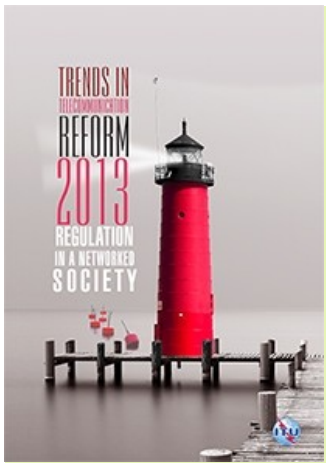
12th Global Symposium for Regulators (Colombo, 2012)

Why regulate in a Networked Society?

Discussion Papers

GSR 2012 Discussion Paper

Net neutrality: A regulatory perspective



Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 19 October 2012.

The views expressed in this paper are those of the author and do not necessarily reflect the opinions of ITU or its Membership.

TABLE OF CONTENTS

1 NET NEUTRALITY: A REGULATORY PERSPECTIVE

Author: Malcolm Webb, Partner, Webb Henderson[1]

Summary

This paper considers net neutrality – the principle that all electronic communication passing through a network is treated equally – in the context of an environment where traffic management, in varying forms and in varying degrees, is ubiquitous. It sets out an overview of these traffic management measures and the factors driving their use. That not all of these measures – despite each contravening a pure concept of "neutrality" – are considered problematic suggests that concerns over the particularly controversial measures may instead stem from a broader issue, such as non-discrimination or the appropriate use of market power.

To the extent that some traffic management practices do raise potential concerns, the regulatory response should be – as it is with all issues – proportionate and evidence-based. In practice, this is likely to mean that reliance on existing regulatory frameworks and market-based mechanisms is an appropriate initial response in many instances. If harmful traffic management continues, refinements may be necessary, particularly to improve transparency and reduce switching costs for consumers and, potentially, introduce powers to restrict specific behavior such as blocking and unreasonable discrimination. A representative study of jurisdictions where net neutrality issues have been prominent is consistent with this approach, and this paper categorizes these graduated responses to net neutrality issues as:

- **Cautious observation**: countries that have taken note of net neutrality issues and have currently chosen not to take any specific measures to address these issues;
- **Tentative refinement**: countries that have adopted a light handed approach, with some refinements to the existing regulatory regime governing communications services, but not going so far as to prohibit certain behaviors; and
- **Active reform**: countries that have gone further and sought to prohibit specific behaviors by ISPs, often subject to reasonable network management practices.

Beyond this framework, the paper considers contextual factors that affect how net neutrality is treated under existing – and potential future – regulation, including the industry's response to net neutrality concerns, the International Telecommunications Regulations, the relevance of investment and future regulatory and business models. As much as possible, reference has been made throughout this paper to the research and empirical findings by national and international ICT regulators, including the Body of European Regulators for Electronic Communications (BEREC), the European Commission, the Federal Communications Commission (FCC), Ofcom and others.

This paper fleshes out the net neutrality debate in an effort to provide national ICT regulators with information and tools to address net neutrality and traffic management in their home jurisdictions. This discussion will conclude with recommendations and a checklist of best practices to guide national regulators, in both developed and developing countries, as they navigate a debate which, despite being centered on neutrality, has seen a remarkable level of polarization.

1 Net neutrality and traffic management

There is a general consensus that there is no one, commonly accepted, definition of net neutrality. This section will present some of the more widely used interpretations of net neutrality and describe the traffic management measures taken by ISPs that contradict the purest ideal of a neutral network.

1.1 What is net neutrality?

In the absence of a standardized definition of net neutrality, BEREC has used the following description of net neutrality:

A literal interpretation of network neutrality, for working purposes, is the principle that all electronic communication passing through a network is treated equally. That all communication is treated equally means that it is treated independent of (i) content, (ii) application, (iii) service, (iv) device, (v) sender address, and (vi) receiver address. Sender and receiver address implies that the treatment is independent of end user and content/application/service provider[2]*.*

Another definition, by Tim Wu, has been described by BEREC as "one of the most famous":

Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites and platforms equally. This allows the network to carry every form of information and support every kind of application.[3]

Other net neutrality proponents argue that net neutrality means ensuring that all services are provided to all parties over the same quality of Internet pipe, with no degradation based on the service chosen by the end user and at the same cost. This definition is based on the assumption that data is transmitted on a "best efforts" basis, with limited exceptions.[4]

1.2 Traffic management: a threat to net neutrality?

1.2.1 What is traffic management?

These broad definitions of net neutrality are being challenged by the reality of an Internet which does require some traffic management to ensure efficient operation for all users and to prevent degradation of service. Traffic management is now widespread and generally accepted, including by BEREC, as a necessary tool that can benefit both content and application providers (CAPs) that rely on the public internet and the end users that expect a QoS when they surf the internet. As BEREC put it, in reference to the above definition:

There have been and continue to be deviations from this strict interpretation. Some of these deviations may well be justified and in the interests of end-users but other forms could cause concern for competition and society. To assess this, NRAs will need to consider a wider set of principles and regulatory objectives.[5]

Most ISPs now have equipment in place that can detect what customers are using their connections for. They can tell the number of websites that a customer visits, or whether those customers are using their connection for online gaming or video streaming, or for other peer-to-peer software, such as Skype or BitTorrent. It is now common for ISPs to direct speeds or bandwidth to different types of applications, making one, such as e-mail, faster while slowing another, such as BitTorrent.

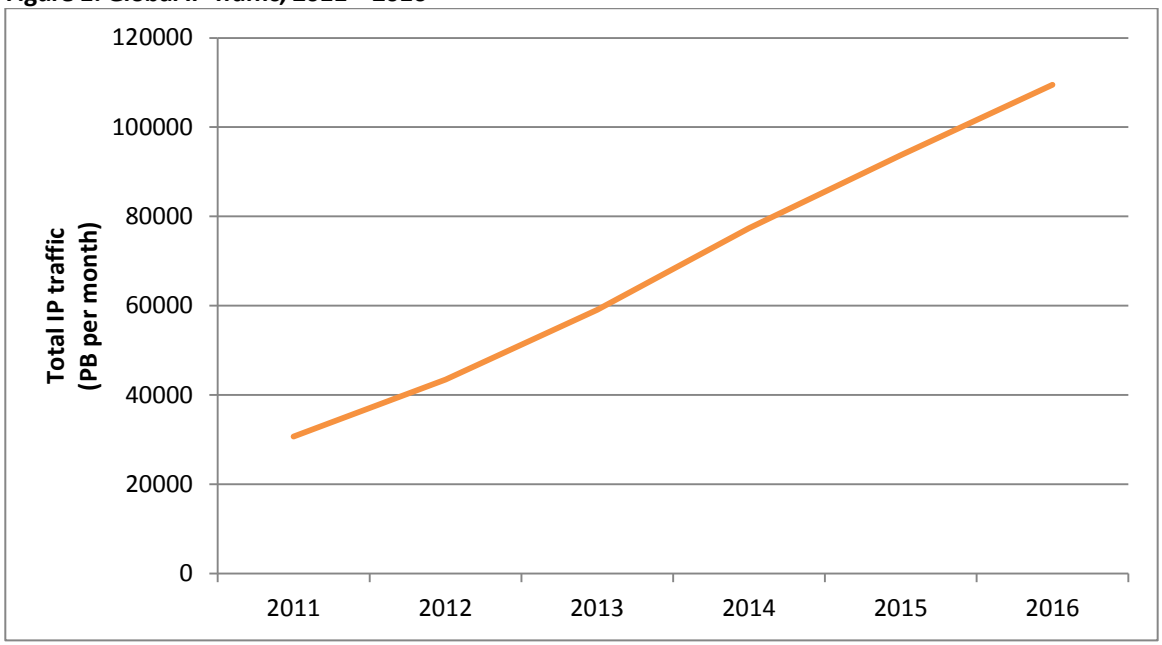
Traffic management can be broadly defined as a collection of techniques that may be used by an ISP to plan and allocate available resources to attain optimum performance for diverse classes of users across a network. These

techniques will often include the use of performance measures to define optional service levels tailored to different user needs, and to assure appropriate quality of service. Traffic management is critical for the proper functioning of the Internet, but it can also be misused by an ISP to create unfair access or use of the Internet.[6]

1.2.2 Reasons for traffic management

The primary reason that is given by ISPs for traffic management is to prevent a small number of their customers from clogging up access to the Internet by using a disproportionate share of the available bandwidth. In this way, proponents of traffic management say that ISPs are justified in controlling the flow of data because it is necessary to maintain the quality of service that is required to ensure all users have an enjoyable browsing experience. Figure 1 illustrates the exponential growth in global IP traffic that is forecast to take place in the coming years.

Figure 1: Global IP Traffic, 2011 – 2016



Source: Cisco, 'Cisco Visual Networking Indexing: Forecast and Methodology, 2010-2016' (30 May 2012), 6.

This forecast rise in demand has significant implications for ISPs and, upstream, wholesale service providers and network operators. The two most obvious likely responses to this growth are traffic management, to manage a greater amount of data using a similar level of capacity, and/or additional investment in upgrades to increase the total network capacity. It is worth pausing to consider that these options, while rational, would not ordinarily be the first-choice response of a generic firm facing a considerable increase in demand. In almost any other industry, a substantial rise in demand would be met with glee and a similarly substantial rise in price (at least until new entrants could enter the market). ISPs are suppliers in a market where prices have dropped over time even as demand and quality has improved; leaving ISPs in the somewhat unique position of facing strong growth forecasts, not with anticipation but with an apparent air of trepidation.

Much of the strongest concern relates to convergence, which has seen ISPs and CAPs increasingly crossing into the traditional territory of the other. CAPs, like Skype and Viber, offer VoIP services that can act as a substitute for the voice telephony services of ISPs that carry their content. Conversely, some ISPs have begun to provide IPTV services that compete with the content of broadcaster CAPs.

This increasing competition can provide incentives for ISPs with significant market power (SMP) to misuse that market power and limit competition from CAPs through discriminatory activities, such as blocking and throttling of the competitive service, in favor of the ISP's own product. ISPs have a key intermediary role between CAPs and end users; neither can reach the other online except through an ISP.

An ISP pre-determining the rate of throughput based on data type contravenes the principle of equal treatment of data. The primary justification for prioritization is to ensure that key services, such as business or other critical services, have reliable access to the network. However, the ability to differentiate between data types also raises the possibility of more questionable discriminatory behavior, which may arise when ISPs have an incentive to prioritize their own services or applications for their own benefit.

The broad recognition of the need for at least some traffic management measures poses difficulties for bright-line regulation; it may not be easy for regulation to clearly and preemptively distinguish between "reasonable" traffic management and measures that justify regulatory intervention.

This section of the paper sets out a more comprehensive list of the range of traffic management techniques available to ISPs, including those generally viewed as innocuous. Although some of these actions will raise more concerns than others, the intent behind listing them is not to enable the sketching of a line demarcating "reasonable" from unacceptable traffic management. The appropriateness of a particular action by an ISP should be considered on its facts, not by its categorization. This paper sets out these traffic management measures for two reasons: first, to inform and set the context for the discussion that follows; and second, to illustrate the ubiquity of traffic management against pure net neutrality.

1.2.3 Traffic management techniques

- **Data caps**: A wide variety of data caps and "fair use" policies may be used by operators to implement a specific business model. In general, a data cap will be imposed to support the operator's pricing strategy, so that the price of traffic is based on volume.

  Data caps are a technical measure that requires monitoring traffic volume and throttling data or charging for extra volume once a pre-defined data cap is reached. Data caps provide a price signal to end users in relation to the cost of their bandwidth consumption. Once a data cap has been reached, several measures may be applied:

  - a speed limit may be activated (e.g. restricting transmission data down to a pre-determined transfer rate);
  - access to the network may be temporarily stopped or suspended; or
  - customers may be given an opportunity to buy extra data volume.[7]

  Data caps tend to be applied indiscriminately. As such, BEREC have argued that limiting data volume or the rate of throughput independent of data types does not technically conflict with the principle of net neutrality.[8] It is only when specific restrictions are tied to the cap as an incentive to attract customers that a data cap may present a problem.

- **Application-agnostic congestion management**: To respond to network congestion, an ISP can react to daily fluctuations or unexpected network environment changes by implementing "congestion controls" at the edge of the network, where the source of the traffic (e.g. computers) slows down the transmission rate when packet loss is occurring. [9]

- **Prioritization:** An ISP might prioritize transmission of certain types of data over others (most often used to prioritize time-sensitive traffic, such as VoIP and IPTV). ISPs may be required to prioritize emergency services, and this is generally not a concern from a net neutrality perspective.

- **Differentiated throttling**: The capacity available for a particular type of content (most often peer-to-peer traffic, particularly in peak times) may be restricted, which preserves capacity for the un-

restricted content. Unlike application-agnostic congestion management, this technique is aimed at a specific type of content; generally a type that is bandwidth-hungry and non-time-critical.

- **Access-tiering:** An ISP may prioritize a specific application or content – for a price to be paid by a CAP. By selling access to a "lane", access providers can generate greater revenue to fund the network investments necessary to handle increasingly bandwidth-hungry services.

  This can be distinguished from prioritization in that access-tiering is typically open to all service providers (that can afford to pay for it) and that it is generally used to promote a particular service provider, rather than a type of content.

  Access-tiering has been criticized for its potential harms to innovation, particularly to start-ups unable to afford the fee. It is also commercially possible that a service prioritization arrangement could be made on an exclusive-by-service basis, to prevent competitors of the preferred CAP from purchasing a similar level of priority.

