10th Global Symposium for Regulators
10-12 November 2010
Dakar
SENEGAL

GSR10
Best Practice Guidelines for Enabling Open Access[1]

With the growing complexity of the ICT market environment, there is a need to rethink the different degrees of regulation to anchor national broadband strategies and regulatory frameworks around the multi-facetted concept of open access to and over networks, which provides for achieving effective competition while ensuring accessible, affordable and reliable services for consumers.

A new ladder of regulation may now be required to set the right balance between service competition and infrastructure competition to address the challenges associated with access to broadband networks and services. This includes ensuring equal and non-discriminatory access to the networks and lifting potential bottlenecks that could prevent end users from enjoying the full benefits of living in a digital world, driven by speed, ubiquity of access and affordable prices, irrespective of the location of the networks providers and users.

We, the regulators participating in the 2010 Global Symposium for Regulators, put forward the following best practice guidelines for enabling open networks.

I. Defining open access: making sense of the various concepts

1. We note that, from a service provider's perspective, open access means the possibility for third parties to use an existing network infrastructure. Open access can have two main forms: regulated open access (such as unbundling, especially where there is a dominant operator), and commercial open access.

2. Every user (consumer) should have access to all services and applications carried over these networks, as long as those services and applications are public and lawful; regardless of the type of network and who is supplying or using them; and in a transparent and non-discriminatory fashion. The user's range of choice should not be unduly constrained by the inability of competitors to obtain access services, especially over the last mile infrastructure.

II. Open access to networks: what policy and regulatory tools are needed to enable opening up access to network facilities (i.e., international fibre networks, "essential" or "bottleneck" facilities, other networks) without harming investment and innovation?

1. We stress the importance of legislation to set out the general principles of open access – non-discrimination, effectiveness and transparency – highlighting the importance of both active and passive infrastructure sharing in the deployment of electronic communications networks in property owned by any operator, private entities and public bodies, even if they are operating in other sectors.

2. We note that in order to encourage broadband deployment, preserve and promote the open and the interconnected nature of the public Internet, regulators may consider mandating dominant providers of national broadband networks, including cable landing

[1] The Best Practice Guidelines were developed based on input received from: Congo (Rep. of), France, India, Lebanon, Liberia, Mauritius, Portugal, Saudi Arabia, Senegal, Suriname, Switzerland, Thailand, and the United States.

stations, to provide open access on a fair and non-discriminatory basis to their networks and essential facilities for competitors at different levels of the networks.

3. We recognize the importance of wholesale regulation, including the obligation to publish reference offers for access to essential facilities and prices oriented to costs, as means to ensure open access.

4. We recognize that, in countries where Fibre-to-the-Building is deployed, the regulators need to define rules that ensure shared and equal access, and prevent discriminatory behaviors and monopolization by the first infrastructure operator in such buildings.

5. We recognize that a centralized information system, containing the data records of infrastructures held by public bodies, electronic communications operators and other public utilities that can be shared, would be of great advantage to all market players. We encourage operators to set up and make available in a database accessible online, information regarding passive infrastructure (i.e., civil elements such as ducts and towers) that can be shared (including paths and space available) with the respective prices oriented to costs.

6. We recognize the importance of coordination among all stakeholders (from the ICT sector and beyond) in the deployment of civil works to prevent any barriers to the spread of broadband networks. We furthermore stress the importance of defining flexible open access rules adapted to the fast-paced broadband growth.

7. We recommend the development of a change management strategy to assist the regulators in reforming their regulatory practices in order to adequately adapt to the exigencies of new market structures, innovations and business models.

III. Open networks: how to ensure that every citizen has access to the benefits of ubiquitous broadband networks (i.e., through policies for universal access to broadband, transition to NGN, leveraging on the digital dividend)

1. We recognize that efficient allocation and assignment of the digital dividend spectrum, will result in social and economic benefits that could stimulate innovation for the provision of lower-cost communications and services, especially in rural and remote areas.

