

## **Ofcom Traffic Management and ‘net neutrality’ Consultation**

*European Privacy Association*

The current debate surrounding traffic management and net neutrality is focused primarily on competition and engineering issues, two very serious issues of concern that are important to consider when discussing this matter. Traffic management presents a tremendous opportunity for engineers who have been seeking for some time to bring order to the chaos of flowing data (or in increasing cases, highly congested data). This will provide much needed capacity for increasingly data-heavy applications and content upon which users have begun to rely upon. To think that little more than 10 years ago, many internet users were able to rely on 56K dial-up modems. Today, this would barely allow a user to check email and read newspapers, let alone do the myriad of other things that content and application providers have made possible through innovation.

However, one issue that has not been addressed, and for which we, at European Privacy Association, have grave concerns, is the privacy implications presented by the threat of not allowing traffic management. By imposing net neutrality regulation on a dynamic medium for economic activity, social interaction, and political engagement, the ever present issue of privacy will become impossible to address as those with the power to intervene are rendered powerless.

Proponents of net neutrality claim that this regulation would ensure that Internet Service Providers (ISP) would not be allowed to “monitor” user activity. However, this reflects a profound misunderstanding of the role of ISPs, and how traffic management would be applied. Traffic management does not involve “monitoring” of user activity, but simply the prioritization of traffic based on the quality of service needs behind specific requests. While this request for prioritization could originate with the consumer, it is more likely to originate from content providers who wish to ensure that download speeds from their sites and/or for their applications are maintained at a predetermined level.

With the application of traffic management, this could also allow for ISPs to ensure that privacy needs are being maintained. An ISP that wishes for its network to be the strongest enforcer of privacy in the industry may offer customers the ability to have data that is collected from them to be suppressed through selective blocking of cookies and requests from content and applications providers.

While such measures have not been undertaken to date by ISPs, the fact that they might have this ability is a boon for consumers, for whom the internet has been both a tremendous opportunity, while also posing its fair share of risks. From online scams and viruses, to isolated predatory practices by some content and application providers, the internet is the new frontier which poses problems every day to users. As these threats evolve, so must the ability and capability for handling these threats evolve.

One of the new internet base services that is emerging is cloud computing, which allows individuals to house data in a manner that can be accessed remotely. As Cloud computing removes the physical control of data, traffic management will contribute by allowing users to efficiently access files. Furthermore, traffic management will add an additional layer of privacy

protection, through limiting and protecting access to personal information from those who do not have a right to access.

As such, it must be remembered that data protection is something wider than privacy: It means also "identity protection". Traffic management, without monitoring users, could instead allow the adoption of "protected-anonymity" and privacy enhancing technologies: the individual user could navigate through a secure and safe Internet, choosing whether and how much information about themselves they want to disclose. At the same time, it would be more effective and sure the fight against cybercrime, because every user could be unmasked if operating illegally on line.

Herein lies the threat presented by net neutrality (and any other innovation stifling form of regulation based on limiting technical progress). While proponents of this regulation seek to promote net neutrality as an equalizer, bringing all data, and thereby consumers down to the same level, they also ignore the perils that such regulation presents. By forcing ISPs to develop and maintain dumb networks, they make it impossible for operators to provide added value to their networks through breakthroughs in technology. What might seem like good legislation today could be the barrier to providing protection to consumers tomorrow.

While we welcome this discussion on the concerns and merits behind net neutrality, we caution Ofcom, along with any other regulator, to avoid overhasty action on this issue. Much of the debate has illustrated extreme views on the concept of the 'net neutrality' – but there is no doubt that such regulation would be legislating technical parameters that continue to change.