Can we keep our hands off the net?

Response of the Open Rights Group

Detail of Respondents

Prepared by:	Jim Killock
Responding on behalf of:	The Open Rights Group
Date	21 May 2009
Address:	Open Rights Group 7th Floor 100 Grays Inn Road London WC1X 8TY United Kingdom
Telephone:	+44 (0)20 7096 1079
Email:	info@openrightsgroup.org
Website:	http://www.openrightsgroup.org

About the Open Rights Group

The Open Rights Group is a grassroots digital rights advocacy group based in the UK. It aims to increase awareness of digital rights issues, help foster grassroots activity and preserve civil liberties in the digital age. It is funded by individual donations and small grants.

Preamble

The questions below are all in various ways affected by the emerging technologies including 'Deep Packet Inspection', which allow Internet Service Providers to take a look at the whole content of the 'packets' of information that travel on their networks.

Up until recently, this detailed look at traffic has not been possible, but increasing computer processing power means it can now take place. The uses are sometimes benign, like 'traffic management' policies, but can also be as malign as the censorship technologies dependent on DPI used in China.

DPI and other technologies are therefore driving changes on the internet but governments' task is to settle the principles by which use of technologies should be judged. As campaigners, we wish to advocate approaches to you that will make sure that citizens' interests are paramount. This includes getting the best out of commercial actors.

#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?

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.

For instance, a user may choose to transfer their legally bought tracks to another machine, or perhaps may obtain a copy of a track from a friend because their copy has in some way been damaged. These examples may be infringement, or may not, but the judgement is a matter of understanding the license, rather than detecting the material.

Assuming that the legal process is fair, takedown as a method for dealing with copyright infringement seems preferable to network blocking or filtering, but neither approach seeks to address the underlying behaviour. In the end, illicit file sharers must be persuaded that there are better ways to get the material they seek: through better services from licensed sites.

For copyright licensed services to work well, they need to take account of the new benefits of internet markets, which include: instant access; a near zero marginal cost of copying and distribution; user participation; user generated content; social recommendation. The best answers are in new business models, like Spotify, rather than stricter enforcement. Strict or unfair enforcement also risks undermine copyright's reputation.

#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?

We need first to separate behavioural advertising from the underlying principle of consent and the enforcement of data protection and intercept laws. The issues as we understand them include:

1. The nature of 'personal information': browsing habits, that can be linked back to the user via a cookie or user ID, is personal information, and should therefore require the informed consent of the user. However, partly because UK data protection law has narrowed the definition of personal information from the EU Directive's intention, this is not enforced. **Government should act to make sure that UK data protection law is in line with EU law, and 'personal information' is information that can be linked to an individual.**

2. 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. For instance, if you switch browser, change user account, wipe your hard disk, delete your cookies, then all knowledge of your 'opt out' is lost and you have to make the choice again. This means 'opting out' requires persistence from users.

   Similarly, because of the nature of cookies being tied to a browser, rather always to a person, opting in or out of having information profiled may not be a true indication of a user's preference.

   Government should make it legally clear that user choices should persist

3. 'Opting in' should happen without duress. **Data sharing or profiling should not be mandatory in order to take up a commercial service.**

4. There are weaknesses in data protection enforcement in the UK. **Privacy rights, such as data protection breaches, should be enforceable by individuals in UK courts.**

5. **The ICO should have powers to spot check private companies, and fines to data protection breaches should be in proportion to company turnover.**

6. Some models of behavioural advertising involve interception of traffic. Phorm is a specific example of this. In this model, data from users and services that have no knowledge of Phorm will be intercepted and read. This is because a Phorm-based

customer may communicate with users on other networks, for instance abroad. This undermines the principle of consent in interception of communications. There is a misconception that communications on the internet may be intercepted, because material is available of the net, and therefore are providing 'implied consent'. This is a misunderstanding of the relationship a user has with a service and users on another website. Websites make different information available according to the user or users. There are long term dangers in ignoring this problem and undermining the principle of consent.

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.

7. 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 non-governmental interceptions. The activities of the Interception of Communications Commissioner must also be properly resourced and open to much greater public scrutiny.

