International Telecommunication Union

QUESTION 18-1/1

Final Report

ITU-D STUDY GROUP 1 4th STUDY PERIOD (2006-2010)

QUESTION 18-1/1:

Domestic enforcement of telecommunication laws, rules and regulations by national telecommunication regulatory authorities

THE STUDY GROUPS OF ITU-D

In accordance with Resolution 2 (Doha, 2006), WTDC-06 maintained two study groups and determined the Questions to be studied by them. The working procedures to be followed by the study groups are defined in Resolution 1 (Doha, 2006) adopted by WTDC-06. For the period 2006-2010, Study Group 1 was entrusted with the study of nine Questions in the field of telecommunication development strategies and policies. Study Group 2 was entrusted with the study of ten Questions in the field of development and management of telecommunication services and networks and ICT applications.

For further information

Please contact:

Mr Makhtar FALL
Telecommunication Development Bureau (BDT)
ITU
Place des Nations
CH-1211 GENEVA 20
Switzerland
Telephone: +41 22 730 6256
Fax: +41 22 730 5484
E-mail: makhtar.fall@itu.int

Placing orders for ITU publications

Please note that orders cannot be taken over the telephone. They should be sent by fax or e-mail.

ITU
Sales Service
Place des Nations
CH-1211 GENEVA 20
Switzerland
Fax: +41 22 730 5194
E-mail: sales@itu.int

The Electronic Bookshop of ITU: www.itu.int/publications

International Telecommunication Union

ITU-D STUDY GROUP 1 4th STUDY PERIOD (2006-2010)

QUESTION 18-1/1:

Domestic enforcement of telecommunication laws, rules, and regulations by national telecommunications regulatory authorities

DISCLAIMER

This report has been prepared by many experts from different administrations and companies. The mention of specific companies or products does not imply any endorsement or recommendation by ITU.

ABSTRACT

Building on the results attained in the last study period, the report describes enforcement practices in selected countries, covering competition, interconnection, spectrum, consumers, network infrastructure (site) sharing, quality of service, and network security.

The 97 guidelines presented are intended to be a menu of choices for Member States to consider and use as they find appropriate in their own circumstances. In addition, the experiences and examples of more than 40 countries are presented to further illustrate the challenges to enforcing communications laws that National Regulatory Authorities (NRAs) are facing – and how many are successfully meeting those challenges. Taken collectively, the contents of this report can assist NRAs and other policy makers as they chart their course toward long-held universal access goals.

TABLE OF CONTENTS

Page

QUESTION 18-1/1

Enforcing national telecommunications laws: Report and best practice guidelines

1 Introduction

The world's national telecommunications regulatory authorities (NRA's) play an important role in executing domestic communications policy, and thereby contribute both to sustainable development of the communications sector and domestic economic development objectives.

Over the last two decades, the number of NRAs has rapidly grown. As recently as the second quarter of 2009, there were 153 across the globe. Back in 1990, there were only 14 NRAs. From 2000 to 2005, their number increased worldwide by approximately 36%.[1] The vast majority, however, have less than 10 year's experience.

Due to persistent and rapid changes in the communications sector, more and more of these agencies are finding it necessary to assert their enforcement authority in dynamic and unfamiliar territory. Like all others in the telecom and information and communications technology (ICT) sectors, NRAs are profoundly affected by convergence and their role will continue to be impacted by this phenomenon for the foreseeable future.

This report will focus on some of the common enforcement challenges facing today's NRAs in a number of areas identified by the membership: competition, interconnection, spectrum, consumer issues, site (network infrastructure) sharing, quality of service, and network security. The final report will suggest guidelines pertaining to each of these areas.

It bears mentioning at the outset that notwithstanding the importance of enforcement to the success of a domestic telecommunications regime, the means and power to enforce policy and regulation is not an end in itself. Rather, it is one of the critical ways for an NRA to attain its chief goal: to facilitate universal access and service to its citizens by enabling industry growth and worldwide competitiveness.[2]

2 Background

During the 2002 – 2006 study cycle, with valuable support and assistance from the ITU Development Bureau (BDT), the Rapporteur's Group for ITU-D Question 18/1 produced a report containing fifty-seven guidelines on how NRAs could enforce their domestic telecommunications laws. *Domestic Enforcement of Telecommunications Laws: Guidelines for the International Community (2006)* broadly covers six areas: legislation; process and procedure; independent decision making; sanctions; organizational structure; and gender.

With regard to **legislation**, the **fourteen** guidelines contained in the 2006 report discuss the statutory authority desirable for an NRA; the **seventeen** guidelines pertaining to **practice and procedure** discuss day-to-day implementation of enforcement procedures; the **ten** guidelines on **sanctions** suggest ways to determine penalties; the **three** guidelines on **independent decision making** suggest ways an NRA can make an independent decision notwithstanding its political or operational independence; the **seven** guidelines on **organizational structure** discuss ways to configure an NRA to maximize domestic goals; the **six** guidelines on enforcement and **gender** address how enforcing telecom laws can be used to narrow the gender gap in ICTs.

---

[1] Trends in Telecommunications Reform 2006, International Telecommunication Union at 12.

[2] See *Report on Domestic Enforcement of Telecommunication Laws; Guidelines for the International Community*, ITU-D Question 18/1/1/ Report, 2002-2006 study period, at v.

As the forerunner to this report, *Enforcement Guidelines 2006* provides an important foundation and basic context for the substantive challenges to enforcement that are addressed in this report. The former addresses fundamental issues of enforcement, which often are embedded in or work in tandem with executing a comprehensive solution to a discrete enforcement problem. Optimally, then, it would be useful to consider both sets of guidelines, and the corresponding reports, together. *Enforcement Guidelines 2006* may be found at http://www.itu.int/pub/D-STG-SG01.18-2006/en[3] and in Annex C to this report.

3 Enforcing Competition Laws, Policies, Regulation

3.1 Overview

The benefits obtained from competition are key to promoting efficiency and consumer welfare. Competition promotes efficiency by inducing firms to produce more with less, better allocate resources, introduce new technology, and meet customer demands.[4] In addition, the introduction and growth of competitive forces in a given market can in some instances help regulators manage the marketplace for the benefit of consumers and the general public.

Globally, most markets have evolved from state-owned monopoly fixed service providers to competitive markets of varying degree. However, even incumbents that remain state owned generally experience competition from at least one source, e.g., mobile and/or Internet service providers, regardless of whether there is private investment. Increasingly, these incumbents also face newcomers of all kinds: wireless service providers, Internet Service Providers (ISPs), cable service providers, even power companies.

Mobile services for example, initially competed indirectly with fixed services, then directly, and now in most cases substitute for fixed service. In response, to preserve both market share and revenue levels, many wire line incumbents now also provide mobile and other services. An interesting snapshot of various NRA's regulatory treatment of Internet and VOIP services illustrates the diversity of responses to this competitive challenge, and is also discussed in this section beginning on page 9.

Most legislatures have decreed some level of competition, and though basic voice services remain less competitive than mobile, over 60% of the world's economies have opened up their basic services market to some degree of competition.[5] Europe reportedly is the most competitive region in both basic and mobile services. And more than half of Africa's markets are open to some form of competition.[6] Nearly every national telecommunications regulatory authority (NRA), then, serves a country in which there is competition at some state.

In the **OECD** countries, markets with healthy levels of competition have led the introduction of innovative services and appealing pricing packages. In some OECD countries, local loop unbundling changed the competitive landscape by allowing multiple providers to sell communications services over the same line.[7] Price decreases and improved services have been the most significant in markets characterized by intense competition. Consumers typically pay less for broadband than they did two years ago, while their connection speeds have generally increased.[8]

---

[3] *Enforcement Guidelines 2006* took into account the experiences, ideas, and views of roughly 100 people from 70 countries shared in written contributions and in meetings and seminars arranged by the ITU BDT, including a seminar and workshop co-hosted by **ANATEL,** the NRA for **Brazil.**

[4] *Domestic Enforcement Challenges and the Brazilian National Telecommunications Agency: **ANATEL** Contribution to ITU-D Question 18/1/1, April 2007* (**ANATEL** Contribution to ITU-D Question 18/1/1 (April 2007) *at 2*.

[5] *World Information Society Report 2007: Beyond WSIS*, International Telecommunications Union, United Nations Conference of Trade and Development, 2007 at 61.

[6] World Information Society Report 2007: Beyond WSIS, ITU, UNCTAD at 60-61.

[7] **OECD** Communications Outlook 2007, Information and Communications Technologies at 13, 14. Unbundling has been treated in various ways in OECD countries. For some countries that do not have cable networks, unbundling has proved an effective way of promoting competition, because in fact, there were few other alternatives. In countries that have a viable cable network, this has been less necessary as there is inter modal competition.

[8] *Id*. at 14.

For the time being, the majority of telecommunication operators in the OECD countries have moved closer to becoming all-in-one shops for voice, video and data.[9] They are evolving from voice providers into data and media companies in an effort to stem the losses from their traditional fixed line or traditional voice businesses.[10]

Most markets are competitive, but how do regulators enforce their competition policy? Are there common themes, or recurring dilemmas or challenges? How do NRAs enforce competition between incumbents and new competitors, between competing operators/infrastructure providers, between competing service providers?

3.2 Country Examples

In **Côte d'Ivoire**, the incumbent's monopoly ended on February 2, 2004. On July 7, 1995 Act 95-526 established the telecommunications code and the legal framework for the sector. The principle of fair competition can be found in Article 4 of the 1995 Act, and to implement this mandate, the statute contains certain minimum regulations that are supplemented by the terms of reference in the licenses of the incumbent operator and the new entrant licensed to provide fixed telephone service and telex service. [11] The 1995 legislation does not clarify the duties or role of the regulator in ensuring fair competition, so any issues relating to, among other things, abuse of dominant position are forwarded by **ATCI** to the Competition Commission, the entity responsible for settling competitive issues bearing on the national economy.[12]

Between 1996 and 2006, the regulator in **Côte d'Ivoire, Agence des Telecommunications de Côte d'Ivoire (ATCI),** authorized 8 mobile telephony networks, 15 Earth Stations, 28 VSATs (private use), and 27 ISPs. The Agency also granted 6 authorizations providing direct access to international, 9 authorizations for radio local loop networks, 13 authorizations to provide resale via prepaid cards, and 3 authorizations for payphones.[13]

Licensees in **Côte d'Ivoire** can provide any service open to competition so long as they abide by the rules of their authorization including non-discrimination, maintain cost accounting, avoid cross subsidies, and provide interconnection if technically compatible. They are also free to establish and change the price for their services.[14]

ANATEL, the NRA in **Brazil**, announced that it would subject a number of key items to public consultation including the framework for designation of significant market power, number portability, a wholesale access plan, migrating interconnection prices to a cost-based system, and rating the consumer's level of satisfaction with fixed, mobile, and pay TV services.[15] Following public consultation, rules governing the framework for designation of significant market power became official in 2007.[16] Additionally, the most recent advance in promoting competition has been the effort to enforce number portability in fixed and mobile telephony. As a result, consumers may keep their telephone number when switching mobile companies or fixed telephone in the same local area. This rule is currently 'official' and is in the process of being implemented before March of 2009.[17]

During the process of extending the concession contracts of wire line telephone service providers held from 2005, **ANATEL** reviewed and adjusted certain competitive aspects of these agreements. As a result of the negotiations, the service provider must, among other things, [promote] an attractive environment for

---

9 *Id*. at 19.

10 *Id*. at 23.

11 Contribution of **Agence des Telecommunications de Côte d'Ivoire (ATCI)** to ITU-D Question 18/1/1 (April, 2007) at 1 (Contribution of **ATCI** to Question 18/1/1, (April, 2007).

12 Contribution of **ATCI** to Question 18/1/1 (April, 2007) at 2.

13 *Id*.

14 *Id.*

15 Contribution of **ANATEL** to ITU-D Question 18/1/1 (April 2007) at 2.

16 *Id*. at 2.

17 *Id.* at 1, 2.

investment.[18] Incumbents were also required to organize and support a permanent Telecommunication Users Board that will handle consumer issues.[19]

The Telecommunications Regulatory Authority of **Lebanon** (**TRA Lebanon**) was established in 2002 under Telecommunications Law 431 and commenced operation in February 2007 after its four Board members were appointed by Ministerial Decree.[20] The agency is managed by its Chairman; each of the four Board members manages one of TRA Lebanon's four principal units: the Telecommunication Technology Unit, the Legal Affairs and Licensing Unit, the Market and Competition Unit, and the Information and Consumer Affairs Unit.[21]

With the exception of fixed telephony, **TRA Lebanon** intends to open the telecommunication sector to competition, and as of February 2008, was therefore working on a liberalization plan covering mobile telephony, international access, and data transmission networks. **TRA Lebanon's** market liberalization plan is part of a larger framework for the development of the Lebanese economy.[22]

A November 2007 decision of the Council of Ministers authorized **TRA Lebanon** and the *Haut Conseil pour la Privatisation* to launch a joint auction for the sale of two mobile telephone networks and two 20-year licenses. This project marked the start of sector liberalization and inaugurated competition.[23] As of February 2008, **TRA Lebanon** was working on a strategy to implement broadband transmission networks, and with the support of international companies in the framework of the "Partnership for Lebanon" to organize the market structure and standards framework and defining a clear regulatory environment. The goal is to issue broadband licenses in 2008.[24]

TRA Lebanon has published five regulation directives for consultation and comment with the public and other stakeholders: quality of service, interconnection, significant market power, (SMP), consumer affairs, and telecommunication equipment standards. Following completion of the public consultation, revision of these directives will mark an important step in advancing **TRA Lebanon'**s work to organize the telecommunications market in Lebanon.[25]

Competition was introduced in **Mali** in 2002.[26] Currently, there are two principal competitors: SOTELMA, a state-owned incumbent, and ORANGE Mali, a private company licensed to provide service in all segments of the market. In this context, the regulator, **Comité de Régulation des Télécommunications du Mali (CRT),** oversees enforcement of the telecommunications regulations and ensures compliance with the general conditions for operation of telecommunications networks and services.[27] **CRT** is supervised by the Minister for Telecommunications and is responsible for ensuring that the legislative and regulatory provisions relating to telecommunications are enforced.[28] **CRT** actively participated in the process of issuing the second operating license to ORANGE **Mali** (formerly Ikatel).[29]

CRT may only intervene when there is an imbalance in the sector and for the purpose of remedying shortcomings and facilitating competition. The agency must also keep in mind the need to fulfil the public

---

[18] *Id.* at 2.

[19] *Id*. at 3.

[20] Contribution of Telecommunications Regulatory Authority of **Lebanon** (**TRA Lebanon**) to ITU-D Question 18/1/1 (February 8, 2008) at 1. The Authority's corporate values are: (i) autonomy and independence; (ii) transparency; (iii) responsibility; (iv) fairness; and (v) efficiency. *Id.*

[21] *Id*. at 2

[22] *Id.*

[23] *Id.*

[24] *Id*. at 3.

[25] *Id*.

[26] Contribution by **Mali** to ITU-D Question 18/1/1 (June 27, 2007) at 2.

[27] On April 4, 2007, **Mali'**s Council of Ministers adopted a draft decree establishing **CRT**'s structure and methods of operation. This law abrogates the Decree of 10 May 2000, pertaining to CRT. *Id*

[28] Contribution by **Mali** to ITU-D Question 18/1/1 (March 7, 2007) at 2.

[29] Contribution by **Mali** to ITU-D Question 18/1/1 (June 27, 2007) at 2.

telecommunication service requirement of universal service.[30] Accordingly, **CRT** handles all matters relating to new market entrants through common law arrangements relating to networks and services.[31] Before any recourse to the courts, **CRT** offers conciliation and dispute arbitration between telecommunication operators, on their request. The mediation procedure cannot exceed two months. **CRT** also has recourse to the National Council for Competition.[32]

In the **United Kingdom**, the overarching philosophy adopted by the NRA **Ofcom** focuses regulation on areas where there are "durable competitive bottlenecks," enabling competition at the "deepest feasible level," and gradually withdrawing regulation everywhere else.[33]

Under the Telecommunications Regulatory Act No. 30/2002 (March 12, 2002), the Telecommunications Regulatory Authority (**TRA)** of **Oman** is authorized to implement the approved general policy for the telecommunications sector, prepare plans to develop the sector, and monitor licensees' implementation of the terms and conditions of their licenses. The **TRA** also determines which acts or events prevent competition, and will investigate complaints.[34] The **TRA** can also issue decisions settling conflicts among telecommunication operators and users. These decisions may be contested before the Administrative Court, according to the procedures specified in the law of the Administrative Judiciary Court. With the consent of the parties, the **TRA** can refer a dispute to an arbitrator, and if requested by one of the parties, can review that decision.[35]

As of March 2007, **Oman** had draft telecommunications amendments legislation pending that would give the **TRA** power to impose economic sanctions up to one million Omani Rials (USD $2,597,470) and administrative sanctions including license suspension and those specified in an operator's license that are supported by Executive Regulations. The draft Amendments would also give power to the courts to impose appropriate penalties.[36]

In **Chad,** it is the Ministry of Posts and New Communication Technologies (MPNTC) that prepares, implements, coordinates and oversees the government's policy on telecommunications and information and communications technology (ICTs).[37] Law Number 009/PR/98 promulgated in August of 1998 liberalized the market, created the regulatory body known as the **Office Tchadien de Régulation des Télécommunications (OTRT),** and created a national telecommunication operator. **OTRT** was established on May 22, 2000, two years following its creation.[38] In addition to the national fixed operator, there is a GSM mobile network operator that is a subsidiary of the incumbent, and two private GSM mobile network operators.[39]

The government of **Canada** began implementing a new regulatory approach for its telecommunications sector in 2007. In general, the country has accelerated its plan for deregulation and adopted a more flexible regulatory environment that is more dependent on market forces. A number of changes were made that affect: (i) how competition is managed and (ii) the requirements for a company to receive forbearance from regulation in a region. Several amendments and clarifications were also made to these rules after public consultation.[40]

---

30 *Id*.

