Net Neutrality & Privacy

The Project

1. What is Network Neutrality?
2. What are the Pros and Cons of Network Neutrality? Highlighting Privacy Concerns.
3. Is Network Neutrality currently backed up by law?
4. In what way could media-aware user-dependent self-adaptive networks be affected by Network Neutrality concerns and regulations?

- What is Net Neutrality?
- Electronic Communications Regulations
- DPI, Privacy and Data Protection.

What is Net Neutrality?

- *The purest version of 'net neutrality' assumes that:*
  - *There should be no prioritisation of any type of traffic by network operators; and*
  - *Those providing content, applications and services via the open Internet should not be charged by network operators/ISPs for the distribution of that content to the network operator/ISPs' customer base*
    - *OFCOM "Traffic Management and Net Neutrality" 2010*

The 2 Aspects of net Neutrality.

- Negative Net Neutrality:
  - The blocking and throttling of content.
- Positive Net Neutrality:
  - Prioritising content for QoS

"Charging more for more and charging the same for less" - Chris Marsden, Net Neutrality pg 38

Electronic Communications Regulation

- Recently updated by 2 new Directives.
- Comes into force on 26th May 2011 (today)
- Article 8(4)(g) Framework Directive states:
  - "The [NRAs] shall promote the interests of the citizens of the [EU] by:
    - (g) promoting the ability of end-users to access and distribute information or run applications and services of their choice"

- However the powers given to NRAs to enforce this are lacking.

Universal Service Directive

- Article 23(3) Universal Service Directive states:
  - *In order to prevent the degradation of service and the hindering or slowing down of traffic over networks. Member States shall ensure that [NRAs] are able to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks.*
- But, as of today, no NRAs have taken the opportunity to specify such a requirement.

Transparency

- Article 21 Universal Service Directive provides for greater transparency.

- In the UK the Broadband Stakeholder Group (BSG) has initiated self-regulation whereby they will provide a standardised table of any restrictions on their service.
  - First tables published in June 2011

Deep Packet Inspection or Flags

- If flags are used to prioritise content for Qos in OTT services then privacy will be maintained to the extent it is today.
  - If all information is in the packet header then nothing changes.
- However this is open to potential spoofing and freeriding on guaranteed QoS.
  - Which leads to the use of DPI.

DPI

- it is possible to tell whether a packet stream is VOIP, email, web browsing, instant messaging, video streaming, file transfer, or peer to peer file sharing. It is possible to examine in detail the content of the email, or web page, or downloaded file. It is possible to distinguish music files from text from pictures. It is possible to search for keywords within any text.
  - Jon M. Peha, The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy

Personal Data

- Article 2(a) DPD:
  - ”Any information relating to an identified or identifiable natural person…; an identifiable personis one who can be identified directly or indirectly”
- Given access to further information an IP address can be considered as Personal data.
- Any data that could identify a person is processed when DPI is invloved.

Special Categories of Data

- Article 8 DPD sets out special categories:
  - Racial of ethnical origin, political opinions, religious or philosophical beliefs, trade union membership, health and sex life.
- As processing could include some of these categories it should be presumed that all data is sensitive personal data.

Article 6

- (b): data must be collected for specific, explicit, and legitimate purposes and not further processed in an incompatible way.
- (c): data must be adequate, relevant and not excessive
  - There is and will continue to be an arms race between network providers and those wishing to circumvent their systems. So over time, more and more data might be required.

Article 7 - Consent

- Unambiguous (7(a))
- Explicit for sensitive data.
  - ”freely given specific and informed indication of his wishes … to personal data being processed”

- Can only be given to a Users’ own ISP as relationship not proximal enough for further network providers.

Privacy of Electronic Communications

- *Member states shall ensure the confidentiality of communications and related traffic data by means of a public communications network and publicly available electronic communications services... In particular,* ***they shall prohibit listening, tapping, storage or other kinds of interception or surveillance*** *of communications and the related traffic data by persons other than users,* ***without the consent of the concerned.****"* (emphasis added)