- **Blocking:** End users may be prevented from using or accessing a particular website or a type of content (e.g., the blocking of VoIP traffic on a mobile data network). Blocking may be implemented to:

  - inhibit competition, particularly if the access provider offers a service that competes with the service being blocked;

  - manage costs, particularly where the cost of carrying a particular service or type of service places a disproportionate burden on the access provider's network; and

  - block unlawful or undesirable content, such as child abuse, viruses or spam. This may be necessary to comply with government or court orders, or done at the request of the end user. The blocking of unlawful and undesirable content generally raises few net neutrality concerns. Lawful interception measures, while not constituting "blocking", are similarly non-controversial from a net neutrality perspective.

Specific restrictions may be applied discriminately or indiscriminately between users and they may be permanent or implemented over certain periods (e.g. peak time). The nature of the restriction will often be contractually disclosed by the ISP, so that the user is made aware that their access to a particular service will be restricted in certain circumstances.

1.2.4 Traffic management concerns

All of these measures are, in a sense, "non-neutral": they mean that different traffic passing through a network is treated differently. The fact that some of these measures have been accepted, even welcomed, while others have been criticized or subject to sanctions, suggests that concerns over these "problematic" categories are derived not so much from their departures from a truly neutral network, but from something broader, such as their departures from the principles of non-discrimination and fair competition (including the abuse of market power).

In particular, the use of traffic management by an operator for anti-competitive purposes by using its control over internet access to discriminate against any competitors that rely on its network has been the subject of greatest concern. As critics point out, that there is a fine line between correctly applying traffic management to ensure a high quality of service and wrongly interfering with Internet traffic to limit applications that threaten the ISP's own lines of business. This discrimination could be through:

- the use of **blocking** technology to completely prevent access to, or use of, a rival's content or application;

- **throttling** a rival's content or application so that the ISP's own service is more attractive in comparison, or conversely, **access-tiering** the ISP's own content and not permitting the competitor to acquire equivalent prioritization;

- even where **access-tiering** is offered widely, discrimination may be problematic if the terms on which access-tiering is offered treat CAPs differently to each other, or differently to the ISP's equivalent content or application, and those differences are not objectively justifiable (e.g., for cost of technical reasons); or

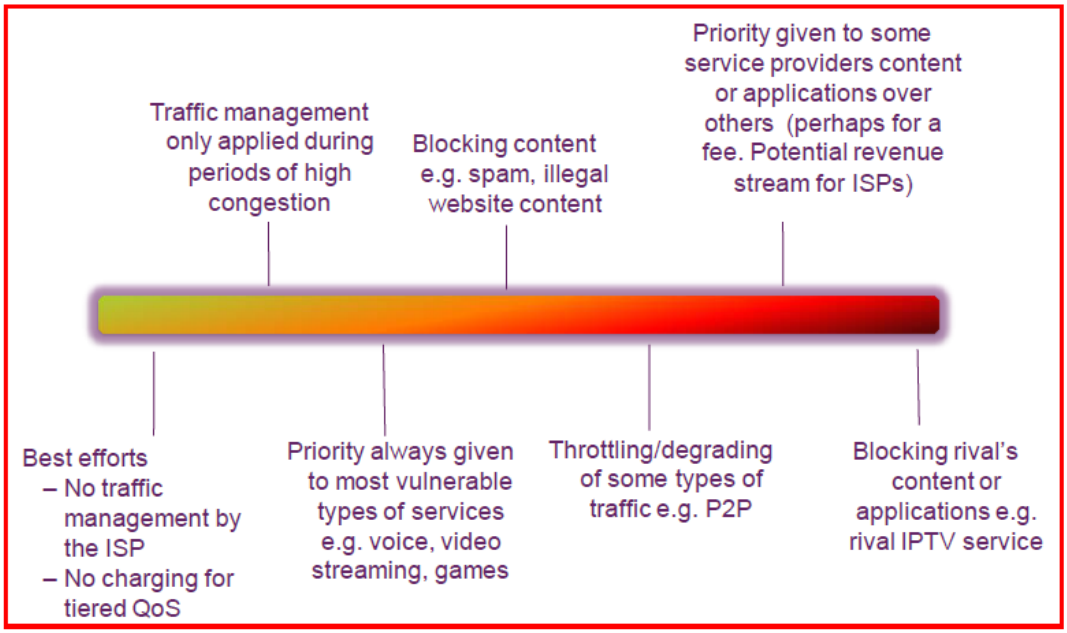
- dedicating so much capacity (either through **access-tiering** or **prioritization**) that the remaining "best efforts" Internet access service is degraded – the so-called "dirt track" issue.

For example, the VoIP application Skype uses peer-to-peer technology to provide free phone calls, which compete directly with the phone services offered by many ISPs. It would be easy at a technical level for an ISP to use its traffic management equipment to limit a customer's Skype experience in an effort to protect its own fixed or mobile telephony services. In BEREC's view, however, blocking VoIP over a mobile network is unlikely to be legitimate from a congestion management perspective. Although the bandwidth required for a VoIP call is roughly 25-30% greater than required for a traditional circuit switched call, and so some capacity is necessary to accommodate VoIP calls, BEREC considered that this use takes up only a small fraction of capacity on the network and so is unlikely to result in a level of congestion that would require traffic management.[10]

In the particular examples to date where intervention has taken place, the intention of the particular measure has been either stated by the parties or the intention of effect has been deemed so obviously inappropriate that regulators and law makers have stepped in. However, intent will often be obscured, and potentially anti-competitive effects difficult to ascertain, making these measures difficult to distinguish from legitimate traffic management policies that can enhance the Internet experience for the vast majority of users. In this regard, moves to regulate and determine appropriate traffic management practices will be particularly challenging.

Ofcom has placed these practices on a spectrum, which shows the progression from traffic management that does not raise concerns (and will generally improve efficiency), to those measures considered more problematic.

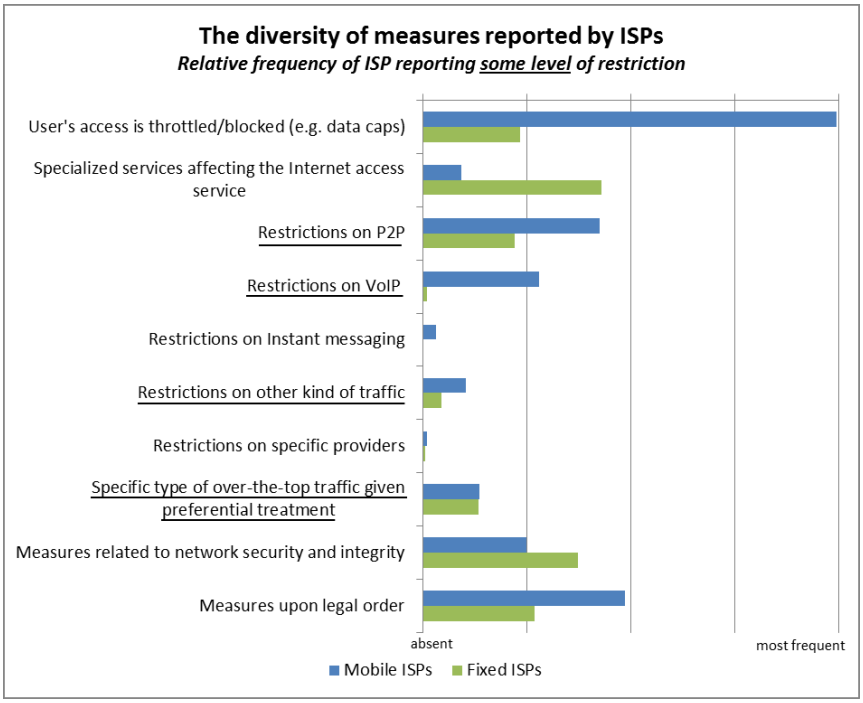
Figure 1: Traffic management conduct



Source: OCFOM, United Kingdom, available online at: *stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf.*

To give an indication of the popularity of traffic management, Figure 2 provides a broad overview of the traffic management measures that were reported to BEREC in its recent survey of 381 operators (266 fixed and 115 mobile) across Europe. When reading this figure, it is important to note that the frequency of ISPs reporting some level of restriction does not necessarily quantify the number of users that may ultimately be affected by a particular traffic management policy. This would depend on factors such as the size of the ISP or whether the restriction is applied to all users or only to some users, etc. However, what this figure does reveal are the similarities as well as the varying restrictions that may be applied by operators (both fixed and mobile).

Figure 2: Overview of traffic management measures by European operators



Source: BEREC, 'A View of Traffic Management and other Practices Resulting in Restrictions to the Open Internet in Europe' (29 May 2012), 13.

1.3 Traffic management technologies

This section will break down the technical issues related to traffic management to help identify what level of operator control over the network is reasonable (and, in some cases, necessary).

1.3.1 Deep packet inspection

Internet traffic is based on the movement of "packets" of data which contain both content (e.g. voice, email, etc.) as well as other information that identifies where each "packet" has come from and where it is going to (among other things).

At the moment, the most important technology for traffic management is deep packet inspection (DPI). DPI equipment inspects the content of packets travelling over an IP network to identify the application or protocol that is in use, which is done by examining the source and destination IP address, the packet payload and the port number of the packet. DPI has become widely deployed because it allows for a relatively fine-grained discrimination among the applications running on an IP network, which allows an ISP to manage traffic at the level of the individual subscriber.

DPI has evolved over time to the point where it now allows ISPs to identify and control the bandwidth available to certain applications in real-time. This effectively means that a packet relating to a particular application or data type may be identified and managed by the ISP in real-time as it travels across the network. This makes DPI a useful tool for traffic management by an ISP, but it also poses an obvious threat to the principle of net neutrality.[11]

1.3.2 Deep flow inspection

Deep flow inspections (DFI) augment DPI by more accurately identifying underlying applications and protocols. DFI makes inferences based on the behavior of the flow of packets rather than looking for protocol signatures or port usage in individual packets. By looking at traffic characteristics, such as rate, shape, size and duration, and uses in conjunction with port numbers, source or destination address and protocol, DFI is being used more and more by ISPs to improve identification.[12]

1.3.3 Policy control and management

Policy control attempts to define the rules for how services are to be delivered and the conditions under which these services are used. In practice, policy control is a broader set of techniques than DPI in that it attempts to manage traffic flows within a structured and standardized architecture, rather than focusing on the contents of individual packets.[13] For example, an ISP could implement a policy that a particular customer be permitted to download unlimited videos after they subscribed to a premium content package.

Policy tools are able to handle a broader range of management tasks more flexibly than DPI. Furthermore, because policy control is more focused on the subscriber than the application, it allows an ISP to tailor its services to an individual user. For these reasons, there has been a rapid growth in the use of policy control and management technologies in recent years.[14]

2 A regulatory perspective: enforcing the principle of net neutrality

There are a number of issues that policy-makers will need to consider when developing a regulatory regime to govern net neutrality. The first, and most important, issue is whether a regulatory response to deal with traffic management is necessary and, if so, what the response should be. This section discusses the range of approaches observed in a number of countries around the world and tries to group these approaches into three different categories. This section also provides an overview of current approaches and perspectives on net neutrality from five leading jurisdictions.

Each country in the jurisdictional review has viewed the issue of net neutrality with an eye to local circumstances, which has resulted in a tailored application of regulation and policy on a country-by-country basis. This raises the question of whether a common set of international rules or principles are needed to allow for greater cross-border collaboration. The focus to date has clearly been at the national level, but the Internet is essentially a global network, so it seems inevitable that at some point there will be a push to extend the regulation of net neutrality from the national to the international level.

This section concludes with a discussion on some broader issues that will also need to be considered by regulators as they consider net neutrality policies.

2.1 Overview of approaches

We have observed three basic approaches to net neutrality issues in the countries we have studied:

- **Cautious observation**: These countries have taken note of net neutrality issues and have currently chosen not to take any specific measures to address these issues;

- **Tentative refinement**: These countries have adopted a light handed approach, with some refinements to the existing regulatory regime governing communications services, but not going so far as to prohibit certain behaviors; and

- **Active reform**: These countries have gone further and sought to prohibit specific behaviors by ISPs, often subject to reasonable network management practices.

	Cautious observers	**Tentative refiners**	**Active reformers**
Measures taken	No specific measures	Light-handed net neutrality measures: e.g., transparency, lowering switching barriers, minimum QoS	Specific net neutrality measures: e.g., no blocking, no discrimination in treatment of traffic
Example countries	Australia Republic of Korea New Zealand	European Commission Japan United Kingdom	Brazil (bill) Chile France Netherlands Singapore USA (FCC rules)

In those countries that are either cautious observers or tentative refiners, there appears to be a degree of confidence that the existing regulatory regime for communications services is adequate to deal with the challenges of net neutrality, or will be adequate with relatively minor "tweaks". There are strong regulatory regimes in countries that are active reformers, but there have been concerns that the lack of open access policies, or effective application of those policies, may have contributed to holding back the retail broadband market in some countries (e.g., in the United States relative to other countries[15]).

2.2 The first step; a competitive retail broadband market

The ability of an ISP to engage in potentially anti-competitive traffic management, without being disciplined by the market, will depend on the degree of market power that it has. The incentive for an ISP to institute these practices, and the attractiveness of particular types of conduct, are likely to be greater where the ISP supplies services that compete with those of the CAPs (VoIP or IPTV for example).

In a competitive retail broadband market, where no single ISP possesses SMP, end users that are adversely affected by traffic management will shift to an ISP with more favorable traffic management practices (all other things being equal). As a result, these practices are unlikely to be sustainable in the long term.

In many countries around the world, there have been regulatory interventions aiming at controlling market power at a wholesale level and promoting competition at the retail level. Open access policies relating to broadband services, such as mandated local loop unbundling, bitstream access and duct access, have been largely successful in many countries in stimulating retail broadband markets, particularly for fixed broadband. These open access policies usually include a general non-discrimination obligation on firms with market power and have been, on occasion, bolstered further by remedies such as functional and structural separation that aim to further control the likelihood of discrimination.