The government can legitimately encourage new advertising if it wishes, but its first role is to enforce the legal framework. There are clearly significant issues with raising revenues on the net, but these are separate to basic legal enforcement of fundamental human rights.

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

We take it as read that privacy is important as a protector of people's identity and freedom of expression, and is recognised in law as a fundamental human right. We also assume that in asking this question, there is an understanding that there are threats to privacy that come from the persistence of data and the increasing ease by which it can be found and analysed.

There are however a number of changes in policy which would help protect privacy. Firstly,

1. The government should educate itself by improving its technical understanding. Privacy Officers should be hired within all government departments and technically

able staff to help them. This is also important for the ICO, who are still debating what technically help they wish to hire. We believe in-house computer science specialists are needed.

2. Procurement policies for government services should take a much higher regard for both security concerns, and privacy concerns. In computer networks, privacy relies on the underlying security, as well as good privacy design. No procurement should take place without a Privacy Impact Assessment.

3. The government should work internationally to promote much more comprehensible standardised privacy agreements, for voluntary use. This would help users understand what they are agreeing to, for instance, by seeing a set of standardised icons.

4. Government itself needs to scale back its own schemes for data retention and online 'black box' surveillance which themselves are undermining privacy rights.

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

The domestic part of this we know best, where takedown notices from the IWF have all but eliminated the problem of hosting within the UK. However, 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 find such material, which is both offensive and illegal to view.

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. We understand the IWF are looking at this with their ISP partners. We also understand that the IWF are reviewing some of their procedures around takedowns. Allowing more flexibility for contextual issues would be helpful, so an individual case does not have wide repercussions (we note that the image on Wikipedia was also available on Google image search and several Amazon sites, so was not an isolated case). Certainly, the case brought unwanted criticism of the IWF. The case also highlights the risks of backlash from any wider 'blocking' policies where the public feels 'censorship' may be taking place.

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.

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.

#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?

The basic premise of the experience most users expect is that they have full and unrestricted access to all services on the net, and they are paying for it. Furthermore, customers are benefiting from the competition that results from an open network, as services are simply set up, without worrying that they may be barred. This is not to underestimate the negotiation which takes place between content and internet service providers to pay for the delivery of content in practice.

Clearly, there are potential competition issues as content companies such as Sky and Virgin also enter the broadband market. There are also potential conflicts between internet telephony providers, and traditional telecoms operators.

Recognising this, Norwegian telecoms operators recently signed a voluntary 'net neutrality' agreement that stated that:

1. Internet users are entitled to an Internet connection with a predefined capacity and quality.

2. Internet users are entitled to an Internet connection that enables them to

    - send and receive content of their choice
    - use services and run applications of their choice
    - connect hardware and use software of their choice that do not harm the network.

3. Internet users are entitled to an Internet connection that is free of discrimination with regard to type of application, service or content or based on sender or receiver address.

(See http://is.gd/C1k5)

These are a good model, and 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.

On mobile internet, restrictions on internet usage are commonplace. VOIP applications in

particular are frequently prevented from functioning fully. Phones are prevented from being used to 'pipe' internet services to another machine owned by the user. Mobile companies do not seem see themselves as merely supplying data over a connection for a price, but seem to expect to provide the specific services. They are therefore in effect acting anti-competitively.

Mobile internet usage is in need of being opened up, but also offers an example of what can happen to the internet if openness is not seen as an important element of the service offered. So far, competition has provided some protection to domestic users, but parts of the proposed European Telecoms Package seem to be enshrining in law the right to discriminate in favour or against certain types of traffic. This would be a very bad step if not balanced by provisions to ensure this is done within the context of traffic management and good service provision. Unfortunately, the EU debate seems to have been driven by large ISPs at the expense of advice from content providers, such as Yahoo, Skype and Google, and consumer groups including BEUC.

The EU proposals seem to expect ISPs to be prevented from acting anti-competitively 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.

Action at UK level may therefore be difficult if the EU Telecoms Package is not correctly shaped. UK Parliamentarians should work with EU colleagues to ensure the best results for consumers, and to promote innovative new uses of technology .