31 *Id*.

32 *Id*. At 3.

33 *See Interconnection in an NGN Environment,* Background Paper, ITU April 15, 2006. http://www.itu.int/osg/spu/ngn/documents/Papers/Marcus-060323-Fin-v2.1.pdf at 7.

34 Contribution from **Oman** to ITU-D Question 18/1/1 (March 2007) at 1.

35 *Id*.

36 *Id*. At 2.

37 Contribution by **Chad** to ITU-D Question 18/1/1 (June 2007) at 2.

38 *Id*. at 3.

39 *Id*. at 2.

40 Global Insight (http://www.globalinsight.com) *Canada: First Residential Markets Deregulated in Canada; Complaints Commission Inaugurated*, Published July 26, 2007.

In Decision 2006-15, "Forbearance from the regulation of retail local exchange services," issued in April 2006, the Canadian government announced that it would change the **Canadian Radio-television and telecommunications Commission (CRTC)** framework on forbearance. Acting to implement this new approach in July 2007, the government of **Canada** established a consumer agency, assigned anticompetitive regulation to the Competition Bureau rather than the CRTC, redefined the Local Forbearance Regions as the local exchange, and changed the forbearance requirement to one which requires the presence of competing facilities rather than a drop of market share to below 75%. Forbearance can now be granted in any local exchange area in **Canada** where the facilities test is met.[41]

The Competition Bureau will now handle anticompetitive issues and reportedly will receive a C$10.5 million grant to fund its new activities in the telecom sector. This organization will reportedly release an enforcement bulletin on its approach to abuse of domination in telecommunications by the end of June 2007.[42]

Advancing deregulation, the **CRTC** announced that specific markets would receive forbearance from regulation under the new facilities-test regime. It was estimated that this group would cover areas that include some 60% of the population; mainly urban areas, where the return on infrastructure investment is greater and has proved more attractive to new competitors.[43]

Canada's old market share test required that the incumbent demonstrate that it had less than 75% of the market in order to receive forbearance. Now, under the facilities-based test, an applicant for forbearance must show that [three] facilities based operators owned by separate companies operate in an area servicing residential markets. For local business markets the requirement is set lower, at [two] such operators to receive forbearance. Incumbent carriers seeking forbearance must also demonstrate that they have met nine quality of service standards regarding wholesale access to competitors for six out of eight months preceding the application. Forbearance can also be sought based on the demonstration of market power according to the criteria laid down by the Competition Bureau.[44]

Within this new regime, prices for basic telephone service have been capped, and small competitors with less than 20,000 local exchange customers in Canada will be given at least 18 months to gain a foothold in the market.

The **Bangladesh** Telecommunication Regulatory Commission (BTRC) was established under the Bangladesh Telecommunication Act-2001 and began operating January 31, 2002. Prior to 2005, there were four mobile providers and one government owned telecommunications service provider. In 2005, BTRC issued 2 mobile licenses and 12 private PSTN licenses. Subscribers increased rapidly and prices were lowered, becoming more affordable. In 2007, BTRC opened the international gateway via the International Long Distance Telecommunication Service (ILDTS) Policy. Under this policy, BTRC issued 3 international gateway licenses, 2 interconnection exchange licenses, and one international Internet Gateway Service license. BTRC may cancel a license for a violation of the Telecommunication Act of 2001, regulations, or conditions in the licenses.[45] As a matter of practice, 30 days notice is given before enforcement action is taken.[46]

BTRC's broad objectives include encouraging orderly development of a telecommunications system that will enable and strengthen the social and economic welfare of Bangladesh; to ensure access to reliable, reasonably priced and modern telecommunication services and internet services; to ensure the efficiency of the national telecommunications system and its capability to compete in the national and international

---

41 *See* Global Insight (http://www.globalinsight.com) *Canadian Government Acts to Speed Up Deregulation*, Published April 5, 2007.

42 *Id*.

43 Global Insight (http://www.globalinsight.com) *Canada: First Residential Markets Deregulated in Canada; Complaints Commission Inaugurated*, Published July 26, 2007.

44 *See* Global Insight (http://www.globalinsight.com) *Canadian Government Acts to Speed Up Deregulation*, Published April 5, 2007.

45 Contribution of **Bangladesh** to ITU-D Question 18/1/1 (March 2009) at 2.

46 Question 18/1/1 Rapportuer's Group Meeting discussion, ITU Headquarters, April 2, 2009.

spheres; to prevent discrimination in providing telecommunications services; to progressively effect reliance on a competitive and market oriented system; to encourage a favorable atmosphere for local and foreign investors. One of BTRC's major functions is to protect the interests of consumers in access to telecom services, the quality, variety, and charges imposed; the privacy of telecommunications; and to prevent discrimination in service provision. Other functions include encouraging research, development, and innovation, collecting information on telecommunications and internet for analysis of its impact in **Bangladesh** and recommendations to the government; and developing and managing a national numbering plan.[47]

In the Union of **Myanmar**, the regulator (the Posts and Telecommunications Department, (PTD)) and the operator (Myanmar Posts and Telecommunications) exist under the policy directive of the Ministry. The government holds the exclusive rights to provide telecommunications services.[48] Myanmar Teleport, a semi-government ISP was formed in 2002 to provide data communications and IP-based services. Services offered include internet access, data, voice, and corporate VPN services. In the last decade less than 1000 km of fiber had been installed; currently up to 9000 km of nationwide fiber has been installed through major cities. With the opening of new International Gateway in Nay Pyi Taw, the new capital, MPT now has two international gateways. The Ministry of Railways also operates a national fiber cable.[49]

The Posts and Telecommunications Department (PTD) has the legal authority and experience to enforce **Myanmar**'s domestic telecommunications laws, rules, and regulations. PTD functions as a regulatory department in support of the Ministry in its policy making function; PTD provides legal and regulatory support to the Ministry. Five laws or notices have been issued to regulate the telecommunications and ICT sectors.[50] PTD is in the final stages of drafting a new telecommunications law. The main duties and responsibilities of PTD include:

1. Supervising the operation of telecommunications and posts;
2. RF Spectrum management;
3. Coordinating and cooperating with international organizations;
4. Issuing and regulating telecommunications licenses and related certificates;
5. Studying emerging telecommunications technology to advise respective authorities;
6. Supervising the production, import, export, sale and use of telecommunications equipment within Union of Myanmar.

In addition, the Communication Policy Supervisory and Working Committee meets regularly with relevant Ministries to discuss with regulatory issues, and the **Myanmar** National Digital Broadcasting Committee has been established.[51]

3.3 Country Examples (Internet and VOIP)

Article 13 of **Côte d'Ivoire'**s 1995 Act requires companies that wish to provide Internet service to obtain prior authorization from **ATCI** where the total access capacity of the leased lines exceeds 2.1. Mbits.[52] For operators offering service below that threshold, a simple declaration is sufficient. Since 1996, **ATCI** has issued 27 authorizations for commercial service, nine of which are currently operational.[53]

Anatel (**Brazil**) grants a Multimedia Communications Service license to companies that wish to provide infrastructure for Internet access. As of 2008, there were 919 companies authorized to provide multimedia

---

47 Contribution of **Bangladesh** to ITU-D Question 18/1/1 (March 2009) at 1 - 2.

48 *Regulatory Function in **Myanmar***, Contribution to ITU-D Question 18/1/1 (February 2009) at 2.

49 *Id* at 4.

50 See Id., The **Myanmar** Telegraphy Act; the **Myanmar** Wireless Telegraphy Act; the Electronic Transaction Law; the Computer Development Law; and the Notification on Wide Area Network Establishment and Provision of Services.

51 *Id*. at 3.

52 Contribution of **ATCI** to Question 18/1/1 (April, 2007) at 4.

53 *Id*. at 5.

services.[54] In addition, every person and company may access the Internet in **Brazil**, if connected to the network through a provider. There is no censorship, though material posted must respect the Federal Constitution and national laws. The Federal Constitution of 1988 establishes criteria applicable to electronic social communications media. Article 222, Section 3 provides that all media, independent of the technology used, must respect principles of broadcasting production and programming provided for in Article 221 (educational, cultural, informational, and artistic, promotion of regional and national culture, respecting ethical and social values).[55] Inter-ministerial Ordinance no 147, (5/31/95), altered by Presidential Decree no 4829 (9/3/03) created the **Brazil**ian Internet Steering Committee or CGI (Portuguese) which is responsible for promoting technical quality, innovation, and dissemination. The CGI is made up of 21 members: 9 federal government representatives, 4 corporate representatives, four representatives elected by entities registered in CGI; 3 representatives of the scientific and technological community and one Internet expert.[56]

In order to provide internet access in **Mali**, approval must be obtained from one of the operators, not from **CRT.** VoIP may not be offered by any entity other than the state-owned incumbent and the other licensed (private) operator.[57]

VOIP calls within **India** are restricted to IP equipment and cannot be made from a PC or VOIP handset to a telephone.[58]

The **United Kingdom's Ofcom** adopted a code of practice for voice-over-Internet-protocol (VoIP) service providers that rests on informing customers about their service offerings, and any potential limitations, rather than regulating the services or mandating functionality. Ofcom is planning a further consultation to examine whether to mandate access to emergency services.[59]

Ofcom's code, released in March 2007, requires VoIP providers to make clear whether the service includes access to emergency services; the extent to which the service depends on the user's home power supply; whether directory assistance, directory listings, access to the operator, or itemization of calls are available; and whether consumers will be able to retain their number if they switch service providers.[60]

Further, if the service does not include emergency services or relies on an external power supply, the VoIP provider is also required to obtain the customer's "positive acknowledgment of this at the point of sale;" to label the capability of service, either on the equipment or through information on the computer screen; and play an announcement each time a call to emergency services is attempted, reminding the caller that the service is not available.[61]

In Section 230(b) of the Communications Act of 1934, as amended (the Act)[62], the **United States** Congress adopted its national Internet policy. Specifically, Congress stated that it is the policy of the United States to "preserve the vibrant and competitive free market that presently exists for the Internet" and to promote its continued development.[63] In section 706(a) of the Act, Congress charged the **Federal Communications**

---

[54] ***Brazil****ian Overview on Consumer Protection, Network Security and Internet,* Contribution to ITU-D, Question 18/1/1 (20 August 2008) at 3.

[55] *Id*. at 4.

[56] *Id*.

[57] Contribution by **Mali** to ITU-D Question 18/1/1 (June 27, 2007) at 3.

[58] **OECD** Communications Outlook 2007, Information and Communications Technologies at 291.

[59] *See, **Ofcom** Relies on Information, Not Rules, for VoIP Code, Sees no Net Neutrality Problem*, Telecommunications Reports Daily, www.tr.com March 30, 2007.

[60] *Id*

[61] *Id*

[62] 47 U.S.C §230(b)(2)

[63] 47 U.S.C §230(b)(1)

Commission with "encouraging the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans.[64]

Consistent with those Congressional directives, and subject to reasonable network management, the FCC adopted a policy statement outlining the following principles to encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet:

- Consumers are entitled to access the lawful Internet content of their choice.
- Consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.
- Consumers are entitled to connect their choice of legal devices that do not harm the network.
- Consumers are entitled to competition among network providers, applications and service providers, and content providers.[65]

In March of 2007 the 8th circuit court of Appeals upheld a decision by the **United States** Federal Communications Commission (**FCC**) that barred states from regulating Internet-based phone services. A three-judge panel of the 8th Circuit Court of Appeals agreed with the FCC's determination in 2004 that companies like Vonage Holdings Corp provide an interstate service that puts them outside state control. The court agreed with the FCC's determination that the nature of VOIP telephone calls allows customers to place "home" phone calls from nearly anywhere, irrespective of state lines.[66]

In an action overruling **CRTC** and the first in a decade and only the 23rd such use of the government's powers since 1976, the **Canadian** government in November 2006 announced that VoIP services were no longer to be regulated as standard telephony service. This decision applied to access independent VoIP services only, and did not affect facilities based VoIP services that do not require a broadband connection. Consequently, incumbent telcos can offer VoIP at unregulated prices.[67]

In the **United States**, blocking of VoIP traffic ports by Madison River Communication, LLC, was stopped by a consent decree and a $15,000 contribution. Blocking voice service was regarded as prohibiting VoIP as a viable voice option for customers. Compliance was required by Section 201(b) of the communications act, which mandates customers' ability to use VoIP over one or more service providers.

3.4 Challenges Identified

- Abuse of an incumbent's dominant position.
- NRA does not have authority to enforce market/competition issues.
- Legislation is inadequate, incomplete or otherwise flawed: no authority to issue regulations unless reviewed by the Ministry of Legal Affairs; no authority to prosecute cases, impose fines or other penalties.
- Absence of legislation governing the duties of the regulator to ensure fair competition, including what to do about abuse of dominant position.
- Does not in all cases have ability to enforce its decisions, incumbents or other players have succeeded in overturning decisions or delaying implementation.
- Regulator's mediation powers need to be strengthened.
- New Regulator is inexperienced, unseasoned, outmatched by experienced players in the market. New regulator begins its mission in an environment that has already been mastered by operators,

---

[64] *In the Matters of Appropriate Framework for Broadband Access to the Internet over wireline facilites CC Docket No 02-33 et al, FCC 05-151, released September, 2005, citing* 47 U.S.C. §157 nt. (incorporating section 706 of the Telecommunications Act of 1996, Pub. Law No. 104-104, 110 Stat. 56 (1996)).

[65] *In the Matters of Appropriate Framework for Broadband Access to the Internet over wireline facilites CC Docket No 02-33 et al, FCC 05-151, released September, 2005 at 3.*

[66] *See*, *Court Backs **FCC** over State Bids to Regulate Web Phones*, Associated Press, March 22, 2007.

[67] *See* Global Insight (http://www.globalinsight.com) *Canada: VoIP Prices Deregulated,* Published November 20, 2006.

licensees and owners of independent networks (embassies, international organizations, and others). Decisions are not respected.

- Some countries have competition commissions that seem to share jurisdiction with the NRA over competition issues.
- Rapid evolution of telecom & ICT; convergence makes the regulator's job more difficult.
- How to improve the co-existence of the Competition Commission and the NRA.
- Blind battle between powerful incumbents; less established ISPs are the casualties; they are sidelined or excluded altogether.
- At times both the new competitors and the NRAs are dwarfed by the power of the incumbent.
- No clear regulatory framework for Internet services.
- Inadequacy or unavailability of broadband service.

3.5 Guidelines

- Focus regulation on persistent or unyielding competitive bottlenecks; gradually withdraw regulation elsewhere.
- Negotiate and incorporate terms that are favorable to competition in concession agreements; use renewal periods accordingly.
- Clearly inform operators of the practices that constitute unfair competition in the sector.
- Conduct a public inquiry involving all stakeholders on telecom and ICT national interests, including competition.
- The Regulator must make its needs and priorities absolutely clear to the country's authorities.
- Establish strategic partnerships with experts in developed and in other developing countries for training on regulatory matters including competition.
- Conduct an awareness campaign directed at all administrators and politicians explaining the role and validity of the NRA.
- Institute a National Competition Council.

4 Enforcing Interconnection Laws, Policy, Regulation

4.1 Overview

With recent technological developments the range of services that depend on interconnection has increased. In addition to the more 'traditional' local, long distance, international fixed and mobile voice services, interconnection is also an essential input for satellite, Internet, e-mail and message services, fixed and mobile broadband data transmission, and a wide range of multimedia services.[68] Interconnection of communications networks is now routinely practiced across the globe, and convergence – the move to digital networks -- has accelerated the pace, need for, and thus acceptance of an expanding array of interconnection arrangements, which are widely recognized as beneficial to interconnecting carriers, consumers, and end users.

One of the key issues in ensuring fair competition and a level playing field is a fair and transparent interconnection regulatory framework. Establishing and implementing such a regime, however, can place significant demands on a country's legal and administrative infrastructure.[69]

Reportedly, transparency in interconnection agreements is highest in the Americas, Asia-Pacific, and Europe. Worldwide, nearly 60 percent of countries do not make interconnection agreements public, although about 58 percent make pricing information available.[70]

---

[68] *See generally*, *info*Dev/ITU Interconnection Toolkit) at 13.

[69] *info*Dev/ITU ICT Regulation Toolkit, Module 2: Competition, Interconnection and Price Regulation (Executive Summary/NERA, Kalba) January 17, 2007 (*info*Dev/ITU Interconnection Toolkit) at 36.

[70] *Trends in Telecommunications Reform 2006*, International Telecommunication Union, at 10.