In the telecommunications sector in many countries, *ex ante* regulation is supplemented by *ex post* competition law. Many of the practices that would infringe on the principle of net neutrality will also be considered anti-competitive conduct if a party, such as an ISP, has a dominant position in the market and has abused this position in the operation of its network.

If the regulatory regime for communications services is working effectively to promote retail broadband competition, with the further backstop of general competition law, then a central issue is whether it is necessary to institute specific measures to deal with the types of discriminatory behavior that infringes net neutrality principles.

It could be said that, generally, the cautious observers have decided that the existing regulatory regime is adequate for now. However, it is not a complacent approach by regulators, but is normally accompanied by a close level of ongoing monitoring and observation of net neutrality concerns, to confirm that confidence in the existing regulatory regime is justified.

2.3 Enhancing competition: transparency and switching costs

In the tentative refiner countries, the decision has been made that reliance on the existing regulatory environment for communications may not be fully adequate for addressing net neutrality concerns. Relatively minor refinements have been made to further improve the operation of retail broadband markets, particularly around transparency, so that end users have accurate and relevant information of the traffic management practices of a particular Internet access service, and reduced switching costs, so that end users can easily leave an unsatisfactory service.

BEREC, for example, has focused particularly on the importance of end users being fully informed of the discriminatory practices and that the costs of switching ISPs are low.

2.3.1 Transparency

The United Kingdom regulator, Ofcom, has given some thought to how best to ensure consumers have access to useful information on traffic management practices. Ofcom has published six principles for the publication of consumer information on traffic management. It suggests that consumer information should be: [16]

- ***Appropriate:*** *ISPs should disclose all information, and only such information, that a consumer needs to make an informed decision.*
- ***Accessible:*** *basic information should be available at the point of purchase, and more detailed technical information should be readily available online or on request.*
- ***Understandable:*** *information should be simple enough for consumers to be able to understand the practical impact of traffic management policies on the way they may use the internet service.*
- ***Verifiable:*** *consumers or third parties (e.g. intermediaries such as price comparison websites) should be able to verify any information provided.*
- ***Comparable:*** *consumers should be able to compare information provided by different providers.*
- ***Current:*** *the information available to consumers should be up-to-date, both at the point of sale and subsequently.*

Principles such as these may be adequately effective as non-binding guidelines, backed up with general consumer protection laws that govern misleading conduct. The relatively light-handed nature of transparency

obligations also means that operators may be more willing to comply on a voluntary basis. Such voluntary co-operation could be seen as driven – at least partially – by a desire to pre-empt more intrusive compulsory restrictions. In the United Kingdom, a number of ISPs developed and launched a Code of Practice on traffic management, cited with approval by Ofcom (referred to in section 2.6 below).

Where voluntary and indicative responses are either not available or are ineffective, compulsory transparency obligations may be considered. These can be assessed, as with most regulatory interventions, against the regulator's ordinary set of regulatory principles. In many cases, transparency obligations are likely to be a proportionate response to concerns regarding traffic management: it is light-handed approach which leaves room for market-based mechanisms, is consistent with competitive market outcomes, and is unlikely to be overly onerous on suppliers.

2.3.2 Switching costs

For competition to affect the traffic management practices used by ISPs, consumers need to able to act on their experiences and information by switching provider. If there are two ISPs, identical except for their traffic management techniques, in a workably competitive market consumers should be able to switch to the more desirable ISP without undue costs or other barriers. The major obstacle to them doing so, other than inertia, is the widespread use of longer term contracts; up to 2 years.

Addressing switching costs is unlikely to be as straightforward as information transparency. Switching costs (and long-term contracts in particular) are not uniformly harmful. There are a number of reasonable justifications for their use. In many cases, they allow the cost recovery of financial and equipment incentives offered to the customers, such as handset subsidies (for mobile), modem or router subsidies (for fixed), or discounted rates. All of these incentives can promote competition.

Forcing a reduction in switching costs would risk diminishing the use of these incentives, and create a reduction in competition that would need to be assessed against the forecast improvements to competition (and to net neutrality) resulting from lower switching costs.

An alternative would be to ensure that switching costs are made clear to consumers; the principles for doing so are similar to the way traffic management information is disclosed, as discussed above. If warranted, a more interventionist response would be to require that fees for early termination of a fixed term contract be cost-reflective.

2.4 Quality of service assurances

There is a residual concern that if prioritization by ISPs becomes widespread, then the un-prioritized traffic will be so degraded that the CAPs that do not participate in prioritization will suffer competitively. This is the "dirt track" argument referred to in section 1.2.4 above. This gives rise to the question of whether to introduce measures that ensure a certain base level of quality of service. Or there may be a more general need for these measures where degradation, hindering or slowing down warrants the introduction of a minimum quality of service requirement.

In the European environment, Article 22(3) of the Universal Service Directive introduces a power for regulators to set minimum Quality of Service (QoS) requirements "[i]n order to prevent the degradation of service and the hindering or slowing down of traffic over networks".

BEREC has recently issued draft guidelines[17] for European regulators in determining what is a reasonable or unreasonable practice by an ISP, and whether an NRA should intervene by imposing minimum QoS requirements.

2.5 No blocking or other discriminatory practices

The active reformers have tended to go beyond tentative refinement of the regulatory regime to introduce specific net neutrality restrictions. The restrictions in particular control:

- blocking of lawful content, applications, services or (on occasion) non-harmful devices (e.g., USA FCC rules); and
- other discriminatory practices, which may be unreasonable or, while not outright blocking, render lawful content, applications or services effectively inaccessible or unusable (e.g., USA FCC rules, Chile, Singapore).

Usually these restrictions on blocking and other discriminatory practices are subject to reasonable network management measures.

The restriction on blocking of lawful content, applications and services may be seen as relatively uncontroversial, particularly when reasonable network management measures may apply. Although not a common practice around the world, blocking in these cases would be seen as concerning, particularly if conducted by an ISP with market power in the retail broadband market.

The more difficult issues arise under the restriction on "other discriminatory practices" and, in particular, whether this permits prioritization or access-tiering. Governments and regulators in active reformer countries have addressed this issue in various ways, mainly by seeking to carve out practices that would otherwise be caught by the general restriction on other discriminatory practices, but which are likely to be legitimate. For example:

- In Chile, regulations have been introduced to allow ISPs to introduce tiered pricing and speeds for Internet access;
- In Singapore, ISPs and telecommunications network operators are allowed to offer niche or differentiated Internet service offerings, provided that they meet transparency, QoS and competition requirements; and
- In the Netherlands, operators may offer a range of mobile data tariffs with different download speeds and levels of service, but they cannot tie specific rates to the use of specific free Internet services.

In relation to the suite of traffic management techniques, actions such as degradation, throttling, prioritization and access-tiering may walk a thin line between "unreasonable discrimination" and "reasonable network management". As discussed earlier, it can be difficult to distinguish between the two.

2.6 Approaches in five leading jurisdictions

This section briefly reviews the approaches and perspectives on traffic management from five leading jurisdictions. The jurisdictional review reveals that there is no one, universal, approach to regulating net neutrality. A more complete international summary of regulatory approaches to net neutrality can be found in the Appendix. Both developed and developing countries have been included in this review.

The United States

The United States is, in many respects, the home of the net neutrality debate. The arguments are louder, the lobbying more intense and the attempted legislative interventions more frequent. Yet although the Internet is a global phenomenon, the particular characteristics of the US market set it somewhat apart from other countries.

In the United States, the standard justification for imposing net neutrality remedies is *Comcast v the Federal Communications Commission* [18] and alleged blocking of certain services using the BitTorrent protocol. The FCC intervened in this instance to rule that Comcast was not entitled to throttle to the extent that it had been. Highlighting the uncertainty as to what constitutes "reasonable" traffic management, the FCC held that:

Although Comcast asserts that its conduct is necessary to ease network congestion, we conclude that the company's discriminatory and arbitrary practice unduly squelches the dynamic benefits of an open and accessible Internet and does not constitute reasonable network management.

However, the order was later vacated with the United States Court of Appeals upholding Comcast's appeal. The Court held that the FCC had acted outside its purported statutory authority under the Communications Act 1934. While the FCC acknowledged that nothing in the Act expressly empowered it to regulate an ISP's network management practices, it had sought to rely on various ancillary powers. The Court rejected all of the FCC's claimed authorities.

Since this case was decided, the FCC has persisted in its efforts to establish a more direct source of control in the form of net neutrality rules. In December 2010, it issued an open access notice which is based on three fundamental principles:

- **Transparency**. Fixed and mobile broadband providers must disclose the network-management practices, performance characteristics and terms and conditions of their broadband services;
- **No blocking**. Fixed broadband providers may not block lawful content, applications, services, or non-harmful devices. Mobile-broadband providers may not block lawful websites or block applications that compete with their voice or video telephony services; and
- **No unreasonable discrimination**. Fixed broadband providers may not unreasonably discriminate in transmitting lawful network traffic.

Both the "no blocking" and "no unreasonable discrimination" principles are expressly subject to a provider's ability to undertake "reasonable network management" as defined:

> *A network management practice is reasonable if it is appropriate and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service.*

These regulations remain highly controversial and are being challenged in federal court. As of writing, a decision has not been released.

European Commission

In Europe, the debate really started in 2009 when the European Commission (EC) issued its initial support for the net neutrality principle in a communication and then secured some basis for these principles in the amended directives issued as part of the new framework (see below). However, the number of actual interventions has been small, relying instead on general principles of competition law and the perceived level of competition available via existing regulatory protections or competitive network provision or both.

The EC, via the amended Universal Services Directive[19], introduced some measures aimed at promoting net neutrality when it mandated that national regulatory authorities should:

- be able to set minimum quality levels for network-transmission services (Article 22(3), *Universal Service Directive*);

- allow consumers to be able to switch between ISPs quickly and without unnecessary penalties (Article 30, *Universal Service Directive*); and

- ensure transparency in relation to ISPs' utilization of any traffic-shaping measures in their contracts with consumers (Article 21(3)(d), *Universal Service Directive*).

In 2010, BEREC conducted a review which did find evidence of particular discriminatory behaviors. More specifically, BEREC found that blocking of VoIP in mobile networks occurred in Austria, Croatia, Germany, Italy, the Netherlands, Portugal, Romania and Switzerland. Incidents of throttling or blocking of Internet traffic (e.g., of certain websites, the entire broadband connection, P2P file sharing or video streaming) occurred in France, Greece, Hungary, Lithuania, Poland and the United Kingdom. With respect to blocking of VoIP in mobile networks, some operators in some countries allowed usage of such VoIP services[20] for an extra charge.

BEREC has recently set out a work program covering different aspects relevant to net neutrality. They are based on different legal foundations, cover various market developments, and differ in their focus on legal, technical or economic analysis. BEREC has been consulting on[21]:

- Guidelines on transparency in the scope of net neutrality;

- Framework and Guidelines for quality of service in the scope of net neutrality, which assesses "degradation of service" and the conditions and ways to use the new Article 22(3) of the Universal Service Directive, i.e. how to intervene when deemed necessary;

- Differentiation practices and related competition issues in the context of net neutrality, which is an economic analysis about which practices may cause harm to end-users, and under which conditions; and

- NGN IP interconnection and net neutrality, which is an overview of IP interconnection markets and economic relationships between operators assessing the regulation with regard to IP interconnection in the context of net neutrality.

United Kingdom

In the UK, the main legislative intervention occurred in the amendment to the Communications Act 2003 and the Wireless Telegraphy Act 2006, which empowered Ofcom to undertake particular actions should it deem it necessary by way of its licensing powers.

These include the ability of Ofcom to impose minimum requirements in relation to the quality of public electronic communications networks to "prevent the degradation of service and the hindering or slowing down of traffic over networks" (the so called quality of service Condition).[22] No such condition has been issued to date.

Ofcom did, however, take steps to enhance transparency and, in May 2011, amended the General Conditions of Entitlement[23] to ensure that there is adequate transparency around the traffic management methods employed by ISPs and mobile operators.

In particular ISPs and mobile operators must provide:

(d) details of the minimum service quality levels offered, namely the time for initial connection and any other quality of service parameters as directed by Ofcom;

(e) information on any procedures put in place by the undertaking to measure and shape traffic so as to avoid filling or overfilling a network link, and information on how those procedures could impact on service quality.

And, finally, given the concern that users could not exercise their ability to change providers as a result of any degradation or blocking, there is a new General Condition 9.3 that requires that communications providers do not include conditions or procedures for contract termination that act as a disincentive for end-users to change providers. However, there are still options under EC law and UK law for period contracts, in particular for ISP services, IPTV and mobile phone contracts to amortize the cost of service provision and particularly the hardware.

Ofcom have undertaken consultations and reviews of the marketplace and found, in late 2011, that the use of market power and discrimination in traffic management to the benefit of an operator's retail arm is the main harm. They found that existing regulation and market structures resulting from those interventions provided substantial protections against discriminatory practices. Ofcom chose not to impose far reaching restrictions on traffic management practices. It also found that there was no need to impose a minimum quality of service at that time and would use existing tools including the competition rules.[24]

In response, many of the UK ISPs signed up to a voluntary code of practice which would require enhanced information for customers on their traffic management practices.[25] The voluntary code has three main components:

- an explicit commitment to provide more information to consumers about what practices are used in networks;
- an agreed set of good practice principles that will inform how ISPs communicate that information to consumers; and
- a commitment by each signatory to publishing a consistent Key Facts Indicator table, summarizing the traffic management practices it uses for each broadband product currently marketed.

