Date 18th May 2009

Name Peter W

Address

Contact

Response to the questions from the

All-Party Parliamentary Group on Communication's inquiry into online privacy.

Q1 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?

There is no easy way to define bad traffic, as it is subjective based on your use of the internet

Spam and viruses would obviously fall into the category of bad traffic but there is no easy way to block all spam or viruses on a reliable basis during their transit through the ISP networks

Using DPI equipment to manage bandwidth can enable the ISP to mask lack of investment in the core infrastructure if used long term, as it enables them to measure and cap user's internet access based on the web usage and programs they use

This can lead to anti competitive practices if used to limit bandwidth of a competitors competing service offering like VoIP, IPTV etc. As very often the fair use policies say that caps will not apply if the customer accesses their own ISP's service (for instance the ISP's own IPTV offering instead of using an external source such as BBC iPlayer)

The other way ISP's try and justify the use of DPI type technology is to control peer to peer networks, peer to peer networks are not illegal but can be used to share copyright material in an illegal way, very much the same as a car is not illegal, but can be used for illegal activity (speeding, transporting illegal goods etc)

Q2 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?

It should be noted there are currently two types of behavioural based advertising

1. Site based advertising systems, like Amazon and Google, this only uses data collected from websites within the advertising network by using small files called cookies, small computer programs called scripts which run inside the users web browser and data of what the user has view on those site. All sites in the advertising network have "OPTED-IN" by hosting the scripts and cookies and providing the user information whilst on the website

2. Interception / DPI based advertising systems, like Phorm's WebWise product intercept the unencrypted private communications between the ISP's customer and the website they are viewing to provide behaviour data to Phorm's OIX advertising network. This interception takes place regardless of whether the website the ISP's customer is viewing regardless of whether it has OPTED-IN to the OIX advertising network. If the website is not part of Phorm's OIX network no attempt is made to get permission to use the websites content for Phorm's commercial gain to provide advertising to the websites potential competitors using it's own data against it to target it's visitors

Site based advertising appears to comply with all current legislation as so long as users are informed and opt-in.

Interception / DPI based advertising where it does not get specific opt-in or informed consent from both sides of the private communication (ISP customer and website) appears to be in breach of several pieces of current legislation

(DPA, PECR, copyright and designs patents act, and RIPA 2000, and others) and many people are concerned that these pieces of current legislation have not been brought enforced

Yes, the government should intervene where the behavioural advertising service breaks any legislation. It should uphold current UK and EU legislation regarding interception, privacy of communications and requirements to make behavioural advertising service OPT-IN as required under PECR, DPA as it will be processing personal information

At present people appear to have fewer and weaker rights online to stop unsolicited advertising compared to direct mail and telephone sales. There is no online equivalent to the telephone or mail preference services

Government should be neutral on behavioural advertising service, so long as behavioural advertising service is used according to all the relevant legislation, but the government should actively discourage non compliant behavioural advertising service by effectively enforcing the existing legislation

It should not be left up to individual users, ISPs and websites, as the ISP's have the legal muscle and money to ride roughshod over individuals and small site operators, who when tied into long term contracts can do little to protect their privacy, copyright or intellectual property

If there is no effective regulation of advertisers and marketing organisations then users will more frequently employ security packages and web browser settings to try and block the collection of personal data / browsing history to protect their privacy. This will have a negative effect on the internet as a whole but more specifically e-commerce as advertisers and marketing agencies will try more and more intrusive tactics to display their adverts to what they consider to be the target audience

The latest generation of behavioural targeted advertising (or interest based advertising as some are now calling it) that has been trialled by BT now on 3 occasions (twice without informing user or asking permission) using a technology called DPI (Deep Packet Inspection) has the ability to read and modify data between the user and the website they are looking at without them being aware, this raises a number of issues,

1. The user can no longer consider their communications as “private”
2. The user can no longer rely on the information they receive as being what the website sent
3. Will lead to more sites using encryption technology (which could impact national security due to the additional time required by the relevant agencies to decrypt the information)
4. Global loss of trust in the UK communication infrastructure
5. UK citizens losing trust in privacy of communications leading to slower take up or even decreased use of e-government services (such as online tax returns, e-voting, local council services) and lower than forecast cost savings from these services
6. Loss of revenue for parts of the UK Ecommerce community due to visitors being targeted by competitors using the site own content against them, very often in breach of the sites own terms and conditions and the designs, copyright and patents act
7. It is very difficult for websites or users to detect this sort of technology tampering with their communications (The vast majority do not have the skills either) as the technology is designed to be stealthy and invisible to both users and websites. (in fact one of the criteria for BT’s earlier trails was the user should not be able to detect the system)

Around the world other countries are considering the legality of DPI based advertising systems

1. There is a moratorium on this technology in the USA, (Democratic Representative Edward Markey of Massachusetts and Representative Joe Barton, a Republican from Texas took the lead in contacting US ISP’s regarding the use of DPI based advertising systems, under US cable privacy laws)
2. the Canadian ICO is investigating the legality of this technology
3. if the technology is rolled out in the UK but other parts of the world declare it undesirable or even illegal we could find UK citizens and businesses being denied access to parts of the internet

If another country deploys interception based behavioural targeted advertising I think the UK government has the duty of care to UK E-Commerce to protect the intellectual property of UK businesses by proportionate action (possible action includes discussion with the other government up to blocking access from the non UK ISP's using the technology)

Q3 Is there a need for new initiatives to deal with online privacy, and if so, what should be done?

