Critical Internet related issues in Europe

ENOG 7, Москве, 27 May 2014

Frédéric Donck, Director, European Regional Bureau

Internet Society™

1.Net Neutrality

ENOG 7, Москве, 27 May 2014

Frédéric Donck, Director, European Regional Bureau

1.Internet key characteristics: the Internet Model

The Internet is successful in large part due to its unique model of development and deployment:

•Shared global ownership- no central control

•Open technical standards

•Collaborative Engagement models- researchers, business, civil society, academia, government

•Freely accessible processes for technology and policy deployment

•Transparent and collaborative governance

Internet key characteristics

- An network of network (inter-network) designed to pass standardized packets of data
- The Internet does **not** care what is in the packets
- **Best-effort** transport between and within networks
- Openness allows
  - innovation in application and services (‘innovation without permission’)
  - rapid growth and distributed coordination (without central control)

2.« Network Neutrality »: the origin of the debate

- Increasing demand for Internet connections with greater bandwidth

- More pressure on network capacity, hence greater deployment and use of congestion management and traffic shaping

- At core of the debate: is traffic management (i.e. ability to treat packets differently) a threat to the open architecture of the Internet?

- *Network Neutrality*: broad term - no clear definition (free expression, user choice, traffic management, pricing, discrimination, etc.)

Desired Outcome: Open Internet

•Openness is the overarching principle that has ensured the success and growth of the Internet to date,

• …and it offers useful guidance on how to best address some of the core issues as part of the NN debate.

•Users expect an Internet in which traffic is conveyed in a manner that is agnostic to source, content and destination.

•Key enablers: Access/Choice/Transparency

3.Internet: need to establish some common terminology

•Key concern to-day stems from the **very success of the Internet Protocol (IP)** as a networking technology:

Number of networked services are offered in addition to Internet service (eg.VoB, TV & video delivery)

➢Some concerns re: traffic priority?

•Need to clearly distinguish Internet service from any other IP-base services…and of course, this should be made clear to consumers

Internet Service

***Internet service* is: connection of an Internet endpoint or network to the rest of the Internet with non-discriminatory, best-effort routing of data packets as part of the Internet.**

- Non-discriminatory by definition
- Networks should simply move the bits along the wire
- Can include application-agnostic congestion management, for example, or traffic management to maintain network resilience

IP-based services (Specialized services)

***IP-based services* are: services that are built using the Internet Protocol, but that operate within a restricted set of networks, or only one network.**

- Often optimized for a single service or service type, and rely on a single administrative domain controlling the network in order to ensure (or enforce) specific service characteristics.
- Examples of IP-based services include video delivery and some communications service offerings (such as voice over broadband).

Internet-based services and applications

***Internet-based services and applications* are: services and applications that are delivered over or made possible by the Internet service direct to end-users.**

- *Do not* rely on administrative control from the network.
- *Do* rely on the underlying Internet service conforming to standardized best practices and non-invasive network management techniques.
- Skype is an example of an Internet-based online communications application.

4. Key challenges: Traffic Management

- Traffic management is a normal part of every day network operation and network management- It is needed to ensure that all subscribers are able to obtain adequate service, esp. at peak time (congestion is a ‘natural’ consequence of the Internet’s design)…but
- Should remain protocol or application neutral
- Should not be used as a tool for anticompetitive behaviour
- Should be transparent
- …and should not be considered as a panacea (adding capacity to networks is alos critical to alleviating congestion!)

Comparison?

Imagine your electricity provider could charge you more for the electricity you use to light, heat and power ICT devices in your home office.

- they can’t do that
- if new technology made that possible, would we welcome it?

This has nothing to do with ‘reasonable network management’ and everything to do with trying to segment the market for commercial advantage.

It is an abuse of the network operator’s role.

Key Challenges for Policymakers and Regulators

- Effective competition
- Enable the users to make an informed choice
- Clear information on limitations and traffic management practices that the subscriber is subject to,
- Reasonable network management, neither anti-competitive nor prejudicial
- Share common terminology of Internet service
- …and Internet service monitoring

5. EU Commission Draft Regulation (September 13, 2013)

- **Strong principles:**

« End-users shall be free to access and distribute information and content, run applications and use services of their choice »

Prohibition « of blocking, slowing down, degrading or discriminating against specific content, applications or services »

- **With some exceptions:**

Exceptions include Legal order or court order; Network integrity and security; Combat of spam; Minimising congestion

What are « reasonable traffic management measures »?

5. EU Commission Draft Regulation (2)

Introduce the right to provide « Specialized services » (explicit):

« Providers of content (…) and providers of electronic communications (…) shall be free to enter into agreements wit each other to transmit the related data volume or traffic as specialised services with a defined quality of services or dedicated capacity »

Questions/Issues:

- **Best effort vs. Least effort?**
- **« specialised services shall not impair the general quality of Internet access »…which level of impairment is (un)acceptable?**
- **Which incentives to add capacity?**
- **Measurements of quality?**

European Parliament Plenary vote (April 3, 2014)

1. Definition of NN in a binding act (« the right –*vs the freedom*- for end users to access and distribute information and content of their choice from a terminal of their choice »)

2. Stricter definition of specialised services- conditions:

1. Network capacity is sufficient to provide them in addition to Internet access services
2. They are not to the detriment of the availability or quality of Internet access services
3. Providers of Internet access to end users **shall not discriminate between functionally equivalent services and applications**

European Parliament vote (2)

3. Traffic management: mixed message

-Broaden traffic management: allow operators to « prevent and mitigate » the effects of congestion (*vs. « minimise »them*)

-Limit traffic management: it could only be applied in case of « <u>temporary and exceptional</u> » network congestion (*vs. Temporary* ***<u>or</u>*** *exceptional congestion***)**

4. Quality of services:

•complaint procedures for users wrt open Internet and traffic management

•Right for NRAs to impose minimum QoS levels and other QoS parameters, beyond minimum QoS.