The most recent flurry of interest over net neutrality in the UK came as a result of the formal launch by BT Wholesale of its wholesale content connect service (a CDN network service). This effectively gave ISPs access to a mechanism for prioritizing traffic via a new CDN service which caches content nearer to the user and so improves resilience and quality. Opinions differ starkly as to whether this flies in the face of net neutrality principles or is an economic reality which will substantially enhance the quality of the Internet.

Chile

After a four year process, Chile's General Telecommunications Law was amended in July 2010, with the implementation regulation published in September 2011. The new law forces ISPs to "ensure access to all types of content, services or applications available on the network and offer a service that does not distinguish content, applications or services, based on the source of it or their property". The law also allows ISPs to offer tiered pricing and service speeds to end users, with the intent being to facilitate a move away from flat fee pricing.

The Chilean law was brought about after a concerted lobbying effort by the pro-neutrality group Neutralidad SI ("Neutrality Yes!"). Although there does not appear to be a single catalyst for the decision to impose net neutrality, Neutralidad Si claimed that broadband operators were persistently restricting peer-to-peer traffic on their networks.

Felipe Morandé, Minister of Transportation and Telecommunications, welcomed the amendments, saying:

> *It is a concrete step toward having greater transparency in the broadband market, stimulating competition for quality of service, which is the pillar of our public policy in telecommunications. [The law] places our country at the forefront in the world in terms of net neutrality. It shows that there is the political will in Chile to modernize the regulation of telecommunications and empower consumers.*[26]

The Netherlands

In the Netherlands, legislation was recently passed on 8 May 2012 that prohibits telephone operators from blocking or charging consumers extra for using Internet-based communications services like Skype or WhatsApp, a popular free SMS service. Internet providers will also be prohibited from making prices for their Internet services dependent on the services that are used by a customer. Operators may still offer a range of mobile data tariffs with different download speeds and levels of service, but they cannot tie specific rates to the use of specific free Internet services.

The law derives from attempts by KPN (the incumbent operator) to charge users for access to Skype and WhatsApp. This was challenged on both privacy and net neutrality grounds. Particular criticism was aimed at the public disclosure by KPN executives that it was aware of the huge take up of free SMS app services based on extensive use of DPI techniques. OPTA, the telecoms regulator, may impose fines of up to 10% of sales for breaches of the new rules.

The rules do not, however, prevent the setting of tariffs based on data usage or specific quality of service provisions (indeed reports in July 2012 note that KPN has introduced new data mobile tariffs at higher rates than previously). The rules apply to all ISPs.

2.7 Other issues to consider during policy formulation

2.7.1 Human rights and the right to access information

In some debates, there can be a human rights element to net neutrality. This is particularly evident in respect of government attempts to block certain web sites or telecommunications services. This blocking may be routine or on an ad hoc basis. Ad hoc blocking of Twitter and SMS was reported in multiple countries during the Arab Spring uprisings for example. This type of blocking, by operators, mandated by government, can be distinguished from blocking undertaken at a commercial level and is not discussed further in this chapter.

2.7.2 Consumer privacy and freedom of communication concerns

An often overlooked issue in the net neutrality debate is the potential privacy concerns that may arise when an Internet users' personal information is managed as it passes over a network. In particular, the use of DPI seems to generate *prima facie* privacy concerns, as data about a users' behavior on the Internet (which will often include sensitive data) is monitored and used for various purposes, such as traffic management or advertising.[27] Privacy and freedom of communication are issues that will only become more pertinent over time as DPI technologies improve, which means they will need to be considered during the policy development process[28].

3 Industry response

In many ways, the net neutrality debate has been led by the major players in the telecommunications industry themselves. Fixed-line and mobile operators facing increasing capital investment costs sought to achieve more equitable business and revenue sharing models. In turn, CAPs have also responded by taking measures to protect their own interests, such as reducing reliance on public networks by using Content Delivery Networks (CDNs) or by having their own networks. The following section will seek to breakdown the interests of the key market participants, as well as outlining some of the potential industry-based solutions that have been discussed to date.

3.1 A tailored application of net neutrality principles

In order to develop appropriate policies to deal with net neutrality issues, it is important to understand the varying positions of the key players in the debate. Some countries, such as the United States, have distinguished between these key groups (i.e., between fixed and wireless networks) in their responses to net neutrality concerns.

3.1.1 Fixed and wireless networks

To date, fixed-line operators have done a relatively good job of increasing average revenues per line from their traditional, mainly copper-based networks, which has helped to offset the increasing costs of investment in new high speed networks and declines in revenue caused by applications such as VoIP. However, the industry is coming to a crossroads and the obstacles associated with the strict implementation of net neutrality principles are beginning to take shape. The primary issue facing fixed-line operators will be finding an appropriate and equitable means of funding the increased investment in new high speed broadband networks to meet the ever-growing demand for digital content.

However, network neutrality seems to be having a more immediate effect on the mobile industry. Increasing demand for capacity caused by new data-intensive applications combined with a shortage in spectrum has put mobile providers under pressure to make the investments that are necessary for growth. The outlook for the mobile industry suggests that wireless networks will continually need to be upgraded in order to keep up with capacity. In addition, applications like Skype or WhatsApp that offer rival services also present a considerable challenge to mobile players, because VoIP and IP-based messaging applications are now cannibalizing their traditional revenue streams.[29]

3.1.2 Content Delivery Networks and private infrastructure

A CDN is essentially a system of servers that are deployed at the edge or within a terminating ISP's network to facilitate an improved distribution of content and application services. CDNs do not interfere with the ISP's network layer and they do not provide connectivity, but instead they operate on top of the network layer. By storing content closer to end users, CDNs help to reduce latency and enhance service quality, which results in faster download speeds and response times for users. Furthermore, by storing content closer to customers, this content only needs to be delivered once from the CAP to the CDN's caching server, which reduces peering volumes and transit costs.[30]

Most major CAPs have started building their own Internet traffic infrastructure or using the dedicated CDNs of companies to ensure that their data-intensive services and applications are not constrained by delays or congestion in the public network. Although the investment in CDNs and private infrastructure are added costs on CAPs' traditional business models, by-passing the backbone of the public Internet allows CAPs to ensure that the immense volume of traffic that they generate reaches their customers at optimal speeds. This ultimately improves QoS and ensures greater customer uptake, which has made it a worthwhile investment for many larger content providers, particularly for those that have the scale to justify the initial costs of investment.

In many ways, the use of CDNs allows larger CAPs to manage their exposure to restrictive traffic management practices, which supports the principle of net neutrality. However, some have argued that this situation merely serves to put a different kind of strain on the principles of net neutrality. This is because the smaller CAPs, who cannot afford to invest in their own infrastructure or CDNs, will typically be unable to match the performance of the larger CAPs. Over time, this could serve as a barrier to entry and a limiting factor on innovation. Whether this disparity represents discrimination or simply a competitive disadvantage is open to debate.[31] It does mean that regulators cannot simply rely on CAPs to invest in CDNs to avoid restrictive traffic management practices because this may not be an option for smaller CAPs.

Figure 4 provides an example of Amazon's global data center and "edge" locations, which have been set up to improve the performance and delivery of Amazon's online services.

Figure 4: Amazon's global CDN and private infrastructure network

Source: Amazon Web Services online (http://aws.amazon.com/about-aws/globalinfrastructure/)

3.1.3 Accounting for the rest: smaller providers and consumers

Smaller CAPs without a CDN rely on the "public Internet" to reach their consumers. These providers face growing threats on two fronts.

On the one hand, their reliance on the public Internet means that traffic management will more significantly affect smaller CAPs whose content may be manipulated or indirectly controlled by an ISP. Content travelling over the public network is exposed to an ISP's traffic management practices. Similarly, as discussed in the previous section, the smaller providers will also continue to be at a competitive disadvantage in comparison to the larger CAPs that are able to offer services at a higher quality by transferring their data outside of the backbone of the public Internet. The risk is a growing barrier to entry for smaller and start-up CAPs.

Net neutrality advocates have argued that regulator involvement will be particularly necessary to ensure the continued existence of the smaller CAPs. To date, consumers have benefitted greatly from the innovation and product diversity that these smaller start-up and niche players provide, so it will be crucial to ensure the right conditions are in place to allow for their continued existence. Expecting CAPs to invest in costly CDNs may not be enough, which means some level of regulator intervention may be required to ensure that smaller CAPs are not disrupted by discriminatory behavior that limits their ability to efficiently distribute their services over the public Internet. For example, minimum QoS obligations could be mandated, which would help to ensure a basic level of competition across public networks.

3.2 Finding industry-based solutions

3.2.1 Self-regulation and co-regulatory models

Some industry players have called for government policy-makers to leave markets to regulate themselves. They argue that a body of technical experts from industry is in the best position to find solutions to the shared issues being faced by both network operators and content providers. Proponents of self-regulation argue that regulator

involvement risks over-regulation (and the added costs associated with regulatory compliance) and can bog down the problem-solving process with political agendas. The Broadband Internet Technical Advisory Group (BITAG) is an example of a body of technical experts that have been brought together to seek industry-based solutions to the net neutrality issue in the United States[32]. A body performing a similar role at the international level is the World Wide Web Consortium (W3C), which is a non-governmental body with extensive private membership and a full time staff that contributes to the regulation of the internet.[33]

Of course, there are a number of problems with relying on self-regulation. For one, self-regulation relies on voluntary compliance instead of punitive or exemplary sanctions to enforce conformity. There is also the question of who develops the industry code of conduct or regulation; the fear is that the larger market players are allowed to dominate the process to the detriment of smaller participants, particularly small CAPs.

A compromise may be to institute co-regulation. A co-regulatory scheme combines elements of self-regulation as well as of traditional regulation to form a new and self-contained regulatory scheme. However, the difficulties with finding the right balance between self- and public- regulation can make this approach challenging, and the likelihood of larger players dominating the process would continue to be a fear as smaller ISPs and CAPs may not have the resources necessary to effectively contribute.

3.2.2 Partnering: opportunities for collaboration between operators and CAPs

ISPs have tended to view over-the-top (OTT) applications and services such as VoIP as a threat to the traditional telecom value chain. It has been estimated that, in North America alone, traditional telco operators, both mobile and fixed, lost approximately US$30 billion of revenue between 2005 and 2010 to OTT applications that substitute for existing revenue streams.[34] However, in recent years, there has been a gradual realization across the industry that working in isolation only serves to harm all players; the market is converging and network operators and CAPs are being forced to adapt to prevent further losses of revenue and market share. The focus is now shifting towards the potential opportunities for collaboration that exist between ISPs and CAPs.

Mobile and fixed-line operators can use partnerships with CAPs to establish themselves as innovators and gain market share through cost-efficient customer acquisition. These partnerships would also provide opportunities for ISPs to increase revenues by reclaiming their footprint in the value chain. Greater collaboration with ISPs could also increase a CAP's end-user exposure by allowing it to gain access to an operator's user base and high quality network services. Partnerships would also present a chance to monetize the existing user base.[35]

4 Net neutrality and the International Telecommunications Regulations

4.1 Internet governance and the ITRs

The International Telecommunication Union (ITU) currently plays an important role in promoting the international interoperability of traditional telecommunications systems. The International Telecommunications Regulations (ITRs) are an international treaty governing the provision and operation of public telecommunications services, as well as the underlying transport mechanisms used to provide them. The regulations provide telecommunications administrations and operators with a broad framework to guide them in the provision of international telecommunications services. They establish general principles relating to the provision and operation of international telecommunication. They are designed to facilitate global interconnection and interoperability of telecommunication infrastructure, underpin the harmonious development and efficient operation of technical facilities, and promote the efficiency and availability of international telecommunication services. However, as an influential international body, the ITU's stance on net neutrality will set important benchmarks to guide national regulators.

The current version of the ITRs was adopted in 1988 in Melbourne, Australia, by the World Administrative Telegraph and Telephone Conference (WATTC), so the current regulatory structure is based largely on voice

telecommunications. The Internet was still in its infancy the last time the ITRs were updated; however, the Internet now forms an important component of the ITU's broader telecommunications mandate. For this reason, a number of proposals have been put forward to update the ITRs to take into account the modern prevalence of data communications. In this context, the ITRs will be revised by the World Conference on International Telecommunications (WCIT12) to be held in December 2012 in Dubai (UAE). The main objectives of the WCIT12 are to adapt the ITRs and facilitate the achievement of the following goals: ensuring the free flow of information, the development of broadband networks and services, continuing investment in networks, services and applications as well as continuing innovation.

4.2 Update of the ITRs

A number of suggestions have been put forward to update the ITRs. Some of the proposals presented to the Council Working Group to prepare the 2012 World Conference on International Telecommunications concern network neutrality. [36]

For one, ITU Member States will need to determine to what extent the ITRs would affect national policies regarding regulation of traffic management and QoS prioritization. For example, some proposals would provide that Member States agree to allow differentiated traffic management, which is basically saying that Member States would agree not to impose strict network neutrality regulations. As discussed earlier, traffic management is a common practice among telecom operators. While QoS prioritization would lead to improved performance and could result in an indirect form of revenue sharing between CAPs and network operators, these benefits will need to be weighed against the added costs and complexity of complying with new QoS obligations. [37]

Ultimately, the key will be taking a broader view on the key net neutrality issues facing national regulators and extending them to the international level. In an effort to situate the principles of net neutrality within the broader ITRs framework, the impending update of the ITRs will need to strike an appropriate balance between public access to international telecommunications services, while still maintaining the ability to prioritize critical services and to ensure adequate service quality.

5 *The future: what's coming next?*

5.1 Is net neutrality going to remain an issue moving forward?

Net neutrality is an issue that is only likely to grow in importance as new data-intensive applications and services put an increasing strain on telecommunications networks. It is important to remain forward looking to try to understand how these issues will likely play out in the future.