As one of the most essential features of competition, and a critical component of achieving universal access, many countries mandate interconnection at technically feasible points in a given network and permit the NRA to intervene if the parties themselves cannot reach agreement on the terms. The interconnection directives of the **European Union** (EU), for example, allow NRAs to impose interconnection or unbundling obligations on carriers that have significant market power where the NRA believes that either denial of access or unreasonable terms and conditions having a similar effect would undermine a sustainable competitive market at the retail level, or would not be in the end-users' interest.[71]

4.2 Country Examples

In **Côte d'Ivoire**, the interconnection agreement is negotiated between the parties, and must be submitted to ATCI for approval prior to signature and execution.[72] **Côte d'Ivoire**'s Act makes no provision for interconnection. It is through the terms of reference of the two licensees that the framework for interconnection is organized.[73] Licensees are required to provide interconnection to any authorized operator requesting it. While adhering to transparency and non discrimination principles, the operator must provide a contract containing the technical, financial, and administrative conditions for service provision. Technical clauses describing the planning and operational aspects of interconnection are housed in an annex to the interconnection agreement. **ATCI** will intervene where there are contradictory terms in the licensee's terms of reference and when there is no response from the licensee to a request for interconnection for 60 calendar days.[74] At 3. **ATCI** also reviews and approves interconnection tariffs.

In **Botswana** all telecom service providers have the right to interconnect their licensed systems to the licensed systems of other telecom service providers. The right to interconnection exists only on condition that the technical standards and specifications for interconnection have been complied with.[75]

In **Mauritania,** the decree of 31 December 2000 (decree no. 2000-163) covers general interconnection conditions for telecommunication networks. The Regulatory Authority ensures that interconnection with major suppliers is possible, at all network points where this is technically feasible, in a timely fashion and under non-discriminatory terms and conditions. The cost of providing the infrastructure must be born by the requesting party. Public network operators and service providers must, according to their license, publish an interconnection catalogue, including a reference set of technical specifications and tariffs for interconnection. A request for interconnection may not be turned down if it is reasonable and the operator is able to meet the request. A refusal must be substantiated.[76]

In **Switzerland**, the *Loi sur les télécommunications* requires both facilities interconnection and interoperability of services of all telecommunication service providers. The price of interconnection is determined entirely by the parties themselves. A dominant service provider must provide interconnection under transparent and non-discriminatory conditions and at a cost oriented price. In principle, prices are fixed by means of commercial agreements between the parties, however, if the parties fail to agree, *ex post* price regulation ensues and the national regulatory authority may be asked to intervene.[77]

4.3 Challenges Identified

- Absence of clear regulatory framework governing interconnection;
- Operators' failure to perform cost accounting makes it difficult to verify the accuracy of the financial data provided.
- Lack of transparency and access to information;[78]

---

71 *Id*. at 14.

72 Contribution of **ATCI** to Question 18/1/1 (April, 2007) at 3.

73 *Id*. at 2

74 *Id*. at 3.

75 Contribution of **Botswana** Telecommunications Authority (BTA) to GSR 2008, at 3.

76 *See* Contribution of **Mauritania** to GSR 2008, at 1.

77 **OFCOM, Swiss** Federation Contribution to GSR 2008, at 1.

78 *Id*.

- Unavailability of a financial calculation model for determining costs and tariffs.
- Unavailability of financial data for a complete financial period in time for annual tariff review.
- The physical state of telecommunications networks;[79]
- The presence of powerful state-owned operators in the market that are not subject to competition and are unwilling to lower interconnection rates.
- Difficulty establishing and administering dispute resolution mechanisms;
- Call blocking;
- Relatively high interconnection rates;

4.4 Guidelines

- In an open and competitive market, permit operators to negotiate access and interconnection arrangements between themselves.
- Operators which receive requests for access or interconnection should in principle conclude such agreements on a commercial basis, and should negotiate in good faith.[80]
- In markets where there continues to be large differences in negotiating power between undertakings, and where some undertakings rely on infrastructure provided by others for delivery of their services, provide NRAs with sufficient power to secure, where commercial negotiation fails, adequate access and interconnection and interoperability of services in the interest of end-users.[81]
- NRAs can publish Reference Interconnection Offers or model interconnection agreements on their website to help ensure that all competitors are aware of terms and conditions.[82]
- An interconnection agreement should include:[83]
  - **Price.** Define the initial level of interconnection charges, the currency in which they will be paid, and how prices will adjust over the term of the agreement to account for exchange rate changes and inflation. Define liability for bad debt and uncollectible bills.
  - **Points of interconnection**. Define the physical locations where interconnection will take place and the technical standards to be employed. Establish a process for requesting and obtaining additional points of interconnection.
  - **Transport charges and traffic routing**. Define the proper routing and hand-off point for each type of call, as well as the applicability of transport charges in the receiving network for calls that must be carried beyond the area local to the point of interconnection.
  - **Quality-of-service standards**. Define quality standards, particularly the time to provide circuits and for call blocking levels. Define the remedy for when those standards are not met. Testing opportunities should be provided to each party.
  - **Billing and collection.** Define when and how to collect traffic data, exchange bills, and make payment. Develop a process for reconciling traffic data and making inquiries to the other party, and for handling claims.
  - **Traffic measurement and settlement.** Define the responsibilities of each interconnecting operator to measure traffic along with settlement procedures to resolve discrepancies. Specify obligations to cooperate in fraud detection and enforcement activities.
  - **Numbering resources**. Define each operator's access to the country's numbering plan and numbering resources.

---

[79] InfoDev/ITU ICT Regulation Toolkit, Module 2: *Competition, Interconnection and Price Regulation* (Executive Summary/NERA, Kalba) January 17, 2007 at 36.

[80] *See, e.g.*, Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) at 5.

[81] *Id*. at 6.

[82] *See Trends in Telecommunications Reform 2006*, International Telecommunication Union, at 10.

[83] *See generally*, InfoDev/ITU ICT Regulation Toolkit, Module 2: *Competition, Interconnection and Price Regulation* (Executive Summary/NERA, Kalba) January 17, 2007, Section 3.2.4.

  - **Forecasting network needs**. Develop and define a process for interconnecting operators to plan, agree, budget for, and install additional capacity to meet forecasted demand. Define procedures to resolve differences over forecasts, as well as what constitutes a bona fide request for additional interconnection capacity. At a minimum, include a mutual obligation to notify the other party well in advance of network changes and upgrades to avoid disadvantaging one competitor over another.
  - **Access to customer information**. Define limits on the permitted uses of this information particularly regarding marketing activities approaching another operator's clients based on information obtained through interconnection activities. Include safeguards to protect customers' privacy.
- Interconnection pricing should:
  - encourage efficient competition and the efficient use of, and investment in telecommunications networks;
  - preserve the financial viability of universal service mechanisms
  - treat technologies and competitors neutrally;
  - allow innovation; and
  - whenever possible, minimize regulatory intervention.[84]

5 Enforcing Site (network infrastructure) Sharing

5.1 Overview

Both developing and developed countries share the goal of network deployment and expansion; thus NRAs around the globe are keen to promote, stimulate, and expand broadband networks and services. By some accounts, as of 2006, a majority of fixed broadband subscribers (38.8%) resided in Asia-Pacific; Europe/CIS had 31.8%; 28.7% resided in the Americas; .09% could be found on the continent of Africa; and .06% in the Arab States.[85] Collectively seeking to improve these percentages, NRA's worldwide have begun to examine the role that sharing network infrastructure could have in promoting broader and more affordable access to telecommunications services, and particularly as a tool to promote IP backbones and broadband access networks. This was the theme discussed at the 2008 ITU Global Symposium for Regulators (GSR).[86]

At the outset it is worthy to note that the term 'infrastructure sharing' often mixes under one umbrella practices that can be very different – and which have distinct consequences. For instance, discussions of this topic have included both interconnection and unbundling – terms that are well known, related, yet distinct. In this context, for example, it has been suggested that interconnection can be considered a less interventionist form of infrastructure sharing than local loop unbundling.[87] The term has also covered sharing physical plant – ducts, manholes, trenches, conduits. The case of access to submarine cables, on the other hand, provides a relatively clear example of active network infrastructure sharing; as such cables are almost always constructed for the express purpose of sharing capacity.

In general, two classes of sharing tend to be discussed: passive and active. "Passive" sharing refers to operators sharing the non-electrical, civil engineering elements of telecommunications networks – rights of way/easements, ducts, pylons, masts, trenches, towers, poles, equipment rooms and their related power supply, air conditioning, and security.[88] "Active" sharing refers to operators sharing transmission links,

---

[84] *info*Dev/ITU ICT Regulation Toolkit, Module 2: Competition, Interconnection and Price Regulation (Executive Summary/NERA, Kalba) January 17, 2007 (*info*Dev/ITU Interconnection Toolkit.

[85] *See,* ITU Trends in Telecommunications Reform 2007, ITU Geneva, at 47.

[86] http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR08/index.html.

[87] *See generally*, *What Do We Mean by 6 Degrees of Sharing?,* 2008 GSR Discussion paper, S. Schorr, ITU, February 2008, at 6 (*6 Degrees,*. Schorr, ITU, February 2008)

[88] *What Do We Mean by 6 Degrees of Sharing?,* 2008 GSR Discussion paper, S. Schorr, ITU, February 2008 at 5.

satellite earth stations, switches, submarine cable landing stations,[89] base stations and Node B's for mobile networks, and access node switches and management systems for fiber networks.[90]

Regulators at the 2008 GSR recognized that certain sharing options can deliver specific benefits[91] while others can pose risks, including, most significantly, by reducing competition and incentives for investment.[92] Therefore, they concluded, when designing the most appropriate regulatory strategy for a given country, anticipated benefits and potential harm must be carefully balanced in light of the specific national circumstances. In so doing, they noted, it is important to hold public consultations with all stakeholders.[93]

The Telecommunications Regulatory Authority of the **Kingdom of Bahrain** takes the position that sharing passive network elements (e.g., rights of way, ducts, masts) is less likely to lessen the degree of competition than sharing in more active levels of service provision (e.g., sharing active networks and services (including national roaming). Accordingly, in its contribution to the 2008 GSR, TRA **Bahrain** recommended a two-tier strategy in which regulatory policy would clearly encourage sharing works, rights of way and passive infrastructure (e.g., ducts, masts, towers), while sharing other levels of service provision would be treated with caution and seen as conditioned transitional arrangements designed to achieve specific objectives.[94]

Most countries that have relied on competition as the most efficient means to deliver innovative, affordable communications services to their consumers and end users, have taken deliberate action to ensure that there is competition in infrastructure. Fully intending to depart from what was often a state-owned monopoly market structure, regulatory actions in these countries were geared toward enabling multiple, facilities-based service providers to enter the market. Many countries have noted that they promote or engage in sharing to further advance a competitive marketplace for the benefit of consumers and end users. To promote competition by eliminating bottlenecks associated with essential facilities must be balanced with the objective to provide sufficient incentive for operators to invest in next generation networks.

It appears that a majority of countries do not mandate active sharing requirements, at least for broadband services, many require sharing only as it relates to passive infrastructure, (ducts, towers, masts) some require active sharing of copper networks, and a few require sharing of both active and passive communications infrastructure. In deciding on their course of action, almost all countries consider the level of market power of the operators, the presence of bottlenecks in essential facilities, and the effects sharing would have on competition, the environment, and investment incentives.

5.2 Country Examples

In **Malta,** traditional concepts of access and interconnection have been fully implemented as mandated by the European Directives, however other forms of what is called infrastructure sharing, such as facility or site sharing, have not been mandated, but have been left up to negotiation between the operators and service providers. Considering the specific circumstances of the country, the **Malta** Communications Authority has deemed mandatory requirements of this kind to be too onerous an obligation to be placed upon its operators.[95]

Similarly, in the **United States,** robust facilities based competition and the corresponding lack of market power by any one provider has minimized a need to mandate active or passive infrastructure sharing for broadband services. In this country, for example, the market has driven passive infrastructure sharing in a

---

89 Infrastructure Sharing Strategies from the Perspective of **Brunei Darussalam**, GSR 2008 at 1-2.

90 *6 Degrees*. Schorr, ITU, February 2008 at 5-6.

91 Benefits can include greatly reduced capital and operating expenses and associated long term efficiencies, faster deployment of networks, and reduced disturbance of the environment. *See generally*, Contribution of the Telecommunications Regulatory Authority of **Bahrain** to GSR 2008 at 1.

92 This in turn is likely to reduce network expansion, diminish service offerings to consumers, and facilitate collusion among competitors. S*ee generally, Id.* at 2.

93 ITU GSR 2008 Best Practice Guidelines on Infrastructure Sharing, at 1.

94 Contribution of the Telecommunications Regulatory Authority of **Bahrain** to GSR 2008 at 2.

95 *See,* Contribution of **Malta** to GSR 2008 at 1 – 2.

trend towards third party ownership of towers used for mobile cellular service and other wireless services. This, in turn has led to such towers hosting equipment for multiple operator's networks.[96]

India is one of the leaders promoting mobile tower sharing. This country grants subsidies from its universal service fund to encourage network rollout to rural areas where towers are shared by at least three competitive operators.[97]

Article 36 of the Telecommunications Law of **Lebanon** requires service providers to make their infrastructure available to other providers. As of March 2008, consultations were on-going in Lebanon on various regulations dealing with infrastructure sharing. The Telecommunications Regulatory Authority of **Lebanon** (TRA Lebanon) intends to promote infrastructure sharing of the civil engineering and non active elements of the network (e.g., towers, masts, ducts, and conduits) in areas where it is not economically sustainable for multiple operators to build infrastructure and where environmental and social concerns are particularly important (e.g., to reduce the proliferation of mobile network masts and limit disruptive civil works). In undertaking these activities, TRA **Lebanon** intends to rely as much as possible on market incentives for such arrangements.[98]

Going forward, TRA **Lebanon** intends to coordinate with government utilities such as power and transport to identify opportunities to obtain rights of way and horizontal corridors that may be used by telecommunications service providers.[99] They are also considering using licensing and network deployment "windows" during which service providers would undertake joint build-outs, and timed organized opportunities for joint access to ducts and conduits to lay fiber. Another option they are considering is to establish an 'infrastructure sharing desk' that would facilitate coordination of trenching and ducting works between telecom service providers and between telecom service providers and other utilities.[100]

In **Mauritania**, all operators must study the possibility of sharing with other operators, specifically leasing infrastructure such as ducts, pipes, drains, terraces of buildings and radio tower locations. Where infrastructure is shared, the regulatory must receive a copy of the sharing agreement and monitors its conditions.[101]

The Telecommunications Regulatory Act of the **Sultanate of Oman** promulgated by Royal Decree 30/2002 addresses access to and sharing telecom facilities by telecom licensees in **Oman**. Under the Act, dominant carriers must make their facilities -- those determined by the regulatory authority – available to other operators on reasonable and fair conditions. Every licensee is entitled to use infrastructure such as towers, ducts, pipes, cable channels, and telecom exchange buildings. Licensees may negotiate with dominant operators for access but if no agreement is reached, a party may request that TRA **Oman** intervene and fashion a resolution.[102]

In 2005, a new mobile entrant complained to TRA Oman that it could not reach an agreement on the technical conditions of site sharing with the dominant mobile operator, Oman Mobile. TRA **Oman** investigated the claim and subsequently announced *Site Sharing Guidelines* mandating sharing masts, towers, and roofs. The guidelines also included technical conditions for horizontal and vertical antenna separation, cost, safety conditions, and a deadline to meet the sharing request.[103]

Portugal was one of the first European Union member States to compel the incumbent operator to have a regulated offer for access to conduits. Pursuant to Article 7 of the Bases of Concession approved by Decree-Law n. °31/2003 of 17 February, the concession agreement of the telecommunications service provider guaranteed access by other operators to the conduits associated with the basic telecommunications network.

---

96 **USA** Contribution to GSR 2008, at 1.

97 *What Do We Mean by 6 Degrees of Sharing?* S. Schorr, ITU GSR, February 2008 at 6.

98 TRA **Lebanon** Contribution to GSR 2008 at 1 – 2.

99 *Id*. at 3.

100 *Id*. at 4.

101 Contribution of **Mauritania** to GSR 2008 at 1.

102 Contribution of the Telecommunication Regulatory Authority of **Oman** to GSR 2008, at 1.

103 *Id*. at 1 – 2.

