

Consumer Focus response to apComms inquiry: ‘Can we keep our hands off the internet?’

May 2009

Response to the apComms inquiry: 'Can we keep our hands off the internet?'

The vision for a competitive future that is safe and secure and fosters creation and new business models must be a joined up one. The lack of co-ordination across Government is evident in the plethora of work that is going on in relation to digital issues, much of it overlapping and interdependent (eg Digital Britain and the Digital Inclusion Action Plan). There is also a lot of good but unconnected work going on in the devolved administrations. Very few Government Departments either have the broad remit in relation to communications technology or the specific statutory responsibilities and it is imperative that the strands of work be brought together and that responsibility is centralised¹.

1. Can we distinguish circumstances where 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?

Traffic management and discretionary 'powers' vested with ISPs seem to be both anti-competitive and ultra vires. If regulation is needed then those decisions need to be made in a measured and non-commercial environment by elected representatives weighing up the public interest elements involved. They are not apt to be delegated to industry players.

If by bad traffic we are talking about illegal traffic, judgments as to what constitutes illegal traffic are open to interpretation and are properly interpreted through the independent executive and judicial bodies set up by law. For example: Are certain publications likely to incite racial hatred? Is an ISP an appropriate decision maker in these circumstances with powers to block distribution without a legitimate weighing up of free speech against potential harm caused.

While acknowledging that external enforcement is difficult, blocks and other traffic management mechanisms are not entirely effective because they are increasingly circumvented. There are other issues to consider such as: What are the commercial/contractual relationships between an ISP and content providers? What information is being collected about traffic and in particular what personal information is being collected? What level of security is provided on contracting with an ISP and how can this be enabled? While we believe it is important that ISP providers be required to meet basic standards of user control, traffic security and transparency, we do not support traffic management except to ensure the operation of the network and in relation to grave criminal conduct (such as child pornography).

¹ See also Consumer Focus, the digital divide, universal service and broadband, May 2009, recommendation 2.

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 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.

Consumers are concerned about privacy issues but not necessarily equipped to protect their own privacy. The profile/tracking process is not transparent and because of lack of transparency, marketing methods may be unfair and deceptive. Information is passed on to third parties with whom consumers have no direct relationship and therefore have no control over the transactions. Offline protection needs to apply to the online environment.

We are aware that industry has invested billions in developing new technology to better identify their market and in particular are carrying out neuro-research to find out the best way for marketing to influence individuals. There is no equivalent independent research on the potential effects of this type of marketing and on the development of technology such as user-controlled identity management. The development of privacy and security measures that are effective, easy to use and genuinely secure would go some way towards redressing the balance. A set of compliance standards for security, privacy settings and user control are an important first step; with these standards acting as necessary building blocks for informed or positive consent.

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. For example, 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.

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

There are real and legitimate concerns among consumers about privacy. Research undertaken by the Information Commissioner's Office indicates that 94 per cent of the population thought that 'protecting people's personal information was a major concern, ranking as the most important social concern along with preventing crime'².

These two major consumer concerns are linked because of lack of security and information control in an online environment. The online black market for personal data is thriving according to the latest Symantec report³. 'Phishing' is the most common medium however the second most-targeted companies are internet service providers, which hold data about email accounts. Hackers can access personal emails and the sensitive information often stored in them, including passwords and codes. Indeed, email accounts are the third most-sold item on the online black market.

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 developments⁴. We call upon the Government to undertake Privacy Impact Assessments (PIAs) for any private or public product or service that will store private data⁵.

Data should only be collected, processed and used with the express and voluntary permission of consumers freely given and not because provision of goods and services is conditional on the supply of personal information. Data protection principles need to be applied and updated in relation to information held digitally. The principles currently apply to personal data, often referred to as Personally Identifiable Information (PII). However the environment is changing and it is clear that while information utilised in profiling and collected by our ISPs and browsers may not be currently recognised as personal data, when combined with other information, it may be associated with a person or an ISP⁶.

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

² Report on the Finding of the Information Commissioner's office, Annual Track 2008, 4.1

³ Symantec, Symantec Global Internet Security Threat Report, Trends for 2008, Volume XIV, April 2009, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

⁴ Ed. Susanne Lacey, *The Glass Consumer: Life in a surveillance society*, National Consumer Council, 2005, pg.210- http://www.amazon.co.uk/gp/reader/1861347359/ref=sib_dp_pt#reader-link

⁵ Consumer Focus, Response to Digital Britain Interim Report, March 2009, p.30.

⁶ FTC Staff Report, Self-Regulatory Principles for Online Behavioural Advertising, February 2009.

provide personal data will depend on whether or not they have confidence in the way data sharing and use is regulated.⁷

Appropriate redress needs to be developed for an online environment. Given the potential for mass harm, collective systems of redress or representative action are fundamental. Liability for compensation should apply to ISPs, browsers and industry hosts where consumers suffer loss through inadequate security and privacy provisions.

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?

Consumer Focus strongly supports the principle of net neutrality. Broadband providers should not be permitted to use their market power to discriminate against competing applications, to prioritise and edit available content or to effectively tax content providers to guarantee speedy delivery of their data.

Traffic management for the purposes of offering premium service distorts the market in the sense that the industry is not profiting from demand for their content or services but from the ability to control the last mile of infrastructure. These controls just add another layer of differentiation to connection services that in some parts are sporadic or non-existent. It has real implications for on-line access to basic citizenship services and for discrimination and censorship.

The Government will need to take responsibility for steering and seeding our digital future. Many countries such as Denmark, Norway, Sweden, Australia and Finland have laid out significant public initiatives to ensure their competitiveness in world markets, impartial transmissions and non-discrimination on the basis of geography or affordability.

We have called upon the Government to act to support net neutrality and to ensure inter-compatibility and inter-operability of digital technologies⁸. It is unacceptable that consumers already face the situation where digital technologies and applications are not compatible beyond what may be termed expected technical difficulties. For example, consumers legitimately expect a MP3 they have purchased legally to play on any MP3 audio player, regardless the manufacturer – in the same way any vinyl record purchased can be played on any record player. However this is currently not universally the case. Similarly Facebook users cannot communicate with friends on other applications eg Bebo and cannot keep/transfer their accumulated data if they switch to another social networking site. Lack of compatibility in digital technologies may be deliberately employed for anti-competitive ends and thus cripple the open and free digital market.

⁷ Consumer Focus, Response to the Digital Britain Interim Report, March 2009, p 30.

⁸ As above, p 32

About Consumer Focus

Consumer Focus is the statutory organisation that champions the interests of consumers across England, Wales, Scotland, and, for post, Northern Ireland.

We were formed through the merger of three organisations – energywatch, Postwatch and the National Consumer Council (including the Scottish and Welsh Consumer Councils).

Through campaigning, advocacy and research, we are the voice of the consumer in private and public sectors by working to secure fairer markets, greater value for money, and improved customer service.

Contact: Linda Weatherhead, Linda.Weatherhead@consumerfocus.org.uk

Copyright: Consumer Focus

Published: May 2009

If you require this publication in Braille, large print or on audio CD please contact us.
For the deaf, hard of hearing or speech impaired, contact Consumer Focus via Text Relay:

From a textphone, call 18001 020 7799 7900

From a telephone, call 18002 0207 799 7900

Consumer Focus

4th Floor
Artillery House
Artillery Row
London SW1P 1RT
www.consumerfocus.org.uk

Tel: 020 7799 7900

Fax: 020 7799 7901

Media Team: 020 7799 8005 / 8006