This means that the debate surrounding the extent to which net neutrality should be regulated will only intensify. This section assesses the arguments for and against the regulation of net neutrality in an effort to tease out what future business models will look like for telecommunications network providers.

5.2 Arguments against net neutrality protections

Those who say there is no problem, or that wide-ranging net neutrality protections are not required, point to the following factors:

5.2.1 The countervailing power of CAPs

The countervailing market power of the CAPs, particularly the major players who are the strongest advocates for net neutrality concepts. If a particular ISP was to threaten to charge a Google or Amazon, they could threaten to withdraw the service from that ISP. The loss of this service would have a substantial impact on the ISP and it would

face a material risk of client loss to other ISPs that did have access to these services. While the CAP would lose access to the ISP's subscriber base, the largest CAPs are now so big and have such a diverse set of users internationally that such a move would have little impact on their total revenue. This argument is strongest when there is a vibrantly competitive retail broadband market.

5.2.2 The importance of traffic management

The general acceptance that traffic management is essential to protect the consumer experience, especially in times of potential extreme network congestion.

5.2.3 Free market solutions already in place

The market now deals with the issue by virtue of a range of new mechanisms, including:

- tiered pricing structures, so that data hungry users are charged additional sums for the data used and utilization and price are more closely aligned; and
- the use of CDNs by CAPs to reduce their access costs and improve the quality of service for their customers.

5.2.4 Charging CAPs would not be sufficient

If charging CAPs was to be widespread, it would be unlikely to provide sufficient sums to drive network upgrades given the scale of the revenues of these providers versus the cost of the network upgrades required. The giant values of many of these CAPs in stock market terms generally does not equate to a material revenue stream or huge profitability, with the exception of one or two of the largest players, whose revenues tend to derive not from content delivery but rather advertising revenues. A good example of this was the recent public offering of Facebook, which valued the company at approximately US$104 billion despite the fact that the company's annual revenue stream was only $US 1 billion per year and its subscriber base had basically peaked at approximately 900 million users.[38]

5.2.5 Net neutrality rules may actually reduce ability to offer tiered services to third parties

An over-application of net neutrality rules will actually reduce the ability of providers to offer properly tiered services to third parties. For example, net neutrality rules should not prevent ISPs from providing higher QoS to business customers (or home workers). However, where the incumbent has market power, then they will need to be applied in such a way that prevents incumbents from acting anti-competitively and discriminating in favor of their own content and applications business in the provision of such services. Therefore, the issue is actually about the effectiveness of any over-arching telecommunications regulatory regime and its ability to effectively target discriminatory conduct, drive competition in retail markets where there is wholesale market power and do so in a timely and effective manner.

5.2.6 Focus should be on other more pressing issues

There are other much greater issues at play, such as incentivizing network investment generally in the face of questionable retail appetite for higher prices for higher speeds or data usage and the perception of "free" services being available. Another issue is the need for effective access regulation more generally, which could be used to improve competitive access to retail and wholesale services and would reduce the need for specific net neutrality type protections. The net neutrality argument in the US has achieved greater resonance due to the view that the access regulatory mechanisms been seen by some as failing to deliver adequate retail or wholesale competition for services, meaning that additional protections for consumers are required.

5.2.7 Competition in the retail space

Retail competition is being bolstered by a range of measures:

- ongoing access regulation to secure the greatest level of retail competition, including functional separation and effective enforcement of existing access remedies and competition rules for non-discrimination and equivalence of inputs/outputs rules;[39]
- increased transparency by operators as to their practices on blocking and network management;
- easier switching mechanisms between ISPs; and
- ongoing monitoring of practices in this space by regulators.

5.3 Arguments in favor of net neutrality protections

Those that predict a problem if specific additional protections to secure net neutrality are not implemented argue:

5.3.1 The insufficiency of competition rules

The inability of competition rules to deal with complex issues of network security, data prioritization and other complex network dialogues in a timely manner. The issue of proof and difficulty in securing injunctions to prevent particular behaviors, as well as the length and cost of court processes in many countries, require specific regulatory protections over and above general competition law.[40]

5.3.2 Lack of competition at the retail level

The lack of competition at the retail level in certain jurisdictions can give power to incumbents, as they would be less likely to lose customers in the face of degradation of traffic/access to certain sites. This is often argued to be the result of flawed access regulation in the particular country and may well require additional intervention at the wholesale level more generally, or functional or structural solutions, to deal with access bottlenecks. Similarly, it may be that it is a problem in specific parts of a member state's market as NGA networks are rolled out on a regional/piecemeal basis and regulatory remedies progressively apply in a sub-national context.

5.3.3 Lack of regulatory protections against network degradation

The lack of regulatory protections against network degradation in mobile networks, with the vast majority of access remedies focused on fixed incumbent providers. The proposed US regulations, for example, place much stricter obligations on fixed operators than wireless operators and the EC access rules are not presently applied to mobile carriers. This is coupled with the move to longer term mobile contracts (often up to 2 years), which could potentially reduce the ability of customers to switch network in the event of blocking or degradation of certain services by mobile players, including of VoIP services.

5.3.4 Inability of smaller CAPs to compete

The ability of smaller and start-up CAPs to compete with the more established CAPs may be affected if they are unable to secure access to specific ISPs or afford access-tiering charges. This would be particularly concerning where an ISP with SMP was to reach an exclusive arrangement with an established CAP or where smaller CAPs were unable to secure affordable access to increasingly-prevalent CDNs. The increasing use of CDNs could increase the risk of the smaller CAPs struggling to secure enhanced access to their services in the face of prioritization of the

more established players. These potential barriers to entry may deter new start-ups from joining the market, which threatens to hinder innovation and diversity in the long run.

5.3.5 Unfair advantage for IPTV services

As IPTV develops and is promoted by incumbent telecommunications providers as a means of driving demand for higher speed networks (and therefore premium service charges), there may be more pressure on these players to prioritize their own IPTV services over those from third parties. The growing movement towards bundled packages that could include a range of related services (e.g. IPTV, telephony, internet, etc.) at cheaper prices gives telecommunications providers an incentive to extend, and discriminate in favor of, their own offerings down the supply chain.

5.4 Future regulatory and business models

5.4.1 Exploring new regulatory models

There is ongoing debate on the appropriate regulatory model for NGA access. Given the underpinning driver for the intensity of the net neutrality debate was the need for investment and upgrades to the network in both access and backhaul, it is hard to see the two regulatory issues not coming into conflict soon. This is particularly true if the widest interpretation of net neutrality is applied and there is pressure to prevent network owners charging extra sums for higher bandwidth or better quality of services. This flexibility will be key to securing economic roll out of NGA services and justifying the investments needed in the network. The rules will need to allow pricing models to recognize enhanced speed and services. The disparaging notion of a "two speed Internet" will need to be replaced by a more nuanced realization of the consumer desire for differential speeds and qualities based on their needs.

Unquestionably, transparency on the services being delivered and how this is realized is relevant and will assist customers to determine the services they wish to secure. Indeed this is the focus of much of the debate at present in Europe and the UK, alongside securing switching and general competitive provision of retail services. For example, the European Commission's NGA Recommendation on access to NGA[41] cites the need for effective access remedies to NGA where there is market power.

Net neutrality alone is not a sufficient reason to justify increasing capacity through investment in next-generation fixed and wireless networks. But to the extent that this investment occurs for broader objectives, then the regulatory model for these developments should at least consider net neutrality concerns and – if necessary – define and restrict the use of unreasonable traffic management measures. Where governments incentivize investment through regulatory concession, governments should be reluctant to make concessions that may unduly threaten net neutrality.

NGA investment and the accompanying regulation are being dealt with in various ways. In certain jurisdictions, the solution has been to create a completely separate entity which will provide basic connectivity services to all comers and with no activity in the retail space itself. This is the case in Singapore, Australia and New Zealand. In the UK, a model of functional separation aims to do something similar by attempting to bolster non-discrimination rules by the creation of a network arm for BT which provides many of the services underpinning NGA on a non-discriminatory basis, but without full structural separation.

The approach that is ultimately taken within a jurisdiction will stem from a broader philosophical decision that will need to be made on the level of state participation in the market. If a more laissez-faire approach is taken, the government will seek to encourage operators to invest in their infrastructure by providing them with regulatory certainty that benefits from investing in new network infrastructure will be captured by those making the initial investments. For example, the United States has sought to encourage investments by relieving operators of the obligation to unbundle their networks.

On the other hand, a government may opt to play a more prominent role in the market in order to guide and promote innovation and investment. This is the approach that was recently taken in Australia and Singapore, where the state injected the capital necessary to update legacy networks when the incumbent operators were unable or unwilling to make the necessary investments themselves.

5.4.2 New revenue models in a converging environment

New business models are being suggested to deal with the investment required due to the growing data consumption and new more bandwidth-hungry content and applications provided by CAPs. These include prioritization for higher prices (including of an ISP's own services, like IPTV), charging CAPs for prioritization for delay-sensitive services and providing guaranteed network capacity for end users.

Under the current prevailing internet business model:

- ISPs charge end users for internet access. ISPs pay for transit from international operators, or they peer; and
- CAPs charge end users for their services, or provide it for free (normally supported by advertising). CAPs pay for hosting and connectivity from ISPs that provide this particular service.

Although not occurring on any widespread basis at the moment, ISPs could require that CAPs pay an ISP for prioritization – faster or higher quality service relating to the ISP's network. This isn't happening probably because ISPs and CAPs typically don't have any physical or contractual relationship – they interface with the myriad of internet intermediaries. However, the absence of this physical or contractual relationship may not prevent an ISP charging a CAP. The risk for the CAP is their services are degraded relative to other competing services and they are prepared to pay for that not to happen.

Internet access can be thought of as a type of platform or intermediary where two groups are involved – CAPs and end users, with ISPs providing the platform on which they interact. Two sided markets theory suggests that this type of charging by an ISP is not necessarily inefficient – depending on the relative elasticities of demand for CAPs and end users.

Large CAPs have significant power to demand reasonable commercial terms in this sort of negotiation. Smaller CAPs may be more vulnerable, but can be represented in negotiations by large hosting and connectivity providers that can have equivalent bargaining power. Also, it must be recognised that there is value to the ISP in CAPs providing a high quality service to end users, as that increases the value of the Internet access services ISPs provide.

6 Recommendations

6.1 Existing market structure and regulatory environment

Recommendation 1: ensure that there is effective competition in the retail broadband market generally and, if not, take steps to increase this effectiveness.

Recommendation 2: review existing telecommunications regulation and competition laws to determine whether the regulatory tools are already in place to adequately address the competition issues that tend to impact on the principle of net neutrality. In many cases anti-discrimination obligations will already be available, which can be used to prevent ISPs from favoring themselves against a rival CAP's content or application, and regulators should consider strengthening these obligations and their effectiveness.

6.2 Transparency

Recommendation 3: to promote competition in the retail broadband market, traffic management practices should be made public through clear and useful consumer information. This should be driven, initially, through voluntary guidelines and self-regulation backed up by consumer protection law. If this proves ineffective, binding information disclosure obligations may be necessary.

6.3 Switching

Recommendation 4: customers should be able to quickly and efficiently end their contract without high switching costs if they wish to change Internet providers. This ensures that customers are able to take action if they disagree with the terms of service in their contract with an ISP. The costs (and other barriers) to consumers switching ISPs should be considered, with a view to ensuring that switching costs are clear and fair. Early termination charges may be justifiable to recover any up-front costs or subsidies provided by the ISP, but these should also be transparent (and potentially be required to reflect cost-recovery).

6.4 Use of DPI

Recommendation 4: the growing use of DPI can create potential privacy concerns as operators are now able to view a users' personal information at a greater level of detail as it passes over a network. A minimum level of transparency should be required from ISPs so that a customer is aware of how their personal information is captured and used by the ISP.

6.5 QoS

Recommendation 6: regulators should possess the power, to be held in reserve, to impose minimum QoS requirements on Internet access services where over-prioritization degrades the "best efforts" Internet.

6.6 Net neutrality-specific regulation

Recommendation 7: if concerning traffic management practices remain despite the recommendations above, regulators should consider specific targeted regulatory remedies, including restrictions on blocking and unreasonable discriminatory behavior in traffic management.

7 Regulatory checklist: asking the right questions

7.1 Effective retail broadband competition

Is there effective competition in the retail broadband market generally or is the market controlled by a small number of powerful ISPs who are largely able to degrade traffic without the fear of losing customers?

If there is not effective competition in the retail broadband market generally, are there other steps that can be taken, consistent with international best practice, to improve the level of competition?

7.2 Traffic management

Are network management practices, such as blocking or throttling, prevalent and, if so, are they generally for legitimate (e.g. to alleviate congestion) or illegitimate (e.g. to discriminate against rivals) purposes?

Are smaller CAPs sufficiently able to compete? If not, is some level of state intervention required (e.g. regulate minimum QoS requirements to ensure reliable service)?

7.2 Existing regulation and competition law

Is the existing regulatory framework for telecommunications, including competition law, able to adequately address the more concerning forms of traffic management?

Would a self- or co- regulatory model be sufficient to address any net neutrality issues that currently exist?

7.3 Transparency

Are ISPs open and transparent with their customers about how they conduct their traffic management practices?

How easy is it for customers to switch service providers if they disagree with their ISP's traffic management practices?