Additionally, under Law n° 5/2004 of 10 February, the incumbent has a duty to provide, by agreement, access to conduits, poles, other equipment and facilities it owns or manages, and must provide an offer of conduit access which includes the conditions for access and use.[104]

Beginning in 2004, **ICP-ANACOM** established the general principles and requirements for access to pipes; the main elements that must be included in a Reference Conduit Access Offer (RCAO) including price, deadlines and standard procedures. The law also requires the incumbent to leave an area corresponding to at least 20% of the internal area of each conduit for use by other entities. The agency also required the incumbent to maintain and update a database describing the conduits and associated infrastructure.[105]

To stimulate flagging competition, in April 2007 **Switzerland**'s dominant operator was required to provide its competitors with fully unbundled access to the local loop, at cost based rates; to provide bitstream access for four years; and to provide access to cable ducts. As in the **United States**, the obligation to unbundle the local loop and bitstream access only applied to the copper network, so these measures only affected the incumbents plain old telephone (POTs) network. The obligation was limited in this way, in order to give the incumbent an incentive to invest in fiber.[106]

In **Germany**, access to cable ducts is imposed as an ancillary service like collocation. As a consequence of the duty of Germany's Federal Network Agency to review every two years the market conditions and obligations imposed upon entities with significant market power, the obligation of Deutsche Telekom AG to provide access to the local loop at the main distribution frame or at a point closer to the end user (e.g., street cabinet) was maintained. In addition, Deutsche Telekom will have to open up to competitors its cable ducts between the main distribution frame and the cable distributors, so that competitors can connect local loops to their own fiber optic cable infrastructure for broadband service. If access to the cable duct is not technically possible or if there is inadequate capacity, Deutsche Telekom must provide access to dark fiber. This approach has been supported by the European Regulator's Group.[107]

In **France** ARCEP requires direct access to France Télécom's copper pair – deemed essential infrastructure – via unbundling, to enable third-party operators to provide DSL services. ARCEP has also required France Télécom to implement a wholesale bitstream offer that provides "activated" access facilities at a given regional point.[108] Recently, ARCEP proposed to require access to France Télécom's ducts so that alternative operators can invest in fiber to the home networks. In anticipation of such regulation, France Télécom contacted alternative operators in late 2007 with a preliminary offer for access to its ducts. This offer is currently under evaluation.[109]

The primary objectives for infrastructure sharing in **Brunei Darussalam** are to promote competition in the telecommunications market, lower costs, maximize geographical coverage, and avoid unnecessary duplication of infrastructure. Brunei Darussalam has designated both active and passive infrastructure to be shared, including masts, ducts and manholes, submarine cable landing stations, satellite earth stations, and switches.[110]

The **Botswana** telecommunications Authority mandates facility sharing mainly through telecom service provider licenses. Licenses issued to operators in **Botswana** require that licensees offer other service providers access to essential facilities, which are defined as any circuit, switch, tower, site duct or other facility owned or operated by the licensee, which other operators wish to use and for which there is no feasible technical or economic substitute or other satisfactory environmental solution. Any telecom services provider in **Botswana** who is in need of essential facilities may request the same from any other telecom service-provider, so long as the facilities are available and the requesting party is able to comply with the technical standards and specifications for access. The hosting party must clearly state the technical standards

---

[104] "Infrastructure Sharing Strategies," Contribution of **Portugal** to GSR 2008 at 1.

[105] *Id.* at 2.

[106] Contribution of OFCOM (**United Kingdom**) to GSR 2008 at 1.

[107] Contribution of the Federal Network Agency (**Germany**) to GSR 2008.

[108] Contribution of ARCEP (**France**) to GSR 2008 at 1.

[109] *Id*. at 2.

[110] Contribution of **Brunei Darussalam** to GSR 2008 at 1 – 2.

and specifications. Prices charged to share facilities, especially for those deemed essential, must be cost oriented.[111] BTA seeks to ensure that facility sharing is not used as a platform for collusion by operators.[112]

Among other things, the government of **Côte d'Ivoire** envisions a common infrastructure shared by fixed and mobile operators. It has established the *Fonds National des Télécommunications* to subsidize operation in rural areas and provide investment for shared infrastructure. The fund is governed by a management board and technical board. All authorized operators contribute with a connectivity fee of two percent of gross revenue.[113]

5.3 Challenges Identified

As observed by a number of NRAs, deploying new networks requires massive investment. Often operators must make further investments for next generation networks even before recouping their investment in existing infrastructure. Fiber optic networks require extensive duct infrastructure, and new wireless networks require towers and masts. Civil engineering works, particularly installation of underground ducts and cable connection facilities constitute the main cost. Construction and land use costs thus constitute a substantial proportion of total cost of network build-out.[114]

In **Bolivia,** a bottleneck has occurred for infrastructure development in mobile service for a number of reasons, particularly because there are different legal frameworks in different parts of the State, and different regulatory frameworks in the telecommunications sector, municipal governments, and the Vice-Ministry for the Environment, all of which have authority over some aspect of tower sites. It is not clear which entity has the authority to give the ultimate approval. In response, the *Superintendencia de Telecommunicaciones* approached municipal governments, the Vice-Ministry of Telecommunications and the Vice-Ministry for the Environment to coordinate and implement activities for sustained infrastructure development. Steps were taken to draft, approve, and promulgate clear rules governing tower and antenna sites, and in July 2007 clear rules to facilitate infrastructure development were established within the municipal laws of two of Bolivia's towns.[115]

Cameroon, which states that it manages its infrastructure as a natural monopoly, observes an imbalance in the geographical distribution of infrastructure, inequality in access to telecommunication services throughout the country, a national digital divide, a failure to exploit the benefits of economies of scale, and high tariffs. In response, the regulator launched consultations with operators from the telecom sector and operators of other networks (e.g., railways, broadcasting, electricity). The consultations resulted in signing a "Framework Agreement on the operation of telecommunication infrastructures."[116]

The incumbent operator in **France** and the main alternative operators have begun deploying fiber to the home (FTTH) networks. Faced with new problems generated by the deployment of such costly networks ARCEP intends to introduce regulations favoring infrastructure-based competition, as well as seeking, to the greatest extent possible, a significant degree of investment sharing among operators. Paris has a network of accessible sewers through which fiber optic cables can be drawn to each building. With the exception of Paris, however, there is no existing civil engineering infrastructure apart from the ducts which France Télécom inherited from the former monopoly.[117]

---

[111] Contribution of **Botswana** Telecommunications Authority to GSR 2008 at 3 – 4.

[112] *Id*. at 1.

[113] Contribution of **Côte d'Ivoire** to GSR 2008.

[114] See generally, Contributions of the Telecommunications Regulatory Authority of the Kingdom of **Bahrain** to GSR 2008, Contribution of **Brunei Darussalam** to GSR 2008, and Contribution of ARCEP (**France**) to GSR 2008.

[115] Contribution of **Bolivia** to GSR 2008 at 1.

[116] Contribution of **Cameroon** to GSR 2008 at 1-2.

[117] *See generally* Contribution of ARCEP (**France**) to GSR 2008 at 2.

5.4 Guidelines

NRAs participating in the 2008 ITU Global Symposium for Regulators agreed upon and produced ***Best Practice Guidelines on innovative infrastructure sharing.***[118] The GSR 2008 guidelines adopted are summarized below, and are shown here with closed bullets. Many submissions to the **consultative process** by participating NRAs suggested additional guidelines that may prove useful to some countries and are also listed below with open bullets.

- It is important that implementation of sharing takes into account the necessity to protect the value of existing investment in infrastructure and services.
- [O]ffering shared facilities must not be biased towards any specific service provider or types of services.
- [R]egulatory policy [should] not prevent competing market players from installing their own independent facilities.
- Regulatory policy] …should promote open access to international capacity and international gateways.
- [E]stablishing Internet Exchange Points could also encourage shared and more affordable access to national and international broadband capacity for Internet service providers willing to enter the market.
- Pricing for shared facilities should help operators make reasonable and commercial "build-or-buy" decisions; it should provide an incentive for investment in infrastructure, but should not act as an artificial barrier to entry for new market players.
- Non-replicable resources such as towers, ducts and rights of way can be shared for installations that serve a similar purpose.
- Shared-use [spectrum] bands could be promoted as long as interference is controlled.
- Regulators could consider licensing or authorizing market players that only provide passive network elements, but which do not compete for end-users, (e.g., mobile tower companies, fiber backhaul providers).
- [I]nfrastructure sharing [must] take place on a neutral, transparent, fair and non discriminatory basis
- [I]nterconnection frameworks can ensure that all licensed operators ...can…interconnect …and can … encourage the sharing of essential facilities.
- Establishing a 'one-stop-shop' would facilitate … coordination of trenching and ducting works between telecommunications service providers [and] …between telecommunications service providers and those of other utilities.
- [T]ransparent processes [are required] to facilitate infrastructure sharing, and market players need to know what is available for sharing under clearly established terms and conditions. [This could be facilitated by website] publication of existing [and] future infrastructure installations available for sharing… [e.g.] the availability of space in existing ducts, planned deployment, or upgrading works and interconnection.
- [R]egulators should introduce necessary enforcement tools to ensure compliance and successful adoption of infrastructure sharing regulations, [e.g.]…alternative dispute resolution mechanisms …to encourage negotiated outcomes …[along with] … maintaining the certainty of an adjudicated decision where necessary.
- [R]egulators can consider the introduction of incentives for service providers that share infrastructure as part of their efforts to deploy to rural and underserved areas …,e.g., [appropriate] regulatory exemptions, or financial subsidies.

[118] GSR 2008 guidelines can be found in their entirety at: http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR08/PDF/GSRguidelines08_E.pdf.

- [S]haring should be encouraged…within the boundaries of the Telecommunications/ICT and Broadcasting industry, [and] …with other infrastructure industries (…electricity, gas, water, sewage, etc.).
- [J]oint infrastructure building with other market players and … other industries may be encouraged, providing for timed, organized opportunities for access to ducts and conduits … to distribute the cost of civil works among service providers, … reduce …inconvenience…in towns and cities, … [and] …provide… a positive environmental…impact.
- [There is a] … need for an appropriate level of international and regional harmonization to ensure that best practice regulatory policies on sharing are [widespread].
- Regulators can consider a two-tier strategy: encourage sharing works, rights of way and passive infrastructure (e.g., ducts, masts, towers), and treat other levels of service provision with caution – e.g., as conditioned transitional arrangements designed to achieve specific objectives.
- NRAs or operators can employ a Reference Conduit Access Offer (RCAO) including price, deadlines and standard procedures.
- NRAs or operators can employ a Reference Conduit Access Offer (RCAO) including price, deadlines and standard procedures.
- Operators or NRAs can maintain and update a database describing the utilized and available conduits and associated infrastructure.
- NRAs can provide grants or subsidies from the universal service fund to encourage network rollout to rural areas where towers are shared by several competitive operators.[119]
- NRA's can coordinate and conduct consultations with government utilities and private entities such as power, transport, railways, broadcasting, or electricity, to identify opportunities to obtain rights of way and horizontal corridors that may be used by telecommunications service providers.
- NRA's can approach municipal governments, relevant offices in related Ministries and other stakeholders, whether pubic or private, to coordinate and implement activities for sustained infrastructure development.
- NRA's can conduct consultations with operators from the telecommunications sector and operators of other networks, e.g., railways, broadcasting, or electricity, to coordinate passive infrastructure sharing.

6 Enforcing Spectrum Policies, Rules and Regulations

6.1 Overview

Spectrum users must comply with license requirements and technical rules and regulations since without effective regulations and enforcement procedures, the integrity of the spectrum management process[120] can be compromised. Spectrum managers are particularly concerned with interference problems affecting public

---

[119] **Indi**a engages in this practice and requires at least three operators to share the tower before making a subsidy available.

[120] The traditional spectrum management regulatory functions include: (i) charting the major trends and developments in technology and considering the needs of current and future users of the radio spectrum; (ii) evaluating information, capabilities and technology choices to support decisions affecting the allocation, allotment and assignment of radio spectrum; (iii) identifying solutions to interference problems and technical compatibility among radio systems are key areas of focus; (iv) licensing radio communication equipment and making frequency assignments. The purpose of spectrum monitoring is to support the spectrum management process in general and, more importantly, to assist in resolving electromagnetic spectrum interference, so that radio services and stations may coexist. This in turn reduces and minimizes resources associated with installing and operating telecommunications services and also provides economic benefits to a country's infrastructure through access to interference-free, accessible telecommunication services. ITU-R Spectrum Management Handbook. National Spectrum Management is closely associated with national law, policy statements, radio regulations and a long-range spectrum plan. National spectrum management must ensure that adequate spectrum is provided over both the short and long term for organizations to fulfill their missions for public and commercial telecommunications, including broadcasting. *See*, ITU-R Report SM 2093 and ITU-R National Spectrum Management Handbook, *Guidance on the Regulating Framework for National Spectrum Management*.

safety and security services such as ambulance, fire fighting, police, and navigational services at airports and harbors.[121]

One of the NRA's roles is to manage the radiofrequency spectrum and ensure that services remain free from harmful interference, as stipulated in the Radio Regulations and national frequency tables. As new wireless services place increasing demands on the radio frequency spectrum, managing interference considerations will become an increasingly important role for NRAs.[122] As various countries seek to implement advanced wireless services for their citizens, it is important to consider how those new services will impact existing installations. Coordination proceedings, both internal and cross-border, and registration of Earth stations through national databases or the ITU Master International Frequency Register (MIFR), are helpful tools to help regulators enforce interference regulations.[123]

To create an optimal environment in which interference regulations can be enforced by an NRA, it would be advisable for Administrations to work with operators to support coordination requirements both internally and cross-border, as needed. Specifically, Administrations could develop internal mechanisms to support coordination of satellite earth stations within their own country. Part of this process could be to develop national registries of satellite Earth stations. These registries would help ensure that when requests are received to deploy a new satellite or terrestrial system, Administrations would be aware of the location of Earth stations already existing within their borders.

Administrations could also put into place mechanisms by which they would meet with border countries that are affected by a proposed new system or by the coordination process] and ensure that [the necessary cross-border coordination] is successfully completed. The information would then be submitted to the ITU for inclusion in the MIFR.[124]

Conducting and completing both internal and cross-border coordination would ensure regulatory certainty for satellite Earth station users as well as users of new wireless systems who will be able to operate in an interference free environment.

Through internal and cross-border coordination proceedings, use of the ITU's MIFR, and national frequency registries, regulators can ensure that as new technologies are deployed existing systems are protected so that citizens do not experience service interruptions.

Monitoring is used to obtain detailed information on the technical and operational characteristics of radio systems which are in use or are being tested for future use.[125] Measurements will typically include frequency, power, occupancy rate, direction finding and location of a transmitter. License conditions can be verified against actual use of equipment aiding in the determination of electromagnetic compatibility (EMC).[126]

In the case of harmful interference, the spectrum manager may, at the owner's expense:

1. Take suitable measures to eliminate or reduce the interference or disturbance;
2. Remedy a fault in or the improper operation of the equipment;
3. Accommodate, modify, or alter the equipment or;
4. Disconnect/seize the equipment.[127]

---

[121] *Info*Dev/ITU *Radio Spectrum Management* Toolkit, McLean Foster/Cave/Jones, January 2007, *see also* IACO Regulations.

[122] Contribution of **SES NEW SKIES (Netherlands)** to ITU-D Question 18/1/1 (March 30, 2009) at 1 – 2.

[123] *Id.*

[124] *Id.*

[125] The basic types of monitoring stations include fixed, mobile, and transportable. Monitoring stations usually contain antennas, receivers, and direction finding equipment with dedicated software. This equipment can also be categorized by frequency band (HF, VHF, UHF, SHF, etc). *See* ITU-R Spectrum Monitoring Handbook. With the advent of spread spectrum and computer-based radio technologies like Cognitive Radio, the sophistication, complexity and prices for monitoring equipment have risen. Simple systems for VHF/UHF monitoring can be comprised of several fixed antennas, receivers and limited function spectrum analyzers. More complex systems can consist of multiple sites and mobile and fixed stations. *Info*Dev/ITU *Radio Spectrum Management* Toolkit, McLean Foster/Cave/Jones, January 2007.

[126] ITU-R Report SM 2125, *Parameters of and measurements procedures on H/V/UHF monitoring receivers and stations*. ITU-R Spectrum Monitoring Handbook, Chapter 4.

[127] ITU-R Report SM 2130, *Inspection of Radio Stations.*

In the course of conducting exercises to resolve interference problems, the spectrum manager may be required to enter the user's premises and inspect radio equipment to determine compliance with license conditions and technical standards. An important aspect of completing these tasks noted above is the requirement to clearly establish the duties and obligations of the spectrum manager/inspector and protect the public's rights during such inspections.[128]

It is therefore necessary to have an appropriate framework and process for responding to and managing complaints, for settling disputes, and resolving interference problems. Consideration needs to be given to penalties, remedies, enforcement and alternative dispute resolution (ADR) mechanisms for industry disputes with the aim of ensuring rapid resolution.

6.2 Country Examples

In **Côte d'Ivoire**, **ATCI** is entrusted with managing and monitoring the radio frequency spectrum. They have domestic rules of procedure along with a publicly available national frequency allocation table. **ATCI** uses two mobile measurement and direction-finding stations and two fixed stations. As of April 2007, administrative management is performed manually, pending receipt of an automated system.[129]

In **Brazil**, broadcast authorizations are within the exclusive jurisdiction of the Ministry of Communications. Due to the falling cost of low power transmitters and the bureaucratic difficulties to obtain authorization, **ANATEL** is seeing an increase in illegal broadcast stations. In 2005 – 2006, these "irregular broadcast entities" as they are referred to accounted for an average of 65% of all inspections of illegal stations. Because these entities can easily move or shut down equipment and operations, and because they reportedly coordinate with one another to evade prosecution, irregular broadcast entities account for a high level of unsuccessful enforcement actions for Anatel.[130]

6.3 Challenges Identified

- No national allocation tables.
- Lack of adequate monitoring equipment; HF and VHF receivers, only.
- Difficulty detecting and prosecuting portable, illegal, broadcast entities.
- Difficulty in solving national interference problems.[131]
- Difficulty solving interference from stations in neighbouring countries.[132]
- Difficulty in carrying out frequency coordination with neighbouring countries.[133]
- Lack of qualified staff.[134]
- Lack of staff.[135]

---

[128] *Info*Dev/ITU *Radio Spectrum Management* Toolkit, McLean Foster/Cave/Jones, January 2007.

[129] Contribution of **ATCI** to Question 18/1/1 (April, 2007) at 4.

[130] **ANATEL** Contribution to ITU-D Question 18/1/1 (April 2007) at 3.

[131] ITU-D Resolution 9, Participation of countries, particularly developing countries, in spectrum management, Draft Analysis Report on Part II of the Questionnaire, Document JGRES09/29 (Rev.2) E at 46-47.

[132] *Id*.