2. We suggest that governments update the definition of universal service as needs evolve to ensure technology neutrality and the inclusion of broadband access.

3. We note the need to put in place concrete national plans and strategies to stimulate deployment of broadband networks, particularly in developing countries. Furthermore, given the challenges in attracting investment for large scale deployments, these strategies should consider the role of the state in funding the national broadband infrastructure, *inter alia* through Public Private Partnerships and promoting the involvement of municipalities or cities.

IV. Open and neutral Internet: how to handle traffic management over increasingly congested networks while applying fair rules?

1. With regard to Internet traffic management, we recommend that only objectively justifiable differentiations be made in the way in which various data streams are treated, whether according to the type of content, the service, application, device or the address of the stream's origin or destination.

2. We recommend that when Internet Service Providers (ISPs) do employ traffic management mechanisms for ensuring access to the Internet at any point of the network, they comply with the general principles of relevance, proportionality, efficiency, non-discrimination between parties and transparency.

3. We recognize that to ensure reasonable traffic management practices, regulators should take measures such as:

- Consider implementing measures for ISPs to disclose information concerning network management, quality of service and other practices as is reasonably required for subscribers and content, application, and service providers;
- Allow clients to quickly end their contracts without high switching costs,
- Allow clients to prescribe minimum quality of service for Internet access, and
- Create policy directives stating the rights of consumers to access any lawful content, applications, and services over their Internet connections.

4. We note that these principles would not supersede any obligation an ISP may have—or limit its ability—to deliver emergency communications or to address the needs of law enforcement, public safety, or national or homeland security authorities, consistent with applicable law.

5. Regulators may consider facilitating the creation of local content and the implementation of local Internet exchange points (IXP), to complement and ease the international data flow.

V. Open access to content: what role for regulators in bringing public services online (i.e. e-government, e-education, e-health) and creating demand for such services?

1. We stress the importance, on one hand, of the creation of preconditions for the organizational, legal and technical, standardization and interoperability aspects, so that public authorities can offer their services electronically and, on the other hand, that public websites be created and maintained to be user friendly and accessible to all, according to relevant guidelines and standards.

2. Regulators may also want to ensure broadband connectivity to all schools, health centres and hospitals so that citizens may benefit when connecting through high bandwidth to these services.

3. We note that there is a definite need to create awareness about the risks of technological progress among consumers and take necessary measures for data protection, privacy, consumer rights, and protection of minors and vulnerable segments of the society.

VI. Challenges to open networks (i.e., cyberthreats, unforeseen aspects of the Information Society, disputes, regulatory efficiency and consistency across services and networks): what strategies?

1. We note that open networks pose challenges in terms of network stability, business continuity, resilience, critical infrastructure protection, data privacy and crime prevention. IP networks, being based on an open architecture and well known protocols, are vulnerable to cyber attacks. The complexity of the challenges require cross-cutting approaches in the form of multi-stakeholder processes on one hand, and enhanced inter-service co-operation between the various authorities concerned on the other.

2. We note that it is essential that service providers exercise reasonable network management practices with respect to outbound as well as inbound traffic. Such practices can help stamp out attacks at the source and thus stop them from spreading, without subjecting the network to congestion.

3. We recommend that measures for outbound traffic monitoring be developed and eventually standardized to add a new layer of security to the existing measures deployed by stakeholders.

4. Regulators may consider implementing measures to prevent ISPs from connecting unlawful user devices to the networks.

5. We recognize that strategies aimed at ensuring security in cyberspace has to transition from the traditional reactive stance to an incrementally proactive stance by reducing windows of vulnerability, improving reaction times, and effectively mitigating attacks. Also, we stress that preventing attacks by patching vulnerable systems, implementing firewalls or other access control technologies, monitoring through intrusion detection systems, and responding to the threats in real time, have become crucial to effective network operation.

6. We stress the importance of a harmonized regulatory framework within regions and the establishment of a broader dialogue between all stakeholders so that this central issue of open access networks can be further discussed and the appropriate measures taken.