The current legislation needs to be enforced effectively and to the fullest extent of the law.

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

The ICO only appears to have 2 options for acting and enforcing Data Protection laws

1. The ICO can fine a company which fails to register for DPA and processes personal data
2. They can issue an enforcement notice to a company which is registered for DPA if they feel the company is going to continue to breach DPA regulations but little else can be done. This power is also used sparingly due to budget constraints of the ICO as it requires the use of an external legal services to prepare the relevant paperwork

People's right to privacy is enshrined under EU law and should be upheld as a minimum

Third party access to the data stream in ISP core networks should be banned as large amounts of personal data (as described by DPA and PECR) traverse the core networks.

Access to DNS logs to provide aggregated statistics might be permissible so long as no profiles are created or data added to third party databases for ISP customers.

We also need to empower the ICO with specific communications privacy legislation and penalties to ensure he can do his job effectively and the UK seen as a leader in DATA PRIVACY instead of the UK being seen as weak or an easy target due to failure to be able to uphold existing weak legislation

Any profiling or data collection must be made "OPT-IN" for both ISP customers and website whose data is being collected or analysed regardless of the end use of the collected data.

Just because information is available on the internet should not mean the same copyright and intellectual property laws should not still apply as they do to hard copy information, but many companies seem to regard information on the internet as fair game due to the difficulty in proving who has accessed and what purpose they have used the data for, as they are often companies outside of the UK legal jurisdiction. Where the company is UK based it must be dealt with to the fullest extent of UK law to act as a deterrent to others

Advertising and marketing companies will argue that "OPT-IN" is not viable and would mean their business model would not have enough subscribers. My answer to that is that people do not see any incentive to OPT-IN. The model can be made to work, just look at the Tesco club card and other store loyalty cards like Nectar. People are not stupid and will OPT-IN if there is tangible benefit to them

Require ISP's to disclose all ways in which data is collected in the ISP network, exactly what data is collected, who processes that data, who buys or is given that data and how it is used in clear and easy to understand language

Q4 Is the current global approach to dealing with child sexual abuse images working effectively? If not, then how should it be improved?

No, it is partially successful in the countries that subscribe to the IWF list, but it still takes too long to get a takedown on the images. It is far more effective to deny the sites hosting space, but many sites hosting such

images are hosted in countries that do not recognise laws from external countries (like Russia etc) and offer to ignore take down notices and claim there servers are “bullet proof”

I think there is worldwide condemnation of child sex abuse and the images there of

The problem is this is a global issue, but around the globe there are many different stands on what is acceptable, it varies by culture and religion, and while a unilateral initiative is a start it is not a long term or complete solution and global co-operation is required

The easiest starting point is the lowest common denominator to the issues to get as many countries onboard as quickly as possible, then build on that to gradually improve and refine the agreement with the goal of denying any hosting space to people hosting this sort of content

One important point to consider when using ISP log data to identify hosts of such content is the ability for criminal gangs to take over computers remotely due to virus and malware infection, then host content on the computer without the computer owner knowledge or consent.

Q5 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?

Users and companies already pay for the transmission of their internet traffic in the service charges levied by the ISP’s; this can be seen in the various tariffs that ISP’s offer based on usage.

The problem has been in the last 5-10 years ISP’s have chased customers by offering cheaper and cheaper services, while also cutting costs and standards in the area of support and investment in new infrastructure and technologies. It has now reached the point where the ISP’s are losing money due to unsustainable business models (look at the service bundles offering TV, phone with free call and internet access for less than £25 being offered by several large communications companies)

What is needed is

1. The removal of the ability of the large communications giants to use loss leading services to try and gain customer base and market share

2. The enforcement of existing legislation relating to unfair contracts

3. Fix the maximum length of contracts or put in place safeguards for customers to break contracts when ISP’s add services like DPI/interception based behavioural advertising. BT currently do not consider DPI and profiling to be a material change to a customer enabling them to move to a new ISP to retain privacy without penalty

4. Make rolling contracts illegal (BT last year introduced a contract where at the end of a twelve month contract the customer was automatically enrolled into a new twelve month contract with no warning, unless the customer waded through the small print of a contract update on the internet) once out of contract a customer should be on a month by month basis, unless they wish to take a new service which entails a new contract, but that new contract should apply to that service only

5. Require ISP’s to disclose all ways in which data is collected in the ISP network, who processes the data, who buys or is given the data and how it is used in clear and easy to understand language

6. ISP’s should be required to remain a “mere conduit” and must be prevented from arbitrarily capping or throttling services, abusing private/confidential communication traffic, and censoring legal communications without explicit consent.