[133] *Id.*

[134] *Id*.

[135] *Id.*

6.4 Guidelines[136]

- Establish and maintain a national spectrum management organization, either independent or part of the telecommunication regulatory authority responsible for managing the radio spectrum in the public interest.
- Promote transparent, fair, economically efficient, and effective spectrum management policies, i.e., regulate the efficient and adequate use of the spectrum, taking into due account the need to avoid harmful interference and the possibility of imposing technical restrictions in order to safeguard the public interest.
- Make public, wherever practicable, national frequency allocation plans and frequency assignment data to encourage openness, and to facilitate development of new radio systems, i.e., carry out public consultations on proposed changes to national frequency allocation plans and on spectrum management decisions likely to affect service providers, to allow interested parties to participate in the decision-making process.
- Maintain a stable decision-making process that permits consideration of the public interest in managing the radio frequency spectrum, i.e., provide legal certainty by having fair and transparent processes for granting licenses for the use of spectrum, using competitive mechanisms, when necessary.
- Provide in the national process, in special cases where adequately justified, for exceptions or waivers to spectrum management decisions.
- Have a process for reconsideration of spectrum management decisions.
- Minimize unnecessary regulations.
- Encourage radiocommunication policies that lead to flexible spectrum use, to the extent practicable, so as to allow for the evolution of services1 and technologies using clearly-defined methods, i.e.:
  (a) eliminate regulatory barriers and allocating frequencies in a manner to facilitate entry into the market of new competitors,
  (b) encourage efficiency in the use of spectrum by reducing or removing unnecessary restrictions on spectrum use, thereby encouraging competition and bringing benefits to consumers, and
  (c) promote innovation and the introduction of new radio applications and technologies.
- Assure open and fair competition in the marketplaces for equipment and services, and remove any barriers that arise to open and fair competition.
- Take note of procedures for registering earth station terminals in the International Frequency Register (MIFR) and use this existing tool to mitigate interference as new systems are planned for deployment.
- Collaborate with regional and other international regulatory authorities/policymakers to develop coordinated regulatory practices to avoid harmful interference, including mechanisms for holding cross-border coordination meetings to ensure harmful cross-border interference is avoided.
- Harmonize, as far as practicable, effective domestic and international spectrum policies, including of radio-frequency use and, for space services, for any associated orbital position in the geostationary-satellite orbit or of any associated characteristics of satellites in other orbits.

---

[136] Suggested Guidelines indicated with **closed bullets** are taken from ITU-R National Spectrum Management Handbook, Annex 2, *Best Practices for National Spectrum Management*. Some of these best practices are intended to interface with or transition to international practices, e.g., those relating either to collaboration with colleagues in other countries, or to coordination, such as that which would occur at a bilateral or multilateral consultation preceding a World Radio Conference, or at an international satellite coordination meeting. These practices are further intended to harmonize global spectrum management policies, to the extent practicable, by harmonizing practices among national administrations.

Guidelines indicated with **open bullets** summarize best practices emerging from the consultation process on this question that add important elements warranting inclusion.

1 Whenever the term “services” is used in the (ITU-R Spectrum Management) Handbook, it means applications and recognized radiocommunication services.

- Work in collaboration with regional and other international colleagues to develop coordinated regulatory practices, i.e., work in collaboration with regulatory authorities of other regions and countries to avoid harmful interference.
- Remove any regulatory barriers to free circulation and global roaming of mobile terminals and similar radiocommunication equipment.
- Use internationally recommended data formats and data elements for exchange of data and coordination purposes, e.g., as in the Radio Regulations Appendix 4, and in the ITU Radiocommunication Data Dictionary (Recommendation ITU-R SM.1413).
- Use "milestone" management steps and phases to monitor and control lengthy radiocommunication system implementation.
- Adopt decisions that are technologically neutral and which allow for evolution to new radio applications.
- Facilitate timely introduction of appropriate new applications and technology while protecting existing services from harmful interference including, when appropriate, the provision of a mechanism to allow compensation for systems that must redeploy for new spectrum needs.
- Consider effective policies to mitigate harm to users of existing services when reallocating spectrum.
- Where spectrum is scarce, promote spectrum sharing using available techniques (frequency, temporal, spatial, modulation coding, processing, etc.), including interference mitigation techniques and economic incentives, to the extent practicable.
- Use enforcement mechanisms, as appropriate, i.e., apply sanctions for non-compliance with obligations and for inefficient use of radio frequency spectrum under relevant appeal processes.
- Utilize regional and international standards whenever possible, and where appropriate, reflect them in national standards.
- Rely to the extent possible on industry standards including those that are included in ITU Recommendations of in lieu of national regulations.

7 Enforcing Regulations that Protect Consumers

7.1 Overview

The World Summit on the Information Society called on governments to develop and update their domestic consumer protection laws to respond to the new requirements of the information society.[137] NRAs may pursue a number of avenues in their aim to regulate the communications market for the benefit of all players, including consumers. Regulators do not need to act alone on behalf of consumers, however. There are a number of consumer organizations – for example, Consumers International and ISOC – for regulators to partner with to achieve their consumer protection objectives.[138] Similarly, NRAs may also facilitate the creation of local consumer associations to provide this assistance.

To protect the consumer, the regulator has four broad functions:

- Voice: allowing the consumer/user to be heard, and being responsive through consultation and redress mechanisms;
- Choice: ensuring plentiful choice in the nature, quality, and amount of services;
- Representation: preventing dominance by large industry interests through consumer councils or committees; and

[137] See, Chairman's Report, ITU Global Seminar on Quality of Service and Consumer Protection (September 2006) at 4.

[138] Id.

- Information: helping consumers to make well informed choices.[139]

Data protection and privacy are two other areas directly impacting consumers of telecommunications services and of increasing concern to NRAs. Laws on this topic vary around the world; the **European Commission** has promulgated the Data Protection Directive (95/46/EC) and the Directive on Privacy and Electronic Communications (2002/58/EC) to be incorporated into the domestic laws of the European Union Member States. The Data Protection Directive establishes principles relating to processing personal data. These include: (i) data should be processed fairly and lawfully; (ii) data is to be collected for specified and legitimate purposes; (iii) data collection is to be relevant, and not excessive for the purpose for which it is collected; and (iv) data must be accurate, updated, and kept no longer than is necessary.[140]

Article 5 of the **European Commission** Directive 2002/58/EC on "Privacy and electronic communications" states that: "Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing, and is offered the right to refuse such processing by the data controller."[141]

7.2 Country Examples

In the **United States**, consumer protection rules applicable to telecommunications services include the following:

- Section 222 of the Communications Act under which telecommunications carriers may disclose **personal customer information** only within the provision of the telecommunications service from which the personal information is derived. The telecommunications carrier may not disclose personal information without the consumer's consent, and is restricted from using the personal information for marketing and other purposes.[142]
- Section 258 of the Communications Act prohibits telecommunications companies from **"slamming"**-- submitting and implementing unauthorized changes to a customer's selection of telephone services.[143]
- "**Truth-in-Billing**" rules require that consumers receive accurate and clear information on their telecommunications bills. The goal is to provide consumers with a better understanding of the **charges on their bill** and the opportunity to compare service offerings. The Commission's rules require that a carrier's bill: "(1) be accompanied by a brief, clear, non-misleading, plain-language description of the service or services rendered; (2) identify the service provider associated with each charge; (3) clearly and conspicuously identify any change in service provider; (4) identify those charges for which failure to pay will not result in disconnect of basic local service; and (5) provide a toll-free number for consumers to inquire or dispute any charges."[144]
- The **Network Outage Reporting** requirement requires telecommunications carriers to notify the Commission when there is a network outage of thirty minutes or more that will affect a large number of customers or that will involve major airports, 911 facilities, nuclear power plants, key government facilities, or military installations.[145]

---

[139] Chairman's Report, ITU Global Seminar on Quality of Service and Consumer Protection (September 2006) at 4, citing R. Southwood (Balancing Act).

[140] *EU Mobile Multimedia and Privacy*, Contribution of **Thales (France)** to ITU-D Question 18/1/1/ (February 2007) at 2.

[141] *Case Study, France: Protection of Personal Data on the Internet,* Contribution of **Thales, France** to ITU-D Question 18/1/1 (February, 2009) at 3.

[142] 47 U.S.C. § 222(c)(1) (1996). See also *Consumer Protection in the Broadband Era,* FCC Notice of Proposed Rulemaking, Docket 05-150 (2005) p. 78, para. 148.

[143] 47 U.S.C. §258(a) (1996). *See also Id*. at para. 150.

[144] 47C.F.R. § 64.2401 (1999). *See also*, *Id*. at para. 151 (2005).

[145] 47 C.F.R. § 63.100(a)-(e) (2004) *See also, Id. at* para. 154.

- Section 214 of the Communications Act limits a telecommunications carrier's ability to unilaterally terminate service with customers. The rules require that "domestic carriers wishing to **discontinue, reduce, or impair services** must first request authority to do so from the FCC and must notify affected customers and others of their plans."[146]

In April of 2009, the **United States** FCC released a Notice of Inquiry (NOI) titled *A National Broadband Plan for the Future*.[147] Therein, the FCC requested comment on the applicability of the existing rules to broadband services as well as several other issues affecting consumers:

- The role privacy protection can play in enhancing consumer welfare;
- How advances in technology help advance consumer welfare;
- How emerging applications now or in the future will advance consumer welfare and what their network requirements will be;
- Whether consumer welfare would be enhanced by more disclosures to customers of limitations that providers of broadband services may place on the services;
- Which aspects of broadband policy have improved consumer welfare, promoted competition, and led to technological innovation;
- The interplay between consumer welfare and the market in general, e.g., when the market falls short of providing adequate consumer protection; and
- How the government can maximize the efficiency of its consumer protection regulations.[148]

Approved by the National Congress on July 16, 1997, the General Telecommunications Law (Law n, 9472) restructured the Brazilian telecommunication sector, authorized the privatization of state-controlled companies and established the national regulatory authority. Three laws have increased service provider's obligations and extended and consolidated consumer rights in **Brazil**: Fixed Telephone Service Regulation in 2005 which included new rules covering accessibility and support for disabled users; Personal Mobile Service Regulation in 2007 which required number portability for consumers; and Pay TV service regulation involving consumer protection in 2007 which permits consumers to request discounts for service interruption.[149]

An important part of **Anatel Brazil'**s mission is to guarantee consumer rights. Accordingly, **Anatel** has taken several significant steps to advance this goal. During its 10 years of existence, for example, Anatel's (consumer) Call Center has received more than 30 million calls. Only 4.5 million of these were not answered instantaneously but were answered in a few days. In 1998, it took an estimated 30 days to respond to consumer's questions; as of 2008 ninety-seven percent of the questions that cannot be answered immediately are answered within 5 days.[150]

Anatel also holds periodic meetings with service providers to establish goals and objectives that will reduce complaints about telecommunications services. In 2008, **Anatel** released regulations on the Fixed Telephone Users Committee (*Comitê de Defesa dos Usuários*), a special council to be established within the service provider to evaluate quality of services and help resolve conflicts between users and fixed telephone companies. This council has 6 representatives for users and 6 representatives for associations and consumer protection entities.[151]

In 2008, **Anatel** issued a public notice calling on members of civil society to establish the Telecommunication Users Advisory Committee, a special advisory council for Anatel's Board of Directors regarding consumer rights. This committee is headed by one of **Anatel's** Commissioners and its function is

---

[146] 47 U.S.C. § 214(a) (2004), 47 U.S.C. § 63.71 (2004), 47 U.S.C. § 63.71(a) (2004). *See also, Id.* at para. 155.

[147] *A National Broadband Plan for Our Future,* FCC, Notice of Inquiry, GN Docket 09-51 pp. 25-26, (2009).

[148] *Id.*

[149] **Brazi**lian Overview on Consumer Protection, Network Security and Internet, Contribution to ITU-D, Question 18/1/1 (20 August 2008) at 2.

[150] *Id.*

[151] *Id.*

to present and discuss consumer's claims, and suggest ways to improve regulation and enforcement practices.[152]

During re-negotiations of the fixed operators concession contracts, **Anatel** adjusted the commitment between itself and the telecommunications operators to extend access to telecommunications services for low income users in Brazil. Additionally, they negotiated that going forward; such users who qualify as short term customers would pay a reduced monthly rate of approximately US $6.62, or roughly 60% of the regular fee.[153]

To further assist consumers, **Anatel** posts information about the complaints consumers file against fixed and mobile operators. As mentioned earlier, they also maintain a toll free service and a "citizen room" in all capital cities where users can file complaints and obtain information. All requests for information are maintained electronically and can be followed via the Internet. **Anatel** also maintains a fee database that shows what long distance call providers charge based on time, origin, and destination of call. Consumers can access this information over the Internet; it is periodically updated.[154]

In **France**, an administrative agency called The National Information and Liberties Commission (CNIL) was established by law 78-17 to protect personal data and privacy.[155] CNIL is the first of its kind in **France**. As a result of the law, personal data may only be collected, processed, and stored if the entity or business has submitted a prior declaration to CNIL, which allocates a registration number. The number must be displayed on the website together with the contact address of the service handling the personal data. Political parties, churches, trade unions, and associations do not have to declare their files, nor do websites set up by private individuals for exclusively personal use.[156]

CNIL informs public authorities and professional entities processing personal data of their duties. It also permits citizens to have indirect access to certain files. Compliance with the law is monitored by examining declarations, and by visits to businesses and entities, either randomly or while following up on a complaint. The punitive powers granted to CNIL by the legislature are warnings, summons and financial penalties. CNIL may also refer the most serious cases to the public prosecutor's office. In 2007, CNIL registered 56,404 new personal data processing files, received 4,455 complaints, carried out 164 inspections, issued 101 summons, gave five warnings, handed down nine financial penalties, and reported five cases to the judicial authorities. On August 6, 2004, the European Directive 2002/58/EC on personal data protection was transposed into French law, amending the law of 1978. The 2004 law substantially decreased the declaration obligations for entities storing files, but increased CNIL's powers, giving it on-site investigations and sanctions, and strengthened the rights of individuals.[157]

On April 4, 2008, "G29", a working party made up of European representatives of each personal data protection authority,[158] published an opinion recommending, among other things, that the maximum retention period for personal data on Internet search engines be reduced to six months. On 29 May 2008, the President of the French Republic and the Prime Minister announced a major initiative to be completed by 2012, called ***France*** *Numerique 2012* (Digital **France** 2012). The plan includes safeguarding the protection of personal data on the Internet, and the LIFL is to be strengthened both in terms of technological expertise and monitoring.[159]

---

[152] *Id.* at 3.

[153] **ANATEL** Contribution to ITU-D Question 18/1/1 (April 2007) at 3.

[154] *Id*. at 4.

[155] Law 78-17 on Information, Files, and Liberties (LIFL), January 6, 1978. *Case Study, France: Protection of Personal Data on the Internet,* Contribution of **Thales, France** to ITU-D Question 18/1/1 (February, 2009) at 2.

[156] *Case Study, France: Protection of Personal Data on the Internet,* Contribution of **Thales, France** to ITU-D Question 18/1/1 (February, 2009) at 2.

[157] *I*d. at 3.

[158] *Id*. The G29 was established pursuant to Article 29 of Directive 95/46/EC. At 3.

[159] *Id*. *France Numérique 2012* was initiated by the Prime Minister in October 2008 and includes 154 actions. It was the outcome of a consultation process instituted by the French government commenced to draw up a nationwide digital development plan. For comprehensive information on *France Numerique 2012,* see *Case Study – **France** Numérique (Digital France) 2012, a Nationwide Digital Development Plan*, Contribution of **Thales, France** to ITU-D Question 18/1/1 (January, 2009).

Tanzania established a Consumer Consultative Council, which was the first of its kind in the country for consumers.[160] **Nigeria** employs a Consumer Parliament which holds public meetings during which both operators and the regulator receive and answer questions from members of the public. **Malaysia**'s Communications and Multimedia Commission includes a Consumer Protection Department, while **India**'s Telecom Disputes Settlement and Appellate Tribunal can adjudicate disputes between a group of consumers and service providers.[161]

In **Côte d'Ivoire**, all public network operators are required to ensure the secrecy of correspondence. The 1995 Act, Decree 97-391 (July 9, 1997) and the terms of reference in the licenses requires operators to respect the confidentiality and neutrality of messages transmitted and ensure the protection, integrity, and confidentiality of identifying information held or processed. In addition, radio network operators are prohibited from installing eavesdropping interfaces, and all terminal equipment must be approved before it can be connected to the public network. **ATCI** has procedures for handling consumer complaints and each operator must provide dispute settlement procedures for consumers.[162]

As recommended by **Canada**'s 2006 Telecommunications Policy Review Panel report, a new entity was created to resolve complaints and develop industry codes of conduct and standards. The Commissioner for Complaints for Telecommunications Services (CCTS) is a consumer and business complaints investigation agency that began operation on July 23, 2007. It is financed by industry and will attempt to resolve complaints and develop industry codes of conduct and standards. CCTS will also publish an annual report on the nature, number and resolution of complaints received about each provider and will identify causes for concern warranting further action. **CRTC w**as charged with creating the CCTS and for meeting its reporting requirements until it was established.[163]

In response to a price increase in the **Gambia** in which the incumbent began charging customers on a per-minute basis for communications services, the NRA gave notice to the incumbent and, following a process of negotiation, won agreement by the incumbent to return to and ultimately issue a refund of the amount collected. This was the first refund of this kind issued in the **Gambia**; under the direction of the NRA the refund was donated to the country's hospital. In another matter, the NRA ordered a 50% phased reduction in interconnection rates for the benefit of users and consumers in the **Gambia**.[164]

7.3 Challenges Identified

- User/consumer complaints about billing practices, new service connections, disconnect errors.
- High international tariffs (not competitive).
- Pressure to protect tariffs for international traffic.

