

Thursday, 30 September 2010

Policy Development Unit (B1), BU33 7/40  
DG Information Society and Media  
European Commission  
B-1049 Brussels, Belgium

**Letter responding the European Commission's Consultation on Net Neutrality**  
*Italian Institute for Privacy and European Privacy Association*

Dear Sir or Madame,

Recent actions and events have highlighted the importance placed on privacy within the European Union, and the continued need to protect it. From the explosive growth of Facebook, to Google's drive to collect any and all information, privacy is a central concern in today's digital revolution. While we welcome innovation and many of the services and technologies that content and application providers offer, privacy continues to be a difficult issue to properly account for.

However, when it comes to regulation of the infrastructure, privacy has been woefully ignored by policymakers and advocates alike. As we seek to establish a solid regulatory framework for the internet's infrastructure, privacy protections must be protected, and in no way limited. Unfortunately, the debate surrounding net neutrality has ignored privacy entirely, at our own peril.

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 promulgate the phony claim that this regulation would ensure that Internet Service Providers (ISP) would not be allowed to "monitor" user activity and would therefore grant users an extraordinary amount of privacy. This, of course, reflects a profound misunderstanding of the role of ISPs, and how traffic management would be applied.

In practice, traffic management does not involve the "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, cognizant of the limited supply of bandwidth, 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", a major issue for any modern day internet user. 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 European Commission, 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.

We understand that net neutrality is an extremely complex issue, and the European debate itself is in its infancy compared to the standoff across the Atlantic. The questions covered in your consultation certainly offer participants the opportunity to provide an in depth insight on both the merits and drawbacks of net neutrality. However, the imposition of net neutrality would completely overthrow the existing governance of the internet, undermining the very structures that are integral to preserving the privacy of the individual.

We therefore call on you to consider the need of all consumers as you discuss the merits of net neutrality regulation. Will consumers be safer with this regulation? Will their internet experience

and online commercial activities be improved? Or will progress be stopped, limited by the very regulatory measures that everyone was told would ensure a vibrant, innovative internet?

Sincerely,

Luca Bolognini,  
Chair of the Italian Institute for Privacy  
Board Member of the European Privacy Association

### **Italian Institute for Privacy**

The Istituto Italiano per la Privacy (IIP), or Italian Institute for Privacy, is a research center dedicated to the thematic of cybersecurity and protection of personal data in global ICT society. IIP is founding partner of the European Privacy Association. The Institute involves and is a network for the best Italian specialists in Privacy Law, but also for significant representatives of the public and private spheres, who often deal with personal data and sensitive information on a daily basis. Working as a think tank, the IIP has consolidated itself as a point of reference for Italian “new law” experts, and for several of the players of high technology content markets.

IIP is part of the European Privacy Association, the sole pan-European coalition focused on personal information. As the only independent cross-sector organization, EPA is ideally positioned to provide a ‘venue’ for bringing together experts from across Europe, and engage with them to shape new policies to enhance privacy, e-security and data protection.