•Annual report from NRAs to EU Commission and BEREC on compliance of NN and effect of Specialised services on cultural diversity and innovation

BEREC Report on « Monitoring quality of Internet access services in the context of net neutrality » (8 March 2014)

•Multiple references to the importance of IETF

•Recommends that NRAs increasingly put emphasis on evaluating performance of IAS as a whole, to assess potential degradation due to specialised services

•Recommends to monitor quality of connectivity to diverse destinations, not just popular ones.

•greater co-operation between European regulators on the subject of building a trans-border measurement system

•greater involvement with IETF as a source of technical expertise, metrics and frameworks for a common measurement platform

US situation

FCC Open Internet Advisory Ctee (July 2013)

- **High level principles**: a service should not be able to escape regulatory burden or acquire a burden by moving to IP
- Specialised services should not deter or limit **investment** in Internet services
- **Measurements** on the Internet? Let’s start looking at the **quality of the user experience**, not the technical parameters.

… January 2014: Is NN still alive in the US?

- **US court of Appeal and FCC authority**
- **Comcast/Netflix deal (a precedent? Apple next deal?)**

US Situation (2)

FCC

- to scrutinize deals (broadband providers not putting non-paying companies' content at a disadvantage)

- seek comments on whether "paid prioritization," should be banned outright, and look to prohibit the big broadband companies from doing deals with some content companies on terms that they aren't offering to others

- invite comments on whether broadband Internet service should be considered a public utility

Mozilla and Tim Wu:

have proposed an approach to apply traditional telecom regulation to last mile relationships between Internet providers and content companies by asking the FCC to designate remote delivery services as telecommunications services under Title II of the Communications Act.

Conclusion

•**Polarisation of the debate (ETNO/Cable Europe/ECTA/ GSMA vs. the others…)**

•**Institutional complexity**

- **Co-legislators** (MS & EP)
- **EP election** (25 May 2014) and…**New Round** in Parliament?
- Council of **Ministers** and (Italian) Presidency (S2-2014)

•EP wants EU Commission to **review framework by mid-2016**

•**Role of BEREC (EU regulators)**

•**Influence of US debate**

2. DNS Blocking

ENOG 7, Москве, 27 May 2014

Frédéric Donck, Director, European Regional Bureau

The « great temptation »…

2012:

US government: SOPA (« Stop Online Privacy Act) / PIPA (« Protect IP act ») which would require ISPs to falsify DNS results in an effort to curtail access to websites offering counterfeit goods

…

2014:

DNS blocking of Twitter and YouTube in Turkey

What we heard from Turkey (March/April)

Blocking being performed at a lower level, in the routing system itself.

- Reports started coming in that *some* Turkish ISPs were taking hijacking routing of the Border Gateway Protocol (BGP) and *pretending to be Google's Public DNS servers* (and the servers of other similar services).
- Apparently, the ISPs were sending the traffic to their own DNS servers which give out the wrong answers.
- So, these servers were masquerading as the Google Public DNS service.

- **In short, with this modification, the Turkish routers were lying about how to get to the Google Public DNS service, and taking all the traffic to a different destination. They were lying about where the Google service resides — by hijacking the traffic.**

ISOC Position wrt DNS blocking

- ***Easily circumventented***

Users who wish to download filtered content can simply use IP addresses instead of DNS names.

As users discover the many ways to work around DNS filtering, the effectiveness of filtering will be reduced. ISPs will be required to implement stronger controls, placing them in the middle of an unwelcome battle between Internet users and national governments.

- ***Doesn’t solve the problem***

Filtering DNS or blocking the name does not remove the illegal content. A different domain name pointing to the same Internet address could be established within minutes.

ISOC Position wrt DNS blocking (2)

- ***Incompatible with DNSSEC and impedes DNSSEC deployment***

DNSSEC ensures that DNS data are not modified by anyone between the data owner and the consumer. To DNSSEC, DNS filtering looks the same as a hacker trying to impersonate a legitimate web site to steal personal information—exactly the problem that DNSSEC is trying to solve. DNSSEC cannot differentiate legally sanctioned filtering from cybercrime.

- ***Causes collateral damage***

When both legal and illegal content share the same domain name, DNS filtering blocks access to everything. For example, blocking access to a single Wikipedia article using DNS filtering would also block millions of other Wikipedia articles.

ISOC Position wrt DNS blocking (3)

- ***Puts users at-risk***
  When local DNS service is not considered reliable and open, Internet users may use alternative and non-standard approaches, such as downloading software that redirects their traffic to avoid filters. These makeshift solutions subject users to additional security risks.

- ***Encourages fragmentation***
  A coherent and consistent structure is important to the successful operation of the Internet. DNS filtering eliminates this consistency and fragments the DNS, which undermines the structure of the Internet.

ISOC Position wrt DNS blocking (4)

- ***Drives service underground***
  If DNS filtering becomes widespread, “underground” DNS services and alternative domain namespaces will be established, further fragmenting the Internet, and taking the content out of easy view of law enforcement.

- ***Raises human rights and due process concerns***
  DNS filtering is a broad measure, unable to distinguish illegal and legitimate content on the same domain. Implemented carelessly or improperly, it has the potential to restrict free and open communications and could be used in ways that limit the rights of individuals or minority groups.