7.4 Guidelines

- Survey users and consumers to obtain their opinions and views about service and other issues; hold public meetings for this purpose as appropriate;
- Encourage and facilitate the creation of independent associations that will represent users and consumer's interests;
- Encourage and facilitate the creation of a unit within the service providers that is dedicated to addressing and resolving consumer issues;
- Create a unit within the NRA that is dedicated to addressing and resolving consumer issues.
- Consider permitting a consumer representative on the NRA board.

---

[160] See, Chairman's Report, ITU Global Seminar on Quality of Service and Consumer Protection (September 2006) at 5.

[161] *Id*.

[162] Contribution of **ATCI** to Question 18/1/1 (April, 2007) at 5 – 6.

[163] *See* Global Insight (http://www.globalinsight.com) *Canadian Government Acts to Speed Up Deregulation*, Published April 5, 2007.

[164] ITU-D Question 18/1/1 Rapporteur's Group Meeting, ITU Headquarters, April 2009.

- Establish appropriate mechanisms to ensure that regulators and the regulatory framework takes into account the opinions and views of consumers and consumer associations;
- Provide notice to users and consumers of telecom/ICT decisions that affect them.
- At the European and international level, foster the development of guidelines, recommendations, or standards if appropriate, specifying a retention period for personal data.

8 Enforcing Quality of Service Policies and Regulations

8.1 Overview

ITU-T recommendation E.800 defines quality of service as "the collective effect of service performances, which determine the degree of satisfaction of a user of the service."[165] Quality of service therefore concerns aspects of services that users experience directly. It can be contrasted with network performance, which, according to ITU-T recommendation E.800, is "the ability of a network portion to provide the functions related to communication between users."[166] The ITU has at least 150 technical recommendations related to quality of service, and several other organizations, such as ETSI and IETF, have also developed related standards.[167]

Competition in a service market should positively affect the quality of the services provided, and NRAs in countries with little or no competition have greater difficulty in ensuring quality for users and consumers. Such NRAs must be more proactive; however measuring quality, establishing targets, and enforcing standards under these circumstances is generally more laborious than when market incentives also exist for operators to provide good service. Poor customer support is sometimes a symptom of deficiencies in staff skills. High fault report rates and low proportions of successful calls generally indicate a need for improved network equipment. In a market where users and consumers can easily choose an alternate service provider, poor performance can be swiftly addressed and punished by customer churn.

8.2 Country Examples

In **Brazil**, the obligations that landline telephone service concessionaires have to provide universal service are established in their concession contracts in accordance with the General Target Plan for Universal Access to Services (PGMU) and the General Plan for Quality Targets (PGMQ). These plans originated prior to privatization of the sector, but have both quantitative and qualitative parameters. These plans require operators, on an annual basis, to guarantee activation of 11.4 million new lines, and to install 381,900 functioning payphones.[168]

Qualitative targets aim to guarantee the speed of deployment of the new lines and stipulate maximum wait times for installation. Renewal of fixed-line contracts in 2006 included new targets in regard to the PGMU and PGMQ. With regard to quality of service the new commitments include an access guarantee to telephony services with priority to the handicapped and hearing impaired, a requirement to deliver a basic service plan, and the obligation to issue a credit of 1/30 of the monthly bill to customers that experience service interruption exceeding 30 minutes in a 24 hour period.

Quality of service requirements in **Côte d'Ivoire** can be found in the operator's license agreement and cover call routing efficiency and speed and efficiency of network maintenance and service provision. In addition, the agreements contain the following performance indicators: fault occurrence and clearance time,

---

[165] *See* ICT Quality of Service Regulation: Practices and Proposals (Background Paper, R. Milne, Antelope Consulting), ITU Global Seminar on Quality of Service and Consumer Protection (2006) at 12, *citing* ITU-T Recommendation E.800, Terms and definitions related to quality of service and network performance including dependability, August 1994, at http://www.itu.int/rec/T-REC-E.800.

[166] *See Id. at 12, citing* ITU-T Recommendation E.600, *Terms and definitions of traffic engineering*, March 1993, at http://www.itu.int/rec/T-REC-E.600.

[167] For a summary of the work of ITU and other organizations on quality of service see ITU, *Quality of Service and Network Performance*, (March 2004) at http://www.itu.int/pub/T-HDB-QOS.02-2004. *See Id.* at pp. 32 and 53.

[168] **ANATEL** Contribution to ITU-D Question 18/1/1 (April 2007) at 4.

call completion ratio for local, long-distance and international calls, and rate of complaints. ATCI conducts a quarterly and an annual review of these elements. The interconnection failure rate and clearance time are also examined. With regard to radio operators, the blocking and handover rates are measured by ATCI together with the operator. The results are then made public. [169]

On February 27, 2007, the **United States Federal Communications Commission (FCC)** released a report entitled *Quality of Service of Incumbent Local Exchange Carriers.* This report summarized quality of service data for 2005 submitted by major incumbent local exchange carriers (regional Bell companies and Sprint), as well as smaller incumbent local exchange carriers. The data is presented separately for each operating entity and includes measures of service quality provided to residential and business end-user customers, as well as service quality provided to long distance carriers. Statistically significant six-year trends were identified in four indicators of industry-wide service quality. The findings were as follows: (i) Complaints per million lines decreased on average 5.1% annually; (ii) Installation intervals decreased on average 4.2% annually; (iii) Repair intervals increased on average 5.1% annually; and (iv) Percentage of switches with outages decreased on average 10.9% annually.

Regulators and policymakers in **Trinidad and Tobago** intend to have a minimal set of measurements for quality of service. The regulator there carried out a consultation process to obtain the feedback of its citizens on this topic. As a result, **Trinidad** has 18 quality of service measurements; they are technology neutral. The **Belgian** Institute for Postal Services and Telecommunications has 17 measurements. ARCEP **France** conducts an annual survey for mobile network services. The measurements were developed over a number of years, in consultation with the operators.[170]

In the **United Kingdom,** the scheme for quality of mobile services is voluntary. Measurements are performed by an independent third party under a three year contract with the operators, but the operators do not see the measurements until they are published. The primary objective of these activities is to provide information for customer choice. TRAI, the regulator in **India** employs a third party to conduct testing, audit operator measurements, and perform customer surveys. TRAI prefers encouragement over enforcement, and publishes QoS measurements on its website. ANRT **Morocco** conducts an annual survey of mobile performance and publishes the aggregate results of third party tests. Individual operators also receive the results. ANRT supervises the third party, and may also conduct spot checks on its own.[171]

8.3 Challenges Identified

- Difficulty in defining a standard for service quality.
- Difficulty in measuring quality of service targets, parameters.

8.4 Guidelines[172]

- Publish complaints received about service quality.
- Discern operator skills and customer opinions through widespread consultations, working groups, and open meetings.
- Quality of service (QoS) measurements should be important to customers, practical for operators, and comparable between operators. They should concentrate on a few aspects of services.
- QoS measurements that are published should be accessible to customers, helpful to customers and fair to operators.
- QoS measurements should be reviewed, to see whether they need to be changed, as the market changes and different aspects of services become most important.

---

[169] Id. at 4 – 6.

[170] See, Chairman's Report, ITU Global Seminar on Quality of Service and Consumer Protection (September 2006) at 2.

[171] *Id*. at 3.

[172] *See generally, ICT Quality of Service Regulation: Practices and Proposals* (Background Paper, R. Milne, Antelope Consulting), ITU Global Seminar on Quality of Service and Consumer Protection (2006) at 6.

- QoS measurements should not require more tests and calculations than are likely to be needed to characterize differences in quality that are perceptible to customers, now or in the future.
- QoS measurements should be the same as or similar to ones that operators already make (or will benefit from making) for their own purposes, if possible.
- QoS measurements should deal with matters that operators can control.
- Any targets set should be useful to customers and realistic for operators. They are most likely to be desirable for wholesale services and retail services of dominant operators.

9 Enforcing Network security Policies, Guidelines, Regulations

9.1 Overview

"Cybersecurity is defined as the prevention of damage to, unauthorized use of, exploitation of, and – if needed – the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems."[173] Cybersecurity may also be defined as "the collection of…policies, security safeguards, guidelines…and risk management approaches…that can be used to protect the cyber environment."[174]

The **United States** Department of Justice divides computer-related crimes into three categories: (1) the theft of a computer, (2) the computer being the subject of a crime, such as the subject of an attack, which encompasses: spam, viruses, and worms, and (3) the computer being an "instrument" used to commit a traditional crime, such as identity theft or child pornography.[175]

In general, networks are not adapted to high level security requirements, and due to the global nature of the Internet, activities and violations in this area transgress national boundaries. Building trust in an electronic environment requires substantial effort and cooperation by private, public and non-governmental sectors. A number of international instruments have been established, including the EU Data Protection Directives and, as mentioned below, the Council of Europe Convention on Cybercrime.[176]

The Council of Europe Convention on Cybercrime[177] serves as the model law for international cybercrime enforcement.[178] The convention is the only legally binding multilateral instrument that specifically addresses computer-related crime.[179] "The Council of Europe established a committee of experts on crime in cyber-space in 1997. The treaty was adopted and opened for signatures in 2001, and entered into force on July 1, 2004. As of 2008, the total number of ratifications/accessions was 23.[180] The Convention is open to states around the world.

The role of NRAs in this issue is evolving, as it is with other departments in government. Some NRAs have a greater role to plan than others, while in some cases no role has been identified for the NRA in network security matters.

---

[173] James Ennis, *Draft Report on Question 22/1: Best Practices for Cybersecurity* (International Telecommunication Union, Telecommunication Development Bureau, ITU-D Study Groups, RGQ22/1/032(Rev.1)-E, 2008) (on file with author).

[174] *Id.*

[175] Dana L. Bazelon, Yun Jung Choi, & Jason F. Conaty, *Computer Crimes*, 43 AM. CRIM. L. REV. 259, 260-264 (2006).

[176] *See generally, Network Information and Security*, *Contribution of* ***Lithuania*** *to ITU-D Question 18/1/1, (February, 2007)* (Contribution of **Lithuania** to ITU-D Question 18/1/1 (February, 2007).

[177] *See* Council of Europe Convention on Cybercrime*, available at* http://conventions.coe.int/treaty/EN/Treaties/html/185.htm (last visited Jul. 15, 2008).

[178] *See* Cybercrime Law*, available at* www.cybercrimelaw.net (last visited Jul.15, 2008). Cybercrimelaw.net is a global information clearinghouse on cybercrime law. The editor is Chief Judge Stein Schjolberg, Moss Tingrett Court, **Norway**.

[179] *See* **United States** Department of State, Fact Sheet: Council of Europe Convention on Cybercrime, *available at* http://www.state.gov/r/pa/prs/ps/2006/73354.htm (last visited Jul. 15, 2008).

[180] **Albania, Armenia, Bulgaria, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Italy, Latvia, Lithuania, Macedonia, Netherlands, Norway, Romania, Slovakia, Slovenia, Ukraine** and the **United States**. *Id*

9.2 Country Examples

Lithuania has adopted a comprehensive approach covering multi-stakeholder cooperation, consumer education/awareness, and an appropriate legal framework.[181] Its activities in this area are guided by the principle of mutual cooperation between the public and business sectors. This public/private partnership has been memorialized in the *Memorandum on the Progress in the Area of Network and Information Security* signed by the NRA, the Association of Lithuanian Banks, and Infobalt, an association of information technology and telecommunications companies.[182]

As an EU member state with an Internet subscriber penetration rate of 45.2% (3rd quarter 20006, up from 2.7% in 2003) **Lithuania** has incorporated the Data Protection Directive into its national laws. It is also a signatory to the Convention on Cybercrime, and participates in international initiatives, such as the awareness-raising EU Safer Internet Project and CERT/CSIRT security incident cooperation examples FIRST and TERENA.[183] **Lithuania** has representatives on the European Network and Information Security Agency (ENISA) Management Board and Permanent Stakeholder's Group. In cooperation with ENISA, an annual European Network and Security Conference is organized in Vilnius, its capital.[184]

Lithuania also has a draft law on Network and Information Security that aims to regulate the providers of public communications networks, publicly available electronic communications services, providers of information society services or providers of information society intermediary services. The draft law defines the institutional structure for the various state institutions that will formulate or supervise policy and strategy: the Ministry of the Interior, the Ministry of Transport and Communications, the Communications Regulatory Authority, the State Data Inspection Protectorate, the Police Department and the State Security Department.[185] The draft law also establishes a basis for network and information security of state and municipal institutions. Its aim is to establish higher security for network and information systems of state and municipal institutions. The draft law assigns specific tasks to the **Communications Regulatory Authority (RRT**) including drafting secondary legislation for securing networks. It also requires the RRT to be informed of network and information security incidents. Finally, the draft law establishes a national CERT.[186]

A governmental strategy for Electronic Data Security in Government institutions is set to run through 2008. A principal objective of this initiative is to raise IT security awareness among government officials. An IT security training programme, including distance learning was created; more than 200 government officials will be educated in 2007. The goal is to train all government officials in the future.[187]

At the end of 2005 and in 2006, a survey was conducted that revealed that almost 80% of residential users and enterprises faced computer viruses and SPAM. A number of security projects were conducted in Lithuania since that time and as a result, residential users experienced fewer viruses, spam, and phishing. Enterprise users, however, experienced an increase in security incidents.[188]

In 2006, the Lithuanian NRA established the network and information security incidents management unit (CERT.RRT) to deal with network and information security incidents in public electronic networks, coordinate activities to solve such incidents and work toward their prevention. CERT.RRT is modeled on the Computer Emergency Response Team (CERT) model; its activities are principally directed at ISP networks.[189]

---

[181] Contribution of **Lithuania** to ITU-D Question 18/1/1 (February, 2007) at 1-2.

[182] *Id*. at 3.

[183] *Id*. at 3, 5.

[184] *Id*. at 3.

[185] *Id*. at 4.

[186] *Id*.

[187] *Id*. at 5.

[188] *Id*. at 2.

[189] *Id*. at 3.

Côte d'Ivoire's legislation identifies network security and protection as one of the essential requirements covered by the 1995 Act. The legislation covers all networks, approval for terminal equipment, and communications services, in particular, value-added services. At 7. All authorized operators must take the necessary steps to ensure the secrecy, neutrality, and confidentiality of information maintained and calls carried as provided for in the 1995 Act, its enacting decree of 1997, and their license terms.[190]

The **United States'** Computer Fraud and Abuse Statute[191] and related federal criminal laws govern cybercrime violations.[192] Violations fall under the following sub-headings: (i) trespassing in government cyberspace; (ii) obtaining information by unauthorized computer access; (iii) causing computer damage; (iv) computer fraud; (v) extortionate threats; (vi) trafficking in computer access; and computer espionage.[193] Convictions in the United States for cybercrime are felonies punishable by a fine, or imprisonment ranging from one to ten years.[194] Punishments by fine range in penalties of not more than one hundred thousand dollars to not more than five hundred thousand dollars.[195] Violations that occur as repeat convictions, however, may result in more severe sentencing such as imprisonment ranging from ten years to life.[196]

In **Korea**, the law governing cybercrime enforcement may be found in three pieces of legislation: (1) Criminal Law, (2) The Act on Promotion of information and communications network utilization and information protection, and (3) The Information Infrastructure Protection Act.[197]

Article 141 of the Criminal Law, entitled, "Invalidity of Public Documents, etc. and Destruction of Public Goods," states that "a person who damages or conceals…electromagnetic records…shall be punished by imprisonment…for not more than seven years or by a fine not exceeding ten thousand dollars."[198] Article 227-2, entitled, "False Preparation or Alteration of Public Electromagnetic Records," states, "A person with the intention of disrupting…electromagnetic documents of a public official…shall be punished by imprisonment…not more than 10 years." Article 232-2, entitled, "Falsification or Alteration of Private Electromagnetic Records," states, "A person who falsifies or alters…electromagnetic records…shall be imprisoned for not more than five years, or a fine not exceeding ten thousand dollars." Section 347-2, "Fraud by the Use of Computer," -- result in no more than ten years of imprisonment, or a fine not exceeding twenty thousand dollars. Violations under 366 "Destruction and Damage of Property" result in no more than 3 years of imprisonment, or a fine not exceeding seven thousand dollars.[199]

Under **Korea**'s "Act on Promotion of Information and Communications Network Utilization and Information Protection," the relevant articles appear under "Chapter VI: Stability of the Information and Communications Network." Article 48, titled "Prohibition on Act of Infiltrating into Information and Communications Networks" states that "(1) Any person shall be prohibited from infiltrating into…networks without justifiable access, (2) any person shall be prohibited from transmitting a malicious program that may damage…the information system, and (3) Any person shall be prohibited from sending…data…for the purpose of hindering the stable operation of communications networks." Chapter IX, Penal Provisions

---

[190] Contribution of **ATCI** to Question 18/1/1 (April, 2007) at 7.

