". We recommend that the Government terminate their current policy-making process, and restart it with a new consultation once the EU has made its decisions.

117. We recommend that the Government review the existing legislation applying to behavioural advertising, and bring forward new rules as needed, to ensure that these systems are only operated on an explicit, informed, opt-in basis.

118. We recommend the UK Council for Child Internet Safety (UKCCIS) consider how behavioural advertising that is aimed at children and young people should be regulated.

145. We recommend that eSafety should be included in the core school curriculum, with appropriate topics being taught at Key Stages 1 through 4.

146. We recommend that the Government establish a national coordinating body to ensure that eSafety messages and teaching remain up-to-date.

147. We recommend that network operators and retail outlets cooperate in providing point-of-sale literature on eSafety messages for mobile phones.

151. We recommend that the Government bring forward a Green Paper on Privacy, with a view to bringing forward a Privacy Bill in the next Parliament that sets out simply expressed, but far-reaching, protection for everyone's privacy, in both the offline and online worlds.

178. We recommend that the Government, in consultation with the EU Commission, establish whether the Internet Watch Foundation (IWF) should extend its "notice and take-down" mechanisms to the whole world, and if not, work to establish such a global system.

212. We recommend that Ofcom keep the issue of "network neutrality" under review and include a section in each annual report that indicates whether there are any signs of change.

214. We recommend that Ofcom regulate to require ISPs to advertise a minimum guaranteed speed for broadband connections.

215. We recommend that for reasons of clarity, Ofcom ensure that child protection filters should be enabled by default for every type of mobile Internet access device, whether they be handsets or "dongles".

Appendix A: Press Notice & Guidelines for Witnesses

22nd April 2009

For immediate release

Press Release – apComms, the All Party Parliamentary Group on Communications, chaired by John Robertson MP and Derek Wyatt MP, is launching an inquiry into Internet traffic to assess regulation of ISPs and a range of Internet traffic issues from behavioural advertising and privacy to child abuse images and Internet neutrality to answer what role Government should play when it comes to Internet traffic.

Submissions are invited on 5 questions (see below) by 22nd May and evidence sessions will be held in Parliament in June, with the final report expected in the Autumn.

Background

Internet Service Providers (ISPs) currently have almost no legal liability for the traffic that passes across their networks this having been seen to be the correct public policy response to their very limited knowledge of what their customers are actually doing.

Recent technical advances are beginning to make it practical to inspect Internet traffic – "bad" traffic might then be blocked; "bulk" traffic might then be slowed; "wicked" traffic detected and crimes investigated; or personal profiles could be built to better target advertising.

Opinions differ very widely as to which of these activities should be forbidden, which should be insisted upon, which raise insurmountable privacy issues, and which should be left to the marketplace to determine whether the idea is viable.

Existing European legislation provides ISPs with some key immunities for "mere conduit" along with protections for "hosting" and "caching". Almost a decade after they were decided upon, are these immunities still appropriate? Should they be recast to reflect the way in which modern networks operate?

Now the Internet is part of daily life, concerns are increasingly raised about a wide range of online privacy issues. Should there be changes to individual behaviour? Should companies be pressed to prioritise privacy issues? Or is there a need for specific regulations that go beyond mere "data protection" and address privacy directly?

Some have argued that ISPs should be forced to take considerably more responsibility for the traffic on their networks, preventing email spam, disabling "botnets", blocking access to websites containing child sexual abuse images and other types of illegal material. Others believe that ISPs should be preventing file sharing, so that their customers cannot infringe copyright laws.

Are any of these arguments valid? Or are there better ways of tackling these problems, especially at the global level? More locally, are the problems being properly addressed by the UK Government, or is there a need to reassign ministerial responsibilities for online matters?
In the United States many of these issues are caught up in the debate about "Network Neutrality", a term with a plethora of meanings, which often comes down to a dispute about

who should meet the costs of Internet traffic. The draft Digital Britain report dismisses the issue by pointing to the competitive nature of the UK market, but others dispute this analysis and argue for legislation to prevent companies from abusing their position. What aspects of network neutrality actually matter in the UK? and do consumers need new laws to protect them?

Inquiry questions

Although we intend to address the broad sweep of all of these topics and make a range of recommendations; we would particularly like to learn how these five specific questions should be answered:

> #1 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?
>
> #2 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?
>
> #3 Is there a need for new initiatives to deal with online privacy, and if so, what should be done?
>
> #4 Is the current global approach to dealing with child sexual abuse images working effectively? If not, then how should it be improved?
>
> #5 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?

Guidelines for responses:

- Written submissions should be concise and address the matters raised by the inquiry. An effective response is unlikely to exceed 4 pages.
- Please do not attempt to address all possible aspects of the inquiry, or to answer all of the questions posed. Instead, focus your response on the matters on which you have particular expertise or particularly strong opinions.
- Submissions should be submitted by email either in plain text (ASCII), PDF, .DOC or .RTF format. Submissions should be dated and should include the name, address, email and telephone contact details of the individual submitter, or the person within an organisation who should be contacted.
- Submissions and any other enquiries should be sent to: admin@apcomms.org.uk
- It is at the inquiry's discretion to publish any evidence it receives. Evidence will be attributed to individuals or organisations, but detailed contact information will be not be made public. Any other information that a witness would not wish to be considered for publication should be clearly marked.
- The inquiry would like all evidence to be submitted by 22nd May 2009. Following consideration of the written evidence, the Officers of apComms will decide which organisations and individuals to invite to oral evidence sessions in Westminster on 15th and 17th June 2009.
- The inquiry is expecting to publish their final report in the Autumn.