Appendix: International summary[xlii]

Country	Summary	Legislation	Regulatory measures in place	Competition regime
Australia	Australia does not regulate the ability of service providers to discriminate between different types of network traffic. There are presently no net neutrality requirements, and it is common practice in Australia for service providers to offer "walled content" or impose download caps or throttling mechanisms.	None specifically applicable to net neutrality. The Competition and Consumer Act 2010 (CCA) provides for access regulation, as well as generic competition law.	None specifically applicable to net neutrality. Regulated services must be offered on set price and/or non-price terms. These include non-discrimination and equivalence requirements. NBN Co, the state-owned company that is building the nationwide FTTP, must give a "special access undertaking" that includes non-discrimination and equivalence.	The CCA is overseen by the Australian Competition and Consumer Commission (ACCC). The CCA contains both generic and sector-specific competition and access regimes that apply to the telecoms sector.
Brazil	The final text of a bill was recently presented to the Brazilian Congress. The bill places Internet access among relevant civil rights. The bill contains net neutrality protections, including a prohi-	The bill - officially named Marco Civil - begins with general principles for the regulation of the Internet, including "IV: to preserve and guarantee network neutrality".		

Country	Summary	Legislation	Regulatory measures in place	Competition regime
	bition of discrimination or degradation by ISPs.	ISPs must treat all data equally, and cannot discriminate or degrade services, except for limited technical reasons. Users have the right to non-suspension or degradation of the quality of contracted Internet connection. ISPs may not monitor, filter, analyze or monitor the content of data packets, except for technical management.		
Canada	The Canadian Radio-television and Telecommunication Commission (CRTC) requires CRTC approval if an ISP employs more restrictive Internet traffic management practices (ITMPs) for its wholesale services than for its retail services.	The Commission must grant prior approval pursuant to section 36 of the Telecommunications Act if an ITMP employed by an ISP would result in the carrier controlling the content or influencing the meaning or purpose of telecommunica-	The CRTC does not regulate retail Internet services or computer-to-computer VoIP services that reside solely on the Internet. However, the CRTC has put industry on notice that it may monitor ITMP upon consumer complaints.	The CRTC is responsible for sector-specific competition issues in the broadcasting and telecommunications industries. The Canadian Competition Bureau is responsible for overseeing the enforcement

Country	Summary	Legislation	Regulatory measures in place	Competition regime
	In order to enhance competitive neutrality, technical ITMPs (i.e., "shaping") of wholesale services must comply with the CRTC's ITMP framework and must not have a significant and disproportionate impact on secondary ISP traffic.	tions.		of competition laws more generally.
Chile	In July 2010, Chile became the first nation to put net neutrality principles into law. In a vote by the Chilean legislature, the law passed by a near unanimous vote. The new law forces ISPs to "ensure access to all types of content, services or applications available on the network and offer a service that does not distinguish content, applications or services, based on the source of it or their property".	The General Telecommunications Law was amended by Bulletin 4915. Under the amendments, no ISP can block, interfere with, discriminate, hinder, nor restrict the right of any Internet user to use, send, receive or offer any content, application, or legitimate service through the Internet, as well as any activity or legitimate use conducted through the Internet.	The regulation proposed by telecoms regulator Subtel in January was criticized by net neutrality supporters. The main sticking point was a clause of "previous disclosure," which appeared to allow ISPs to discriminate against certain content providing they stated their intentions in the terms and conditions of the contracts. The amended regulation published in the official gazette on March 18 2011 eliminated the controversial clause and	

Country	Summary	Legislation	Regulatory measures in place	Competition regime
			replaced it with clearer guidelines. The regulations allow ISPs to introduce tiered pricing and speeds for Internet access.	
Egypt	There are currently no limits on an ISP's freedom to control or prioritize the type or source of data that it delivers, unless otherwise specified in the provider's telecoms licence.	The telecoms and media sectors are governed by the Telecommunications Law No. 10 of 2003 (Telecoms Law).	There are no specific regulations or other policies in place to deal with net neutrality. However, specific net neutrality provisions may be included in the terms and conditions of an ISP's telecoms licence.	Telecoms services are regulated by the National Telecommunications Regulatory Authority (NTRA). Through the Telecoms Law, the NTRA is responsible for regulating competition within the telecoms and media sectors. Telcos will also be subject to general competition laws, which are regulated by the Egyptian Competition Authority.
European Commission[xliii]	In 2009, the European Commission issued its initial support for the net neutrality principle	There is no specifically applicable legislation.	The Commission, via the revised universal services	The Commission relies on general competition law principles (as well as existing

Country	Summary	Legislation	Regulatory measures in place	Competition regime
	in a communication and then incorporated these principles in the amended directives issued as part of the new framework. However, the number of actual interventions is low, relying instead on general principles of competition law and the perceived level of competition available via existing regulatory protections or competitive network provision or both.		directive, allows NRAs to: ▪ set minimum quality levels for network-transmission services; ▪ allow consumers to be able to switch between ISPs quickly and without unnecessary penalties; and ▪ ensure transparency in contracts in relation to traffic-shaping.	regulation) to protect against the main harm of market power being used to unfairly discriminate.
France	On 13 April 2011, the French Parliament released the 'Report of the Fact Finding Mission on Net and Network Neutrality' which put forward 9 proposals for addressing net neutrality. The proposals included enshrining net neutrality as a policy objective; amending Internet blocking obligations; regulating Internet universality	The legislative instruments that set out some minimal requirements related to net neutrality are the Postal and Electronic Communications Code (CPCE) and the Third Telecom Package.	Under the CPCE and the Third Telecom Package, various regulatory provisions exist that require service providers to block certain types of criminal conduct once the provider becomes aware of the conduct.	The Competition Authority is responsible for applying general competition laws. The ARCEP is the telecoms-specific regulator. The ARCEP brings matters before the Competition Authority when questions concerning anti-competitive practices arise.

Country	Summary	Legislation	Regulatory measures in place	Competition regime
	and quality; and ensuring viable financing of the Internet.			
Japan	The Ministry of Internal Affairs and Communications (MIAC) released a report regarding network neutrality in September 2007. The report identified two issues — fair allocation of network development costs and fair access to the network by telecommunications operators, including content providers. The report discussed whether telecommunications operators may engage in packet shaping (or traffic blocking) to ensure the network's service quality. ISPs may impose additional charges on heavy users and content distributors.	Under industry guidelines, packet shaping may violate the Telecommunications Business Law (TBL) but is permitted in exceptional situations, such as heavy user traffic or a specific application excessively occupying the network. The guideline also states that telecommunications operators should let users know of the possibility of packet shaping and how and when it would occur. The Law concerning Providers' Responsibility is applicable to providers of telecom services intended for the public.	The Net Neutrality Report was published in September 2007.	The competition law authority is the Fair Trade Commission, an independent administrative agency with the authority to prevent unfair trade or market dominance.

Country	Summary	Legislation	Regulatory measures in place	Competition regime
New Zealand	No specific provision for net neutrality, but ISPs are subject to general regulatory and competition obligations.	None specifically applicable to net neutrality. The Telecommunications Act 2001 sets out an access regime for certain telecommunications services. The Commerce Act 1986 is New Zealand's generic competition law legislation.	None specifically applicable to net neutrality. Regulated services must be offered on set price and/or non-price terms. These include non-discrimination and equivalence requirements. Fiber providers under the Government's FTTP initiative must give open access undertakings that include non-discrimination and equivalence. The Commerce Commission is currently undertaking a Demand Side Review, looking at possible impediments to the uptake of ultra-fast broadband. The terms of reference for this review include net neutrality.	Generally superseded by service-specific telecommunications regulation, but still available.
Republic of Korea	While legislation does not expressly address net neutrality and the KCC has not formally published its policy on the issue	There is no legislation specifically applicable to net neutrality.	The KCC has not published any policy in relation to net neutrality, although it has taken action	KCC is the Korean telecommunications regulatory authority.

Country	Summary	Legislation	Regulatory measures in place	Competition regime
	yet, there is a precedent in which a broadband carrier was sanctioned for blocking VOD service provided by another VOD service provider. The KCC found such blocking was a prohibited activity. The dispute was resolved by the VOD service provider's agreement to pay a network usage fee to the carrier.	The primary laws in this area are the Act on Framework of Telecommunication and the Telecommunication Business Act (TBA). The Radio Waves Act governs radio frequencies and the Broadcasting Act regulates the radio waves used in broadcasting.	under the TBA (see summary).	The KCC also makes specific regulations for the telecommunication and broadcasting industry. The Korea Fair Trade Commission (KTFC) is the competition authority. The Monopoly Regulation and Fair Trade Act (MRFTA) is the generic competition legislation.
Singapore	The Info-communications Development Authority (IDA) issued its decision on net neutrality in June 2011, following a consultation process. ISPs and network operators are prohibited from blocking legitimate Internet content. They cannot impose discriminatory practices, restrictions, charges or other measures	There is no legislation directly relevant to net neutrality.	ISPs and telecommunications network operators must comply with information transparency requirements and disclose to end-users their network management practices. Reasonable network management practices are allowed, subject to minimum QoS requirements and not render-	Under the IDA's decision, ISPs and network operators must comply with the competition and interconnection rules set out by the IDA in the Telecom Competition Code.

Country	Summary	Legislation	Regulatory measures in place	Competition regime
	which, while not outright locking, will render any legitimate Internet content effectively inaccessible or unusable.		ing legitimate content inaccessible or unusable. ISPs and telecommunications network operators are allowed to offer niche or differentiated Internet service offerings that meet transparency, QoS and competition requirements.	
South Africa	There are currently no limits on an ISP's freedom to control or prioritize the type or source of data that it delivers. Net neutrality is not regulated in South Africa at the moment.	The Electronic Communications and Transactions Act 2002 (ECTA) provides for the facilitation and regulation of electronic communications and transactions, including the broader development of a national Internet strategy. There are currently no general obligations on the service provider to monitor the data that it transmits or stores – ISPs are largely free to manage data flow as they deem	There are no specific regulations or other policies in place to deal with net neutrality.	The Competition Act 1998 is the generic competition legislation that deals with all economic activity in South Africa, including the telecoms sector. The Competition Commission oversees compliance with the Competition Act. Telecoms firms are also subject to sector-specific regulation from the Independent Communications Authority of South Africa (ICASA). There is overlapping

Country	Summary	Legislation	Regulatory measures in place	Competition regime
		appropriate.		jurisdiction between the regulators.
The Netherlands	Recent legislation was passed on 8 May 2012 that will prohibit mobile operators from blocking or charging consumers extra for using Internet-based communications services. Operators may still offer a range of mobile data tariffs with different download speeds and levels of service, but they cannot tie specific rates to the use of specific free Internet services.	The Netherlands is one of the few countries to address net neutrality concerns through legislation. The recent amendments were to the existing Telecommunications Act.		The Netherlands has decided to implement specific net neutrality provisions in legislation, as opposed to relying on general competition law.
United Kingdom	Ofcom have found that the use of market power and discrimination in traffic management to the benefit of one's retail arm is the main harm. Ofcom has not imposed strict restrictions on traffic manage-	The main legislative intervention occurred in the amendment to the Communications Act 2003 and the Wireless Telegraphy Act 2006, which empowered Ofcom to undertake particular actions	In May 2011, Ofcom amended the General Conditions of Entitlement to ensure that there is adequate transparency around the traffic-shaping methods employed by ISPs and mobile operators.	Ofcom is largely relying on existing regulation and market structure to protect against harm from the use of market power to discriminate in a non-neutral fashion.

Country	Summary	Legislation	Regulatory measures in place	Competition regime
	ment, but instead relies on existing regulation and market structures. In another light touch approach, they found that if ISPs failed to secure an efficient degree of transparency only then would Ofcom consider introducing "more prescriptive policy options". In response, most UK ISPs signed up to a voluntary code of practice which required enhanced information for customers.	should it deem it necessary by way of its licensing powers. These include the ability of Ofcom to impose minimum requirements in relation to quality of service. No such condition has been issued to date.	In particular, ISPs and mobile operators must provide details of the minimum QoS that is offered and information on procedures put in place by the undertaking to measure and shape traffic. Finally, given the concern that users could not exercise their ability to change providers as a result of any degradation or blocking there is a new General Condition 9.3 that requires that communications providers do not include conditions or procedures for contract termination that act as a disincentive for end-users to change communications provider.	
United States	The FCC has adopted targeted regulations, including net neutrality requirements, which apply to retail broadband	There have been a number of attempts to legislate net neutrality principles, but these have all been strongly opposed and none have	The FCC generally does not regulate the Internet or Internet-related services. Under the federal statutory framework, services are either regulated	The FCC regulates the competitive aspect of the telecommunications marketplace concurrently with the United States Department of

Country	Summary	Legislation	Regulatory measures in place	Competition regime
	access services. The FCC's rules prohibit fixed broadband service providers from blocking lawful content, applications, services or non-harmful devices. A narrower mandate applies to mobile broadband providers. The no-blocking rule is qualified by reasonable network management practices. The FCC's rules also forbid fixed broadband service providers from unreasonably discriminating in transmitting lawful traffic over a consumer broadband service. These regulations remain highly controversial and are being challenged in federal court. As of writing, a decision has not been released.	passed.	telecommunications services or unregulated information services, although the FCC has the authority to adopt regulations that apply to information services where necessary to achieve a specific statutory goal relating to telecommunications services. The FCC has deemed most broadband services to be unregulated information services. Generalized "pay for priority" practices would be unlikely to satisfy the unreasonable discrimination standard, but the rules allow tiered pricing based on bandwidth usage or speed.	Justice and the Federal Trade Commission, which holds general jurisdiction over antitrust and competition issues.

[1] Malcolm Webb thanks Gordon Moir, Jordan Cox and Chris Taylor of Webb Henderson for their contributions to this paper.

[2] See BEREC, 'Response to the European Commission's Consultation on the Open Internet and Net Neutrality in Europe', BoR (10)42, September 2010, 2-3.