[191] The Computer Fraud and Abuse Act, which was enacted by Congress in 1986, amended Title 18: Crimes and Criminal Procedure, Part I-Crimes, Chapter 47- Fraud and False Statements, Section 1030: Fraud and related activity in connection with computers. *See* Scott Eltringham, *Prosecuting Computer Crimes* (United States Department of Justice: Computer Crime & Intellectual Property Section, 2007) *available at* http://www.cybercrime.gov/ccmanual/index.html (last visited Jul. 15, 2008). *See also* Cybercrime Law, Survey: United States, *available at* www.cybercrimelaw.net/laws/countries/us.html (last visited Jul.15, 2008).

[192] *Id.*

[193] Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Congressional Research Service Report for Congress, Order Code 97-1025, 2008).

[194] Eltringham, *supra* note 16.

[195] Doyle, *supra* note 18.

[196] The court may impose life in prison "where the offender knowingly or recklessly causes or attempts to cause death." Eltringham, *supra* note 16. *See also* 18 U.S.C. § 1030 (c) (5).

[197] *See* Cybercrime Law, Survey: Korea, *available at* http://www.cybercrimelaw.net/laws/countries/korea.html (last visited Jul.15, 2008).

[198] Amended by Act No. 5057 (Dec. 29, 1995.) *Id.*

[199] *Id.*

contains four articles: 61, 62, 63 and 65. The penal provisions range in punishments from one to five years of imprisonment, or ten to forty-nine thousand dollars in fines.

Finally, Article 28 of **Korea**'s Information Infrastructure Protection Act states, "Any person who disrupts…or destroys a Critical Information Infrastructure will be imprisoned for not more than 10 years, or punished by a fine not exceeding ninety-nine thousand dollars."[200]

In **Japan**, The Ministry of Internal Affairs and Communications has provided financial support for national cyber-attack exercises from 2006-2009.[201] Japan's "Unauthorized Computer Access Law," governs cybercrime violations.[202] Article 3 lists the prohibited acts of unauthorized computer access; and Article 4, "Prohibition of acts of facilitating unauthorized computer access," states, "No person shall provide another person's identification code relating to an access control function to a person other than the access administrator…" Under Article 9, a person who has violated Article 4 shall be punished with a fine of not more than 3 thousand dollars." Penal Code Article 258 "Damage to Documents in Public Use," states, "a person who damages documents or electronic-magnetic record in public official use shall be punished with imprisonment for not less than three months or more than seven years." Under Penal code Article 259 "Damage to Documents in Private Use," a person who damages documents or electro-magnetic record in private use and owned by another person who proves a right or duty shall be punished with imprisonment for not more than five years."[203]

Australia passed legislation in 2001 amending its law governing computer offenses. Violations of these laws will result in imprisonment from two to ten years. Sections 477.2 and 477.3 of the Cybercrime Act of 2001[204] entitled "Unauthorized modification of data to cause impairment" and "Unauthorized impairment of electronic communication" each carry penalties of ten years imprisonment for their violation. Sections 478.1 and 478.2 titled "Unauthorized Access to, or Modification of Restricted Data," and "Unauthorized impairment of data held to a computer disk," each have a penalty of 2 years imprisonment for violation. "478.3, Possession or control of data with intent to commit a computer offense," found in Section 478.3 and Section 478.4, "Producing, supplying or obtaining data with intent to commit a computer offense," both carry penalties of 3 years imprisonment for a violation.[205]

In **China**, the Public Security Bureau (PSB) oversees internal security; the Ministry of State Security (MSS), oversees external security.[206] The Criminal Law of the People's Republic of China (March 14, 1997) governs cybercrime. Article 285 of this law states: "Whoever violates…and intrudes into computer systems…is to be sentenced to not more than three years…" Article 286 states, "Whoever…interferes in computer information systems…is to be sentenced to not more than five years…"[207] In **Hong Kong**, two sections from a telecommunications ordinance govern cybercrime offenses.[208] Section 27A, titled, "Unauthorized access to computer by telecommunication," states: "Any person who… knowingly causes a computer to perform a function to obtain unauthorized access…is liable on conviction to a fine of twenty thousand dollars."[209] Section 161, titled "Access to computer with criminal or dishonest intent" states, "Any person who obtains

---

[200] *Id.*

[201] Koichi Arimura, *Case Study Introduction of Cyber Attack Exercise Conducted by Japanese Telecommunication Carriers* (Telecom-ISAC-SAC **Japan**: Telecom information Sharing and Analysis Center Japan, 2007) *available at* http://www.apectelwg.org/ (last visited Jul. 15, 2008).

[202] Law No. 128 of 1999, "Husei access kinski hou." *See* Cybercrimelaw.net, Survey: **Japan**, *available at* www.cybercrimelaw.net/laws/countries/japan.html (last visited Jul.15, 2008).

[203] *Id.*

[204] *See* Cybercrime Law, Survey: **Australia**, *available at* www.cybercrimelaw.net/laws/countries/australia.html (last visited Jul.15, 2008).

[205] *Id.*

[206] *See* Cybercrime Law, Survey: **China**, *available at* www.cybercrimelaw.net/laws/countries/china.html (last visited Jul.15, 2008).

[207] *Id.*

[208] *Id.*

[209] *Id.*

access to a computer…with intent to commit an offense…is liable on conviction upon indictment to imprisonment for five years."[210]

As of 2008, **Brazil** did not have specific regulation covering network security. Rather, network security is accomplished via the cooperation of three groups: telecommunications operators, Computer Emergency Response Teams (Brazil) (CERT.br), and the Critical Telecommunication Infrastructure Protection Project. Operators have developed voluntary security measures to protect their networks and customer base. CERT.br is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Internet in **Brazil.** The Critical Telecommunication Infrastructure protection project is a two-year program aiming to (identify critical points of **Brazil's** telecom infrastructure; (ii) propose recommendations to prevent security incidents and guarantee service and business continuity; (iii) develop strategies and policies to protect Brazil's telecom infrastructure; (iv) analyze interdependence between different networks. The program was developed by Anatel and CPqD, a private telecom research center and is sponsored by the Fund for Technological Development of Telecommunications.[211]

In **Venezuela**, the Ministry, through the Superintendent of Electronic Certification Services, (SUSCERTE) is developing a risk management model that includes processes, methodologies, and policies for proper management of information security risks in the institutions of the Venezuelan State. Venezuela is also working on creating an Incident Response Center, which will aim to prevent, detect and manage such incidents. In addition, the National Center for computer Forensics (CENÍFER), a high-level center for collection, preservation, analysis and presentation of evidence related to information technology to support criminal investigations will complement SUSCERTE, and will provide reliability, integrity, security, and stability to the forensic process.[212]

In **Madagascar**, the state, together with the regulator and the operators are in the process of preparing the requisite regulatory texts for the nation's cybersecurity policy. Accordingly the following actions will be undertaken:

- adopt regulatory text
- install filtering and security technology e.g., firewalls, by ISPs
- extend cybersecurity measures to mobile telephone operators;
- collaborate with ISPs to block "morally undesirable" sites;
- combat spam; and – encourage users to be more vigilant (use passwords, caution in downloading message attachments, avoiding peer to peer downloading as much as possible.)[213]

9.3 Challenges Identified

- In a case where authorization is required in order to engage in encryption, the legislative decree setting forth the conditions under which this authorization may occur has not yet been enacted.
- No laws covering cyber crime.

9.4 Guidelines

- Proactively deal with security challenges.
- Develop and practice close cooperation between the domestic public and private sectors.
- Give special attention to management of security incidents through CERT groups.
- As network and information security issues go far beyond the boundaries of one country or a particular region, engage in international cooperation.
- Conduct awareness raising campaigns on safeguarding measures and building a culture of cyber security on the international level.

---

[210] *Id.*

[211] **Brazi**lian Overview on Consumer Protection, Network Security and Internet, Contribution to ITU-D, Question 18/1/1 (20 August 2008) at 3.

[212] Contribution of the Bolivarian Republic of Venezuela to ITU-D Question 18/1/1/ (September 2008) at 6.

[213] Contribution from **Madagascar** to ITU-D Question 18/1/1 (July 2009) at 2.

- Recognize and participate, as appropriate, in the efforts made by various international organizations on this issue.
- Develop and promote a common legal framework for network security including setting a proper legal environment for CERT work.

Conclusion

The NRA's ability to enforce national communications laws is vital to bringing the benefits of information and communications technology and services to their country's inhabitants, and to achieving national economic development goals.

In striving to bring high quality, advanced, and affordable communications services to the residents of their individual countries, NRA's around the world, whether in a developing or developed country, are encountering many of the same challenges. And while no two countries are exactly alike, and not all face the same challenges at the same time, most NRA's proceed along the same continuum, working through changes in the market, technology, and applications while learning to deal with ever-growing constituencies – users, consumers, and various governmental ministries -- and adjudicate newer issues such as network security and consumer privacy.

The 97 guidelines suggested in this report are not exhaustive. They may not be applicable in their entirety to a given country. They are intended to be a menu of choices for Member States to consider and use as they find appropriate in their own circumstances. In addition, the experiences and examples of more than 40 countries are presented to further illustrate the challenges to enforcing communications laws that NRAs are facing – and how many are successfully meeting those challenges. Taken collectively, the contents of this report can assist NRAs and other policy makers as they chart their course toward long-held universal access goals.

ANNEX A

Summary of guidelines: common enforcement challenges 2009

Enforcing Competition Laws, Policies, Regulation

- Focus regulation on persistent or unyielding competitive bottlenecks; gradually withdraw regulation elsewhere.
- Negotiate and incorporate terms that are favorable to competition in concession agreements; use renewal periods accordingly.
- Clearly inform operators of the practices that constitute unfair competition in the sector.
- Conduct a public inquiry involving all stakeholders on telecom and ICT national interests, including competition.
- Regulator must make its needs and priorities absolutely clear to the country's authorities.
- Establish strategic partnerships with experts in developed and in other developing countries for training on regulatory matters including competition .
- Conduct an awareness campaign directed at all administrators and politicians explaining the role and validity of the NRA.
- Institute a National Competition Council.

Enforcing Interconnection Laws, Policy, Regulation

- In an open and competitive market, permit operators to negotiate access and interconnection arrangements between themselves.
- Operators which receive requests for access or interconnection should in principle conclude such agreements on a commercial basis, and should negotiate in good faith.
- In markets where there continues to be large differences in negotiating power between undertakings, and where some undertakings rely on infrastructure provided by others for delivery of their services, provide NRAs with sufficient power to secure, where commercial negotiation fails, adequate access and interconnection and interoperability of services in the interest of end-users.
- NRAs can publish Reference Interconnection Offers or model interconnection agreements on their website to help ensure that all competitors are aware of terms and conditions.
- An interconnection agreement should include:
  - **Price.** Define the initial level of interconnection charges, the currency in which they will be paid, and how prices will adjust over the term of the agreement to account for exchange rate changes and inflation. Define liability for bad debt and uncollectible bills.
  - **Points of interconnection**. Define the physical locations where interconnection will take place and the technical standards to be employed. Establish a process for requesting and obtaining additional points of interconnection.
  - **Transport charges and traffic routing**. Define the proper routing and hand-off point for each type of call, as well as the applicability of transport charges in the receiving network for calls that must be carried beyond the area local to the point of interconnection.
  - **Quality-of-service standards**. Define quality standards, particularly the time to provide circuits and for call blocking levels. Define the remedy for when those standards are not met. Testing opportunities should be provided to each party.
  - **Billing and collection.** Define when and how to collect traffic data, exchange bills, and make payment. Develop a process for reconciling traffic data and making inquiries to the other party, and for handling claims.

- **Traffic measurement and settlement.** Define the responsibilities of each interconnecting operator to measure traffic along with settlement procedures to resolve discrepancies. Specify obligations to cooperate in fraud detection and enforcement activities.
- **Numbering resources**. Define each operator's access to the country's numbering plan and numbering resources.
- **Forecasting network needs**. Develop and define a process for interconnecting operators to plan, agree, budget for, and install additional capacity to meet forecasted demand. Define procedures to resolve differences over forecasts, as well as what constitutes a bona fide request for additional interconnection capacity. At a minimum, include a mutual obligation to notify the other party well in advance of network changes and upgrades to avoid disadvantaging one competitor over another.
- **Access to customer information**. Define limits on the permitted uses of this information particularly regarding marketing activities approaching another operator's clients based on information obtained through interconnection activities. Include safeguards to protect customers' privacy.

• Interconnection pricing should:

- encourage efficient competition and the efficient use of, and investment in telecommunications networks;
- preserve the financial viability of universal service mechanisms
- treat technologies and competitors neutrally;
- allow innovation; and
- whenever possible, minimize regulatory intervention.

Enforcing Site (network infrastructure) Sharing

• GSR 2008 Guidelines are shown here with closed bullets; Guidelines derived from the Rapporteur/Study Group consultative process are shown here with open bullets.

• It is important that implementation of sharing takes into account the necessity to protect the value of existing investment in infrastructures and services.

• [O]ffering shared facilities must not be biased towards any specific service provider or types of services.

• [R]egulatory policy [should] not prevent competing market players from installing their own independent facilities.

• Regulatory policy]… should promote open access to international capacity and international gateways.

• [E]stablishing Internet Exchange Points could also encourage shared and more affordable access to national and international broadband capacity for Internet service providers willing to enter the market.

• Pricing for shared facilities should help operators make reasonable and commercial "build-or-buy" decisions; it should provide an incentive for investment in infrastructure, but should not act as an artificial barrier to entry for new market players.

• Non-replicable resources such as towers, ducts and rights of way can be shared for installations that serve a similar purpose.

• Shared-use [spectrum] bands could be promoted as long as interference is controlled.

• Regulators could consider licensing or authorizing market players that only provide passive network elements, but which do not compete for end-users, (e.g., mobile tower companies, fiber backhaul providers).

• [I]nfrastructure sharing [must] take place on a neutral, transparent, fair and non discriminatory basis…

- [I]nterconnection frameworks can ensure that all licensed operators… can… interconnect… and can… encourage the sharing of essential facilities…
- Establishing a 'one-stop-shop' would facilitate… coordination of trenching and ducting works between telecommunications service providers [and]… between telecommunications service providers and those of other utilities.
- [T]ransparent processes [are required] to facilitate infrastructure sharing, and market players need to know what is available for sharing under clearly established terms and conditions. [This could be facilitated by website] publication of existing [and] future infrastructure installations available for sharing… [e.g.] the availability of space in existing ducts, planned deployment, or upgrading works and interconnection.
- [R]egulators should introduce necessary enforcement tools to ensure compliance and successful adoption of infrastructure sharing regulations, [e.g.]… alternative dispute resolution mechanisms… to encourage negotiated outcomes… [along with]… maintaining the certainty of an adjudicated decision where necessary.
- [R]egulators can consider the introduction of incentives for service providers that share infrastructure as part of their efforts to deploy to rural and underserved areas…, e.g., [appropriate] regulatory exemptions, or financial subsidies.
- [S]haring should be encouraged… within the boundaries of the Telecommunications/ICT and Broadcasting industry, [and]… with other infrastructure industries (…electricity, gas, water, sewage, etc.).
- [J]oint infrastructure building with other market players and… other industries may be encouraged, providing for timed, organized opportunities for access to ducts and conduits… to distribute the cost of civil works among service providers… reduce… inconvenience… in towns and cities… [and]… provide… a positive environmental… impact…
- [There is a]… need for an appropriate level of international and regional harmonization to ensure that best practice regulatory policies on sharing are [widespread]…
  - Regulators can consider a two-tier strategy: encourage sharing works, rights of way and passive infrastructure (e.g., ducts, masts, towers), and treat other levels of service provision with caution – as conditioned transitional arrangements designed to achieve specific objectives.
  - NRAs or operators can employ a Reference Conduit Access Offer (RCAO) including price, deadlines and standard procedures.
  - Operators or NRAs can maintain and update a database describing the utilized and available conduits and associated infrastructure.
  - NRAs can provide grants or subsidies from the universal service fund to encourage network rollout to rural areas where towers are shared by several competitive operators.
  - NRA's can coordinate and conduct consultations with government utilities and private entities such as power, transport, railways, broadcasting, or electricity, to identify opportunities to obtain rights of way and horizontal corridors that may be used by telecommunications service providers.
  - NRA's can approach municipal governments, relevant offices in related Ministries and other stakeholders, whether public or private, to coordinate and implement activities for sustained infrastructure development.
  - NRA's can conduct consultations with operators from the telecommunications sector and operators of other networks, e.g., railways, broadcasting, or electricity, to coordinate passive

Enforcing Spectrum Policies, Rules and Regulations

Suggested Guidelines indicated with closed bullets are taken from ITU-R National Spectrum Management Handbook, Annex 2, Best Practices for National Spectrum Management. Guidelines indicated with open bullets summarize best practices emerging from the consultation process on this question.