Appendix B: Glossary of Terms

ADSL
Asymmetric digital subscriber line. One of the technologies used for broadband access to the Internet.

botnet
Network of compromised machines being used for criminal purposes.

BPI
British Recorded Music Industry (once “Phonographic”)
http://www.bpi.co.uk

BSG
Broadband Stakeholder Group
http://www.broadbanduk.org

CEOP
Child Exploitation and Online Protection Centre
http://www.ceop.gov.uk

cookie
Text file created by a website and stored on a visiting machine to be resupplied back to the website at the next visit.

dongle
Small hardware device used with laptop or desktop computers to permit use of mobile phone protocols to access the Internet.

DPI
Deep packet inspection. Examining packet content within the core of the network.

EU
European Union

FIPR
Foundation for Information Policy Research
http://www.fipr.org

GSMA
GSM (Groupe Speciale Mobile) Association
http://www.gsmworld.com

IAB
Internet Advertising Bureau
http://www.iabuk.net

ICO
Office of the Information Commissioner
http://www.ico.gov.uk

INHOPE
International Association of Internet Hotlines
http://www.inhope.org

IP
Internet protocol

IP
Intellectual property

ISP
Internet Service Provider

ISPA
Internet Service Providers Association UK
http://www.ispa.org.uk/

IT
Information Technology

IWF
: Internet Watch Foundation
http://www.iwf.org.uk

LEA
: Law enforcement agency

malware
: Malicious software. Sometimes distinguished as a worm, virus or trojan.

MBG
: Mobile Broadband Group
http://www.mobilebroadbandgroup.com/

NGO
: Non-governmental organisation.

ORG
: Open Rights Group
http://www.openrightsgroup.org

PC
: Personal computer

PPA
: Periodical Publishers Association
http://www.ppa.co.uk

RIPA
: Regulation of Investigatory Powers Act 2000

rightsholder
: Owner of intellectual property, usually in the entertainment industries.

SMS
: Short message service. A text message on a mobile phone.

spam
: Bulk unsolicited email.

UK
: United Kingdom

UKCCIS
: UK Council for Child Internet Safety
http://www.dcsf.gov.uk/ukccis/

URL
: Universal resource locator. Address of a world-wide-web item.

US
: United States of America

Appendix C: Bibliography

Oral evidence URLs

http://www.apcomms.org.uk/uploads/090706_apComms_Oral_Evidence1.doc
http://www.apcomms.org.uk/uploads/090707_apComms_Oral_Evidence2.doc
http://www.apcomms.org.uk/uploads/090707_apComms_Oral_Evidence3.doc

Documents mentioned in this report

Ross Anderson, Rainer Bohme, Richard Clayton and Tyler Moore: *Security Economics and the Internal Market.* ENISA, 31 January 2008.
http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport

Internet Advertising Bureau: *Good Practice Principles for Online Behavioural Advertising*. March 2009
http://youronlinechoices.co.uk/wp-content/uploads/2009/09/IAB-Good-Practice-Principles-for-Online-Behavioural-Advertising.pdf

Tyler Moore and Richard Clayton: *The Impact of Incentives on Notice and Take-down.* Seventh Annual Workshop on Economics and Information Security (WEIS08), Dartmouth NH, USA, June 25–28 2008. In: M. Eric Johnson, editor: *Managing Information Risk and the Economics of Security*, pages 119–223, Springer, New York, 2008.
http://www.cl.cam.ac.uk/~rnc1/takedown.pdf

Internet Industry Association: *Internet Service Providers Voluntary Code of Practice for Industry Self-regulation in the Area of e-Security.* Consultation Version 1.0, September 2009.
http://iia.net.au/images/resources/pdf/esecurity_code_consultation_version.pdf

Norwegian Post and Telecommunications Authority: *Network neutrality Guidelines for Internet neutrality.* Version 1.0, 24 February 2009.
http://www.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf

Previous inquiries by APIG (a forerunner of apComms):

Report of an Inquiry on 'Digital Rights Management', June 2006
http://www.apcomms.org.uk/apig/current-activities/apig-inquiry-into-digital-rights-management/DRMreport.pdf

Report of an Inquiry on 'Revision of the Computer Misuse Act', June 2004
http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry/CMAReportFinalVersion1.pdf

Report of an Inquiry on 'Spam', October 2003
http://www.apcomms.org.uk/apig/archive/activities-2003/spam-public-enquiry/spam_report.pdf

Report of an Inquiry on 'Communications Data', January 2003
http://www.apcomms.org.uk/apig/archive/activities-2002/data-retention-inquiry/APIGreport.pdf


apComms