[3] See BEREC, Draft BEREC Guidelines on Net Neutrality and Transparency', BoR (11) 44, September 2010, 7.

[4] See European Union, 'Legal Analysis of a Single Market for an Information Society – Net Neutrality' *(*November 2009), 3.

[5] See BEREC, 'Response to the European Commission's Consultation on the Open Internet and Net Neutrality in Europe', BoR (10) 42, September 2010, 3.

[6] See IEEE, 'Network Traffic Management and the Evolving Internet (White Paper)' (2 November 2010), 4.

[7] See BEREC, A View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe, BoR (12)30, 29 May 2012, 10.

[8] See BEREC, Response to the European Commission's Consultation on the Open Internet and Net Neutrality in Europe BoR, (10)42, September 2010, 15.

[9] See BEREC, A View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe, BoR (12)30, 29 May 2012, 9.

[10] See BEREC, 'Differentiation Practices and related competition issues in the scope of Net Neutrality', BoR (12) 31, 29 May 2012, 49.

[11] See CRTC, ISP Traffic Management Technologies: The State of the Art, January 2009.

[12] Ibid.

[13] See Napatech, Scaling Policy Enforcement and Deep Packet Inspection (white paper), January 2011, 3.

[14] See CRTC, ISP Traffic Management Technologies: The State of the Art, January 2009.

[15] Berkman Center for Internet & Society, 'Next Generation Connectivity, A review of broadband Internet transitions and policy from around the world', http://cyber.law.harvard.edu/pubrelease/broadband/

[16] See Ofcom, 'Ofcom's approach to net neutrality', (24 November 2011), 13-14.

[17] http://berec.europa.eu/files/news/bor_12_32_guidelines.pdf.

[18] Comcast Corporation v Federal Communications Commission and United States of America, 600 3f.D 642.

[19] Directive 2002/22/EC (the 'Universal Services Directive'), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:en:NOT.

[20] Germany: 3 out of 4 mobile operators now allow VoIP, one of them without additional costs.

[21]http://berec.europa.eu/files/document_register/2012/8/BoR_%2812%29_34_Expl._paper_to_PC_on_NN_2012.05.29.pdf.

[22] See Directive 2009/136/EC of the European Union Parliament and of the Council of 25 November 2009, Art 22(3).

[23] See Ofcom, 'Consolidated Version of General Conditions as at 9 July 2012' available online at http://stakeholders.ofcom.org.uk/binaries/telecoms/ga/general-conditions.pdf.

[24] See Ofcom, 'Ofcom's approach to net neutrality' available online at http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf.

[25] See http://www.broadbanduk.org/component/option,com_docman/task,doc_download/gid,1335/ See also BT's Broadband Usage Policy: http://bt.custhelp.com/app/answers/detail/a_id/10495/~/broadband-usage-policy.

[26] See 'Chile: A Leader in Net Neutrality Legislation' (accessed 18 July 2012) available online at: http://openmedia.ca/plan/international-comparisons/chile.

[27] Angela Daly, 'The Legality of Deep Packet Inspection' (June 2010), 8.

[28] For more information on the issue, see the ITU GSR12 Discussion Paper on "Safety and security in the cloud".

[29] See Scott Beardsley et al, 'Network Neutrality: An Opportunity to Create a Sustainable Business Model' in *The Global Information Technology Report 2012: Living in a Hyper Connected World*, 58.

[30] See BEREC, 'An Assessment of IP-Interconnection in the Context of Net Neutrality (Draft)' (29 May 2012), 14.

[31] See Scott Beardsley et al, 'Network Neutrality: An Opportunity to Create a Sustainable Business Model' in *The Global Information Technology Report 2012: Living in a Hyper Connected World*, 57 – 58.

[32] The BITAG Technical Working Group brings together experts from across the industry to research and formulate opinions and "best practices" on technical management issues that impact on internet management. Some of the stated roles of BITAG are to: (1) educate policy-makers on technical issues; (2) identify "best practices" and issue advisory opinions; and (3) provide technical guidance to affected industries and the public.

[33] See W3C homepage available online at: http://www.w3.org/ (accessed 11 September 2012).

[34] See Scott Beardsley et al, 'Network Neutrality: An Opportunity to Create a Sustainable Business Model' in *The Global Information Technology Report 2012: Living in a Hyper Connected World*, 59.

[35] See Thunstrom, B et al, 'Disruptive Threat or Innovative Opportunity? Scenarios for Mobile Voice OTT', 5.

[36] For more information, see www.itu.int/wcit.

[37] See Center for Democracy & Technology, 'ETNO Proposal Threatens to Impair Access to Open, Global Internet' (21 June 2012), 5-6.

[38] See BBC, 'Facebook Valued at $104bn as Share Price Unveiled', available online at: http://www.bbc.co.uk/news/business-18105608 (accessed 20 May 2012).

[39] See latest EC discussion paper on enforcing non-discrimination principles - http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/non_discrimination/index_en.htm

[40] See European Commission, Progress Report on the Single European Electronic Communications Market 2009, SEC (2010)630, p 6.

[41] Commission Recommendation of 20 September 2010 on regulated access to Next Generation Access Networks, 2010/572/EU.

[xlii] Unless sourced separately, for most jurisdictions see Getting the Deal Through, 'Telecoms and Media: An Overview of Regulation in 46 Jurisdictions Worldwide' (2011 and 2012).

[xliii] Directive 2002/22/EC (the 'Universal Services Directive'), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:en:NOT.

GSR 2012 Discussion Paper

Spectrum Policy in a Hyperconnected Digital Mobile World

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 19 October 2012.

ACKNOWLEDGEMENTS

The author is grateful to Mindel De La Torre and Walt Strack (USA), H. Nwana, Wesley Milton and Mike Goddard (UK), Veena Rawat, Marc Dupuis and Eric Vachon (Canada), Marianne Treschow (Sweden), Kyu Jin Wee (Korea), Maureen Cahill and Catherine Gladman (Australia), Dave Kershaw (New Zealand), and Mercy Wanjau (Kenya) for their inputs and advice.

TABLE OF CONTENTS

SPECTRUM POLICY IN A HYPERCONNECTED DIGITAL MOBILE WORLD

Author: Dr Bob Horton, Senior ICT Expert[1]

1. *The Forces of Change*

1.1 Introduction

In the ICT sector, there are many forces at work which may cause governments to rethink spectrum policy. These include convergence, globalization, use of the Internet, the increasing demand for broadband and mobility, competitive conditions, much broader availability of wireless and the trend toward integrated national broadband policies. These have created a greater complexity in which policy-makers face the challenge of how to best utilize the limited resource of spectrum.

Within this context, a well-designed spectrum policy is essential in a digital world. In this digital world, advances in broadband have put a strain on wireless capacity compared to an age when the Internet was not easily accessible through mobile devices. In turn, this has caused a re-evaluation of the different options in bringing spectrum to market and the regulatory basis for this to happen in an efficient, cost-effective way, while also allowing continuing innovation to occur.

Therefore, as a prelude to examining the modern practices in spectrum policy and its implementation, it is necessary to review this broader scope of developments as background to succeeding sections of this paper. This paper firstly addresses the general evolving nature of the wireless industry, and with this the changes for regulators over the past two decades. Bourgeoning demand for data has emphasized the critical nature of the limited resource of spectrum and the need to accommodate foreshadowed demand for spectrum. These considerations have a particular relevance to considerations of national spectrum policy and planning which should be regarded as a key component in evolving national broadband policies.

In the second section of the paper, high level policy principles are examined, along with the beginnings of an approach to discovering best practice in spectrum policy.

The third section moves into the most important elements which comprise best practice in contemporary spectrum policy and its implementation to satisfy today's needs, including the need for a National Spectrum Plan and periodic consultation to maintain an up to date Plan. Also needed is a well understood, market-based plan for making spectrum available. This section includes "pathfinding" examples from several countries and regions which aim to achieve the sought after efficiencies and objectives of spectrum policy in a world that is experiencing exploding demand for mobile broadband services.

1.2 Digitization effects and convergence

Whilst networks used to be built vertically around specific applications (e.g., the public switched telephone network for voice or broadcasting systems for television), digitization and the advent of the Next Generation Network (NGN) has 'de-layered' networks so that content or applications are no longer network specific. Thus, an IP network can easily transmit all forms of voice, data, and video. This, in turn, is paving the way for 'over the top' (OTT) content and service providers. The impact of such convergence for regulation is profound, as formerly distinct regulatory regimes become less suited to today's converged networks and services. Determining how wireless networks fit into this world, and how spectrum policy can be designed to maximize the potential of wireless broadband will be an important issue for regulators going forward.

1.3 Data serves up a new date with destiny

The digitization of communications networks is a phenomenon which is not new and is no longer unexpected. It has been occurring for decades. However, digitization, in combination with the development of the Internet protocol (IP) and the rapid deployment of IP-based networks, has accelerated convergence and enhanced the immediacy of all types of communications which were at one time comparmentalized and self-contained.

The explosive global growth of mobile data has swamped voice traffic. Demand for new broadband applications and services is a game changing development for carriers and service providers. In combination with the arrival of smart phones and tablets, these developments have created the beginnings of a seismic shift in industry structure and relationships. For example, emerging machine-to-machine (m2m) communications, cloud services, and other OTT services are giving rise to a new breed of service provider. Many of these new services and providers are in their infancy, but the evidence of greater things to come is overwhelming.

As a result of these new technologies and services, traditional business models and concepts of regulation are now being challenged. The implications of these changes for wireless regulation are especially relevant to developing countries, where wireless is likely to be the primary vehicle for broadband service delivery.

Both fixed and mobile voice services have been the bedrock business for carriers until recent times. Margins in the past have been significant and the augmented service of SMS tied to mobile voice services has been a digital addition which has been highly lucrative on a per character basis.

The advent of faster, more advanced technologies, however, has begun to radically change the wireless industry. With smartphones and tablets, mobile broadband users are now able to take advantage of a wide range of wireless services and applications, including mobile VOIP (e.g., Skype) and other WiFi or on-net applications. Networks will require some degree of re-design and dimensioning for the future to meet the demands of new consumer and business applications. Looking ahead, several trends can be identified that will put even more pressure on wireless networks—heightening the need to plan for and manage/regulate the spectrum resource.

The introduction of smart phones/tablets has allowed third-party service providers to treat carriers as simply providing "dumb pipes," with the service providers taking increasing charge of applications/services and users.
In a recent report, Google provided current penetration rates for smartphones in selected countries around the world.[2] This is reproduced in Figure 1. Of particular interest are comparisons between developed and developing countries, where penetration rates do not appear to reflect the status of development. ITU data also confirms the rapid take-up of broadband-enabled mobile phones.[3] A recent report from Pyramid Research indicates that by 2017 emerging markets will account for 63 per cent of all smartphone sales, compared with 42 per cent in 2011.[4] This again points to mobile service developments being the vehicle for breaking down barriers to advancement and helping to reduce the digital divide. The implication is that the foundation for future IP service development is much more promising for all countries.

Figure 1: Penetration of smartphones in selected countries (May 2012)

Penetration	%	Penetration	%
USA	44	JAPAN	20
UK	51	GERMANY	29
UAE	61	EGYPT	26
SWEDEN	51	CANADA	33
SAUDI ARABIA	60	BRAZIL	14
NZ	44	AUSTRALIA	52
MEXICO	20	ARGENTINA	24

Source : Google/IPSOS

m2m communications and similar transactional scenarios

The impressive forecasts of 50billion communicating (m2m) devices by 2020[5] will demand a greater relative signalling capacity, and indeed signalling congestion may pose a threat for networks if they continue as they are currently dimensioned. This is a consequence of "hyperconnectivity" as distinct from the simpler connectivity between persons (Metcalfe's Law) or social networks (Reed's Law).

Such applications will see the transmission of only a small amount of data per transaction but done on a more frequent basis. This might be from interactions to alleviate battery drain, or applications such as interactive gaming, patient monitoring, meter reading, intelligent transport systems etc. Smartphones also contribute to this situation by making constant queries to the network as they move amongst cell sites to convey email, to access social networking and to conduct repetitive actions. Always-on applications rely on constant signalling messages to and from the network. Consequently, whilst end-user data traffic is growing quickly, signalling traffic (which is overhead data for networking purposes) is outpacing it by 30 to 50 per cent.[6]

Cloud communications

Cloud communications is another growing trend, whereby information is stored in remote servers and then accessed by consumers and business users on an as-needed basis. For consumers, this can be a way to securely store music, photos and other information, with the advantage of being able to access that information from anywhere there is a broadband connection. For businesses, the cloud can store all types of information that workers in the field can access when they need it. This, however, adds to the growing needs for data carriage capacity for the bulk transfer of data amongst data sites and destinations and ultimately for the spectrum to make wireless access and carriage solutions possible.

1.4 A closer focus on mobile developments: traffic is increasing rapidly

Reflecting these growth trends, at the end of 2011, there were close to 6 billion mobile-cellular subscriptions with global penetration reaching 86 per cent, with 78 per cent in the developing world.[7] Mobile-broadband

subscriptions have grown 45 per cent annually over the last four years, and there are now twice as many mobile-broadband subscriptions as there are fixed-broadband subscriptions. While people in developed countries use mobile-broadband networks in addition to fixed-broadband connections, mobile broadband is often the only access method available to people in developing countries, especially outside urban areas.

In its studies of the future, Cisco predicts that global mobile data traffic will grow 18-fold from 2011 to 2016 with a compound growth rate of 78 per cent.[8] This is three times faster than fixed broadband traffic. Mobile data traffic in 2016 is expected to reach 10.8 exabytes per month.