- Establish and maintain a national spectrum management organization, either independent or part of the telecommunication regulatory authority responsible for managing the radio spectrum in the public interest.
- Promote transparent, fair, economically efficient, and effective spectrum management policies, i.e., regulate the efficient and adequate use of the spectrum, taking into due account the need to avoid harmful interference and the possibility of imposing technical restrictions in order to safeguard the public interest.
- Make public, wherever practicable, national frequency allocation plans and frequency assignment data to encourage openness, and to facilitate development of new radio systems, i.e., carry out public consultations on proposed changes to national frequency allocation plans and on spectrum management decisions likely to affect service providers, to allow interested parties to participate in the decision-making process.
- Maintain a stable decision-making process that permits consideration of the public interest in managing the radio frequency spectrum, i.e., provide legal certainty by having fair and transparent processes for granting licenses for the use of spectrum, using competitive mechanisms, when necessary.
- Provide in the national process, in special cases where adequately justified, for exceptions or waivers to spectrum management decisions.
- Have a process for reconsideration of spectrum management decisions.
- Minimize unnecessary regulations.
- Encourage radiocommunication policies that lead to flexible spectrum use, to the extent practicable, so as to allow for the evolution of services and technologies using clearly-defined methods, i.e.:
  (a) eliminate regulatory barriers and allocating frequencies in a manner to facilitate entry into the market of new competitors,
  (b) encourage efficiency in the use of spectrum by reducing or removing unnecessary restrictions on spectrum use, thereby encouraging competition and bringing benefits to consumers, and
  (c) promote innovation and the introduction of new radio applications and technologies.
- Assure open and fair competition in the marketplaces for equipment and services, and remove any barriers that arise to open and fair competition.
- Take note of procedures for registering earth station terminals in the International Frequency Register (MIFR) and use this existing tool to mitigate interference as new systems are planned for deployment.
- Collaborate with regional and other international regulatory authorities/policymakers to develop coordinated regulatory practices to avoid harmful interference, including mechanisms for holding cross-border coordination meetings to ensure harmful cross-border interference is avoided.
- Harmonize, as far as practicable, effective domestic and international spectrum policies, including of radio-frequency use and, for space services, for any associated orbital position in the geostationary-satellite orbit or of any associated characteristics of satellites in other orbits.
- Work in collaboration with regional and other international colleagues to develop coordinated regulatory practices, i.e., work in collaboration with regulatory authorities of other regions and countries to avoid harmful interference.
- Remove any regulatory barriers to free circulation and global roaming of mobile terminals and similar radiocommunication equipment.
- Use internationally recommended data formats and data elements for exchange of data and coordination purposes, e.g., as in the Radio Regulations Appendix 4, and in the ITU Radiocommunication Data Dictionary (Recommendation ITU-R SM.1413).
- Use “milestone” management steps and phases to monitor and control lengthy radiocommunication system implementation.
- Adopt decisions that are technologically neutral and which allow for evolution to new radio applications.

- Facilitate timely introduction of appropriate new applications and technology while protecting existing services from harmful interference including, when appropriate, the provision of a mechanism to allow compensation for systems that must redeploy for new spectrum needs.
- Consider effective policies to mitigate harm to users of existing services when reallocating spectrum.
- Where spectrum is scarce, promote spectrum sharing using available techniques (frequency, temporal, spatial, modulation coding, processing, etc.), including interference mitigation techniques and economic incentives, to the extent practicable.
- Use enforcement mechanisms, as appropriate, i.e., apply sanctions for non-compliance with obligations and for inefficient use of radio frequency spectrum under relevant appeal processes.
- Utilize regional and international standards whenever possible, and where appropriate, reflect them in national standards.
- Rely to the extent possible on industry standards including those that are included in ITU Recommendations of in lieu of national regulations

Enforcing Regulations that Protect Consumers

- Survey users and consumers to obtain their opinions and views about service and other issues; hold public meetings for this purpose as appropriate;
- Encourage and facilitate the creation of independent associations that will represent users and consumer's interests;
- Encourage and facilitate the creation of a unit within the operators that is dedicated to addressing and resolving consumer issues;
- Create a unit within the NRA that is dedicated to addressing and resolving consumer issues.
- Ensure that regulators and the regulatory framework take into account the opinions and views of consumers and consumer associations;
- Provide notice to users and consumers of telecom/ICT decisions that affect them.
- At the European and international level, foster the development of guidelines, recommendations, or standards if appropriate, specifying a retention period for personal data.

Enforcing Quality of Service Policies and Regulations

- Publish complaints received about service quality.
- Use operator skills and customer opinions through widespread consultations, working groups, and open meetings.
- Measurements should be important to customers, practical for operators, and comparable between operators. They should concentrate on a few aspects of services.
- Measurements that are published should be accessible to customers, helpful to customers and fair to operators.
- The measurements should be reviewed, to see whether they need to be changed, as the market changes and different aspects of services become most important.
- The measurements should not require more tests and calculations than are likely to be needed to characterize differences in quality that are perceptible to customers, now or in the future.
- The measurements should be the same as or similar to ones that operators already make (or will benefit from making) for their own purposes, if possible.
- The measurements should deal with matters that operators can control.
- Any targets set should be useful to customers and realistic for operators. They are most likely to be desirable for wholesale services and retail services of dominant operators.

Enforcing Network security Policies, Guidelines, Regulations

- Proactively deal with security challenges.

- Develop and practice close cooperation between the domestic public and private sectors.
- Give special attention to management of security incidents through CERT groups.
- As network and information security issues go far beyond the boundaries of one country or a particular region, engage in international cooperation.
- Conduct awareness raising campaigns on safeguarding measures and building a culture of cyber security on the international level.
- Recognize and participate, as appropriate, in the efforts made by various international organizations on this issue.
- Develop and promote a common legal framework for network security including setting a proper legal environment for CERT work.

ANNEX B

Index of country/industry examples and references

ANNEX C

Summary of enforcement guidelines 2006[214]

National Regulatory Authorities (NRAs) play a central role in executing domestic communications policy. The means and power to enforce those regulations, however, is not an end in itself. It is one of the critical ways for an NRA to achieve its chief goal: facilitate universal access and service to its citizens by enabling industry growth and worldwide competitiveness.

The following guidelines suggest a range of options that may be applied in diverse circumstances to assist ITU Member States' efforts to enforce their domestic telecommunications laws. NRAs are encouraged to review the guidelines and select those which will be useful in their domestic circumstances. Concepts of regulation that are inapplicable, or practices or solutions that are not suitable in one country may work well in another. We trust that this "menu" of choices will assist Member States as they facilitate delivery of a robust communications sector that is capable of providing benefits to all.

1. Enforcement Powers – Legislation

Most regulatory authorities derive their power to enforce regulation from their domestic enabling legislation. Many also promulgate rules and regulations of their own that carry out the legislature's stated goals. Some place conditions for enforcement or even enforcement mechanisms themselves in the licenses they issue. Regardless of the source, it is clear that without the proper authority for an NRA to enforce laws, a regulatory regime is likely to fail to achieve its policy objectives: promote competition, growth, and investment in the sector for the benefit of users and consumers. Accordingly, NRAs are encouraged to:

- As appropriate, NRAs should seek to provide written input to the law making body on ways to improve the efficiency and substantive applicability of the law.
- Ensure harmony between the constitution, legislation, and administrative powers. Identify change as necessary.
- Ensure that the telecom law provides sufficient authority, independence, and financial resources for the NRA to gather information to impartially, swiftly, and transparently carry out the will of the legislature.
- Ensure that the telecom law provides sufficient authority, independence, and financial resources for the NRA to acquire the human and financial resources (via state budget, or NRA self funding) to impartially, swiftly, and transparently carry out the will of the legislature.
- Ensure that the law contains clear and unambiguous language describing the jurisdiction of the NRA and, where appropriate, other interested state agencies.
- Where there is more than one entity with jurisdiction over telecommunication matters, provide for and describe a coordination mechanism between these entities.
- Ensure that the law promulgated is clear, transparent, and precise. Avoid technical terms that are not understandable by the public or that may be unclear before a reviewing court. Define terms as far as practicable.
- In preparing legislation, gather the opinions of primary stakeholders. Organize meetings to review and discuss draft legislation before it is submitted for adoption.

---

[214] *See, Domestic enforcement of Telecommunications Laws: Guidelines for the International Community ITU-D Question 18/1*, http://www.itu.int/pub/D-STG-SG01.18-2006/en. These Guidelines are a product of the Rapporteur Group's analysis and discussion of individual country experiences shared in written contributions and in meetings and seminars arranged by the ITU Development Bureau. These events brought together roughly 100 people from 70 countries to contribute their ideas and views.

- To the extent possible, promulgate laws that can address new technology; give broad powers to the NRA to adjust to changes in the industry.
- Describe the objectives and rationale of promulgated laws to induce enforcement and compliance by all parties, including enforcement agents of the state.
- Ensure that users/subscribers/consumers[215], operators, and service providers have recourse at the regulatory agency.
- Ensure jurisdiction over service providers who may not be licensed.
- Ensure that the enabling law/legislation provides the NRA with a wide range of penalties to include those appropriate for minor, mid range, and maximum offences.
- Ensure that all stakeholders are made aware of the law and the responsibility of the NRA to enforce the law. Conduct awareness-raising activities such as seminars, lectures, publication of short brochures, and trainng materials on the law for magistrates.

2. Enforcement Practice & Process; Resolution Of Disputes

Second only in importance to an NRA's enabling act or statute are the day-to-day practices and procedures it employs to implement the law. It is essential to have processes in place that enable swift and fair adjudication of violations and complaints. Transparency in these procedures will facilitate compliance and is necessary for NRA decisions to gain public trust and withstand judicial, ministerial, or royal review. Accordingly, NRAs are encouraged to:

- Develop and publish procedures for the NRA's internal operations and its external public functions that reflect fairness, speed, efficiency, and transparency goals.
- Design and employ transparent procedures that enable the NRA to render and publish a decision that considers all relevant facts and law, including, as appropriate, the views of all different stakeholders in the sector.
- Consult, as appropriate, the different stakeholders in the sector on issues involving decisions made by the regulator.
- Observe relevant legal precedent.
- Adopt procedures to protect confidential or commercially sensitive information provided by operators, service providers, or other licensees to facilitate the supply of information necessary to evaluate compliance with laws, policies or regulations.
- Identify areas where the actions of other interested public authorities (e.g., courts, local representatives, administrative authorities) frequently or significantly affect NRA enforcement processes. Where feasible and appropriate, develop a plan for communication, coordination, and cooperation with the goal of facilitating equitable and speedy resolution of violations.[216]

---

[215] The meaning of the terms user, subscriber, and consumer may differ from country to country. In this context, user/subscriber/consumer refers to each of these groups including the general public.

[216] Good examples of this approach include actions taken by **Uganda**, **Peru**, **Brazil, Mexico, and Colombia.** Noting that under the law only the Director of Criminal Prosecutions could prosecute criminal offences under the Communications Act, and wishing to minimize any potential administrative delay or other inefficiencies, **Uganda's** NRA, UCC, petitioned the Director of Criminal Prosecutions for authority to prosecute criminal offences under the Communications Act and won this authority. As a result, UCC compliance efforts in this area are less complex.

Recognizing that coordination with the judiciary is essential to successful enforcement of its telecom policies and laws, **Peru's** NRA, OSIPTEL, sponsored a 1-week training course in Lima for 30 – 40 judges at the end of 2003 covering highly specialized communications issues. In **Colombia** and **Brazil**'s ANATEL have also sponsored similar seminars for the judiciary. In 2003, **Mexico'**s COFETEL provided technical training for new judges on mobile quality regulations. Such outreach efforts serve to familiarize the judiciary with telecommunications issues, procedures, objectives, and personnel, and to expose the NRA to the court's procedures, objectives and views. As a result, inefficiencies are minimized, and the necessary coordination between these institutions on communications issues is optimized. *See* Rapporteur's Report: Meeting of the Rapporteur's Group on ITU-D Question 18/1, Rio de Janeiro, 21-22 April 2004 (ITU-D/1/RGQ18/024(Rev.1)-E at 3.

- Consider employing a variety of tools for investigation to include letters of inquiry, on-site inspections, subpoenas, or summons.
- Insofar as possible, use technology to facilitate speedy but deliberative decision-making, and subsequent publication of these decisions.
- Place decisions and comments on the web.
- Consider placing the burden to produce information needed by the NRA upon service providers/licensees to compensate for limited staff and resources. Make this information public so that competitors and consumers can notify the NRA if they believe the information is inaccurate or otherwise flawed.
- Consider publishing a standard format for gathering information from regulatees and for receiving complaints from consumers.
- Prepare internal, standardized work sheets, in electronic format if possible, for NRA staff to gather information from regulates, render a decision on license applications or other line processing work, and review complaints from consumers to assist the NRA in ensuring that all issues have been reviewed and relevant rules have been complied with.
- Consider encouraging self-reporting by regulates; this can lower enforcement costs, reduce the risk of harm, or mitigate harm.
- When establishing penalties, seek to minimize the cost of compliance with regulations for business users and consumers.
- Develop and maintain a database or other appropriate record keeping system to track violators and violations for use in reporting to the government and the public, tracking industry trends, and in setting future penalties or sanctions.
- Consider employing a voluntary compliance scheme featuring industry self-regulation as a low-cost, potentially low-risk alternative to, or supplement for, formal enforcement processes. Such rules can either be operational or consumer focused, and though developed by industry, should reflect current government objectives.
- Information about which companies have agreed to follow voluntary standards or rules should be made publicly available.

3. Independent Decision Making

NRA-issued decisions that are considered to be independent are widely believed to be the most desirable and widely respected. When an NRA has the authority and freedom to render a decision that: (i) is based on all relevant facts; (ii) applies and implements the appropriate law, policy, or regulation; and (iii) is free of undue pressure from political entities, powerful incumbents, or others having a stake in the outcome, it can be said that its decisions are independent. In short, an impartial NRA decision is an independent decision. Accordingly, NRAs are encouraged to:

- Design transparent procedures that enable the NRA to render and publish a decision that considers all relevant facts and law.
- Identify and institute internal and external procedures to facilitate impartial decision making.
- Revise current procedures, if necessary, to implement a process designed to reach impartial decisions that include public participation.

4. Sanctions and Penalties

Having established that the NRA: (i) has the authority to act; (ii) has determined culpability of a violator through a fair, expeditious, and transparent process; and (iii) rendered an independent decision on the matter, the NRA is now prepared to impose sanctions. Accordingly, NRAs are encouraged to:

- Ensure that the NRA has authority to impose a wide range of penalties that include minor, mid range, and maximum.

- In determining a sanction, consider the severity of the harm, the probability of detection, the risk sensitivity of the offender, and the cost of enforcement.
- Risk aversion of injurers should usually lower the level of the fine.
- Establish and employ sanctions that are reasonable (proportional to the offence) and effective, but high enough to deter wrongdoing and achieve compliance with rules.
- Consider imposing a fine that exceeds the benefit the offender received from committing the offence.
- Considering the cost of enforcement, seek effective alternatives to fines (for example employ voluntary industry compliance schemes, or include specific requirements in license obligations).
- Consider providing a range of responses to violations including, *e.g.,* warning letters, fines, consent decrees, preventive cease and desist orders, license revocation, equipment seizure, damage awards, and referral for criminal prosecution.
- Consider developing, publishing, and employing specific but flexible guidelines for determining the severity of a sanction as these can deter violations of important rules and can assist the NRA in developing priorities among different violations.
- Consider setting a fine that represents a percentage of the offender's revenues as this may permit regulators to discipline market players without seriously undermining small, non-dominant operators.
- Consider employing the strictest penalties available to the NRA for offences involving misrepresentation.

5. Gender and Enforcement

The importance of ICT as a tool to promote the full participation of women in the information society has been widely recognized. Identifying and enforcing those domestic communications policies and rules that address women's access, use, and participation in ICT can help implement domestic objectives to reverse existing inequalities for the benefit of the communications sector and society as a whole. Accordingly, NRAs are encouraged to:

- Adopt and promote a formal commitment to gender equality.
- Develop and maintain an awareness of the data available that reflect how enforcing telecom policy can impact gender. For example, gender-disaggregated statistics on access and use, incomes, differential impact of costs and technology choice, and on employment and entrepreneurship. If possible, collect such data for the NRA's domestic market.
- Identify, support, and enforce those domestic policies and rules that would increase women's access, use, and participation in ICT and ICT services (e.g., rural build-out requirements, universal access targets or other connectivity schemes, particularly those that promote user-friendly technologies for low literacy/illiteracy levels, technology access points located near places frequented by women, or low cost technology recognizing disparities in wages).
- Promote gender analysis as part of the policy process so that the policies described above can be identified.[217]
- Create, support, and enforce internal NRA procedures that encourage gender equality.
- Involve women regulators and policy makers in analyzing and resolving the impact certain regulations may have on gender including proposing ways to achieve balance.

[217] International Telecommunication Union, "Gender Aware Guidelines for Policy making and Regulatory Agencies", http://www.itu.int/ITU-D/gender/projects/FinalGendAwrnGuidelns.pdf, at 2.

6. Organization and Resources

It is advisable for an NRA to understand its national communications priorities so that it can configure and maintain an organizational structure to accomplish important state goals. Where staff and other resources are too severely limited to meet this minimum aim, an objective basis exists for reallocating existing resources or seeking additional support, e.g., regulatory fees, additional allocations from state budgets, or other sources.

- In devising its organizational structure to enforce telecom law and policy, it is advisable for an NRA to:
  - Know national and regional priorities;
  - Assess and seek resources needed to enforce regulations that implement national priorities; and
  - design the organization so that it can support activities that implement national priorities.
- The NRA is encouraged to seek human, technical and financial resources needed to enforce regulations that implement the country's national telecommunications priorities.
- Hire and retain multidisciplinary experts (legal, economic, technical).
- Employ interdisciplinary teams for competency reinforcement and skill development;
- Consider, if possible, allocating a significant portion of the NRA's resources to enforcement efforts.
- Consider dedicating separate staff for enforcement efforts.
- Target internal training to enhance the capacity of the NRA's staff to address consumer, market competition, and technical issues.

Printed in Switzerland
Geneva, 2010

Photo credits: ITU Photo Library