The implications of this growth for carriers are serious. A study by Tellabs[9] suggests that profitability could be extremely challenging for some mobile operators within three years. This is a result of the mobile Internet forcing operators to transform their networks and business plans. Without rethinking the design and capabilities of their networks, the study claims that costs will surpass revenue for many operators throughout North America, the developed Asia-Pacific countries, and Western Europe in this three-year time frame. Since users have embraced the mobile Internet, traditional ways of handling traffic growth (e.g., cell splitting) have become expensive, and competition has increased pressure on revenues. Box 1 discusses the changes that result from demographic shifts and their potential to increase demand for services, particularly in urban areas of developing countries.

Box 1: The Impact of Demographic Shifts on Mobile Demand in Africa

By 2050 the market in Africa for telecommunications services (and for many other goods and services) will grow by an additional 1.5 billion people, representing almost half of the total market expansion worldwide.[10] The majority of this region's population will be living in urban areas, where telecommunications infrastructure is relatively easier to roll out and upgrade. An additional 800 million people will be living in Africa's cities by 2050 (taking the total to 1.2 billion), compared to 500 million in India and 340 million in China. This represents 300 per cent growth in urbanisation in Africa compared to 70 per cent in Asia.

With mobile market penetration currently standing at about 65 per cent, this huge growth will undoubtedly bring a range of challenges to Africa but the opportunities for the telecommunications industry are unparalleled.

The demographic challenge of significant urbanization will make ICT and education key enablers to allow the citizen of the metropolis to fully participate in and derive a living from the information age. This is not an issue which is unique to Africa, though it is more poignant. It is not an issue that is even unique to developing countries, but equally applies to developed countries and hence unites the world in a common cause. Wireless infrastructure is highly important in this scenario and probably more critical to developing countries. Ergo good spectrum management is a future centrepiece of economic and social cohesion in society.

Source: Author.

Future regulation needs to reflect these important developments, and the industry challenges which have arisen.

2. *Spectrum policy: high level principles*

2.1 Introduction

The changes in the wireless communications environment described in Section 1 have prompted consideration of the effects of these changes on regulation in a number of the ITU's areas of activity.[11]

Regulators rely on a combination of administrative and market-oriented approaches to managing spectrum. In addition, there are pioneering considerations of new approaches to aspects of spectrum allocation and assignment within some regulatory bodies, such as in the areas of spectrum sharing, greater use of unlicensed spectrum, incentive pricing, etc. A question is whether traditional regulatory approaches and principles (and implementation) of spectrum policy are sufficient and appropriate to carry forward into the future – or whether there is a need for a re-assessment of parts of the regulatory approach to deployment of spectrum.

Best practice in the fully digital era with national regulation is influenced more than ever by externalities such as links to other domestic imperatives like a national broadband plan and NGN expectations, the achievement of universal access and service, support for industry, and political concerns for privacy, security, a degree of control, and social ambitions. Regional influence and interaction is now more evident than ever, and the voice of regional bodies is far more effective in international fora such as the ITU. Manufacturers significantly define the boundaries of what is possible, and they prefer production on a global (rather than a country- or region-specific) basis. Consequently, international harmonization is particularly important and a leading factor in spectrum policy decisions.

Some differences have also emerged in the past between developed and developing countries, and these differences may be holding back progress in some cases. The differences can be traced to a lack of confidence or involvement in change, and tardiness in regulatory reform. However, mobile broadband does enable a narrowing of the broadband gap because of the adaptability of the technology to different environments and needs. In order to realize this goal, however, one of the biggest issues for policy and regulation going forward is making spectrum available to support the growth of broadband services. Other major companion challenges are dealt with elsewhere in GSR12 discussion papers.

2.2 Approaching best practice

A number of attempts have been made in the past to capture the important constituents of best practice in spectrum policy.[12] Some conclusions – such as the applicability of high level principles - are still valid today. Other implementation considerations need refreshing and re-casting in the developing environment. It is therefore useful to subdivide "best practice" into high level principles and then their achievement.

With regard to high level spectrum policy principles, there are some durable factors that still remain as valid as they were seven years ago at GSR05[13] and will likely still remain valid for years to come (see section 2.3). Thus, the focus of best practice lies with developing new implementation approaches that flow from these enduring principles.

The main influence in re-assessing best practice is the broadened scope of consideration. In the past, attention has been closely focused on the unique and narrow issues associated with radiocommunications. Today, a greater influence of wireless services in society and mainstream economics causes a need to examine policies for their suitability. It is, however, worthwhile to analyze existing views on best practice and to then address those areas which could be updated to better fit today's circumstances.

For example, mobile networks have made universal access to voice services feasible in most countries, and most markets have been able to support at least limited facilities-based mobile competition, which makes regulation less

necessary than for fixed networks (which historically have been provided by a monopoly incumbent). In addition, in recent years, wireless technology has advanced to the point that it can now also support (increasingly capable) broadband.

2.3 High level policy principles and their implementation

GSR05 in Tunisia produced high level Best Practice Guidelines for Spectrum Management to Promote Broadband Access.[14] The Guidelines focused on 10 key areas that demand consideration in the quest for best practice:

- Facilitate broadband deployment;
- Promote transparency;
- Support technology neutrality;
- Enhance flexible use measures;
- Ensure affordability;
- Make spectrum available in a time fashion;;
- Manage spectrum efficiently;
- Level the competitive playing field;
- Harmonize (International and Regional) policies; and
- Take a broad approach to promoting broadband access.

These formed a durable set of high level principles that are still relevant today. They provide a baseline for first principles consultation by policy makers with stakeholders, especially industry, and they provide a starting point for the implementation of other elements of a National Spectrum Policy. The output statement from the ITU's 2011 Global Symposium for Regulators (GSR11) is worth repeating for completeness. At that meeting, participants drew attention to the challenges of making spectrum - which is a cornerstone of growth in the digital information age - available for mobile broadband.[15] Regulators and policy makers were urged to address a host of issues in order to ensure that spectrum is used in the most efficient manner.

GSR11 participants expressed a preference for implementing incentive-based, market-driven approaches to making more spectrum available (where scarcity of spectrum exists).[16] For example, a number of auction techniques were cited as having the potential to extend broadband to underserved areas. Furthermore, allowing flexible use of spectrum, including spectrum refarming and secondary markets was seen as key to ensuring that with market maturity and evolution, spectrum moves to more productive uses. The Guidelines also envisage leveraging the "digital dividend" spectrum, and the use of TV "white spaces" for unlicensed broadband device use.

To implement such principles, many countries are now developing national spectrum plans to guide their wireless sector development. To support the development of such a National Spectrum Plan, other implementation and policy considerations deriving from the high level principles involve the conduct of an inventory of national spectrum needs, comprehensive public consultation on a national basis, and the development of a spectrum program that is market-based and brings transparency and certainty to prospective investors in wireless applications. These national implementation efforts are often complemented by and dependent on an engagement strategy with regional and international bodies in order to achieve the full benefits of harmonization and standardization.

2.4 The changed regulatory model – *'Third Generation Regulation'*

To address such issues, a new model for spectrum regulation is coming into practice. In step with evolving regulatory approaches in telecommunications as a whole, the strategy of dealing with the allocation and assignment of spectrum has also matured through three phases during the last two decades, irrespective of whether the regulatory function in any particular country has been associated closely in an organizational sense with telecommunications regulation or not. The evolution of wireless regulatory models has changed in accordance with

policy priorities at the time and shifting market and industry structures. Each of these shifts in approach has been heavily influenced by advances in technology, the opportunities afforded through convergence, and socio-economic needs.

Since the days of the traditional Post Telephone and Telegraph (PTT) organizations, in which regulation and operations were entwined within a single government body (or "Administration", there have been three clearly distinguishable generations of regulation, as shown in **Table 1**.

Table 1: Generational changes in regulation

Regulatory Phase	Policy Priorities	Regulation Focus	Spectrum Management
1st Generation	Regulation of a monopoly	Independent regulation, correcting monopolistic behaviour, price regulation (ROR[17] or price caps)	Separate administrative methods of spectrum allocation and assignment
2nd Generation	Infrastructure Competition	Resale, pricing, access, call selection, unbundling, bitstream access, cross-subsidised universal access	Increasing use of market methods for allocation of spectrum. Some merging of regulatory bodies
3rd Generation	Service Provider Competition	Network and spectrum sharing, net neutrality, more focus on regulation of content and applications, bitstream access, universal access no longer cross subsidy.	Broader integrated spectrum policies. Affordable new spectrum. Re-use of existing spectrum. Sharing and flexibility. Alternatives in using spectrum

Source: Author.

Across these three generations, because of quickly growing demand and a realization of spectrum scarcity, administrative methods of assignment have increasingly been replaced by market approaches that seek to apply economic criteria for achieving the highest-valued use of the spectrum where appropriate. More recently, questions have been posed over how spectrum should be valued and the disconnect between socio-political and economic descriptions of value.

The transition from the second generation to third generation regulatory models has been led by convergence, spectrum scarcity and a pervasiveness of broadband communications throughout the world's economy. From the point of view of spectrum and its management, wireless is now seen as part of a broader scheme within the communications field largely brought about by the growing importance and visibility of mobile broadband. Because of the pressure on spectrum and its availability, the focus of the spectrum regulator is moving to evaluation of alternative uses of spectrum, re-use, re-farming, liberalization and a renewed scrutiny of the efficiency of current spectrum uses. This broader ambit, for example, has led to more in-depth consideration in many countries of how broadcast spectrum is used and how that spectrum could be used to create a "digital dividend" that would benefit wireless broadband users..

Today, such matters require resolution by the 'third generation regulator." The underlying principles in the model apply whether the spectrum regulatory function is managed by a converged ICT regulator or a more narrowly constituted body. Thus, it is not necessary to converge the regulatory functions in an organizational sense, but to recognize the increased interdependence and interworking which is now necessary. The third generation will take us into the future.

3. *Creating a national spectrum policy*

3.1 Introduction

Accounting for the bourgeoning need for data delivery and the spectrum to support it, as well as providing for many other users of the spectrum creates a considerable challenge for the regulation of spectrum. The massive uptake foreseen for mobile data and video applications and services, short range devices, m2m communications, fixed/mobile cloud services, m commerce, etc. provide the genesis of much greater demand.

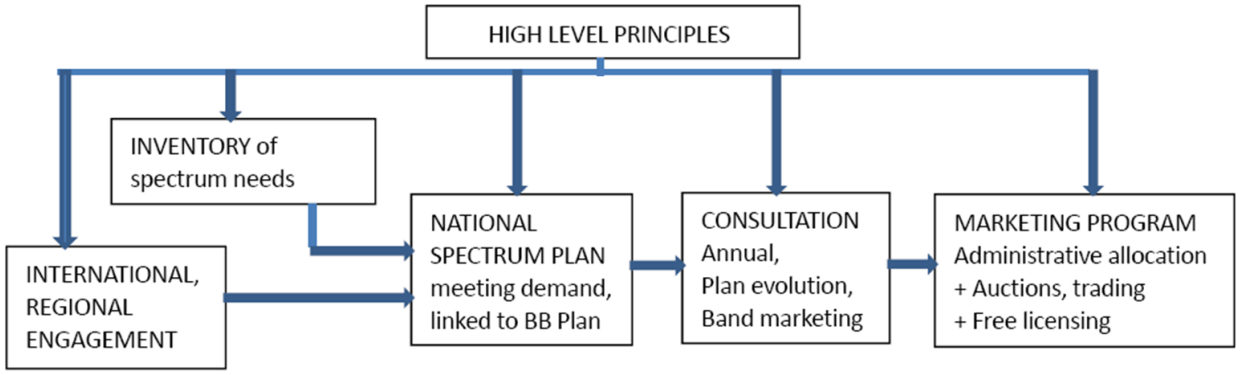
In seeking to meet that demand, operators know that optimum technical efficiency is extremely important in emerging network and system developments. Regulators and policy-makers also have tools at their disposal when it comes to making sure that the supply of spectrum is sufficient to meet rising demands. These include re-farming existing allocations or assignments for to allow new services, using the digital dividend that comes from the migration of broadcasting services, as well as new or re-purposed bands for mobile services (such as in unlicensed applications). For such approaches to be most successful, they should be considered as elements in an overall National Spectrum Policy that starts with clear goals and can serve as a blueprint for managing spectrum over time.

This Section addresses the elements needed in a National Spectrum Policy, introduces some contemporary best practice and provides relevant examples of how some countries have addressed spectrum management issues. The elements are:

- wider recognition, visibility and accountability of the spectrum function;
- an inventory of spectrum needs;
- a National Spectrum Plan and rolling annual consultation;
- a Market-based approach for assignment of spectrum; and
- a strategy of international and regional engagement.

These elements are summarized in Figure 2 as five implementation elements flowing from the high level principles, and which have the aim of achieving spectral efficiency while meeting demand. Each element is discussed in detail in the following sections.

Figure 2: Elements of a National Spectrum Policy



Source: Author.

3.2 Wider recognition of the spectrum function

Historically, the function of spectrum management has been concealed behind high technical barriers to understanding. The job of allocating spectrum has largely been left to specialists and engineers who are responsible for allocating wireless services within particular bands and providing for acceptable interference arrangements between licensees.

Some of the factors that have given spectrum management a higher profile include –

- significant returns to treasuries from the auction of commercial services;
- convergence (the ability of wireless to deliver voice, data and video services); and
- increasing demand for spectrum to support emerging broadband applications.

As a result, spectrum policy now needs to be factored into the wider canvas of national broadband policies, and should be widely consulted as part of the development of a national broadband plan. Interdependencies of converging industries and services affect the implementation of spectrum policies and vice versa. In addition, there is an increasing need to consider how wireless services can assist the goals of universal service. As a result of these interrelated considerations, governments are also considering the further integration or convergence in an organizational sense of the regulator where this has not already taken place.

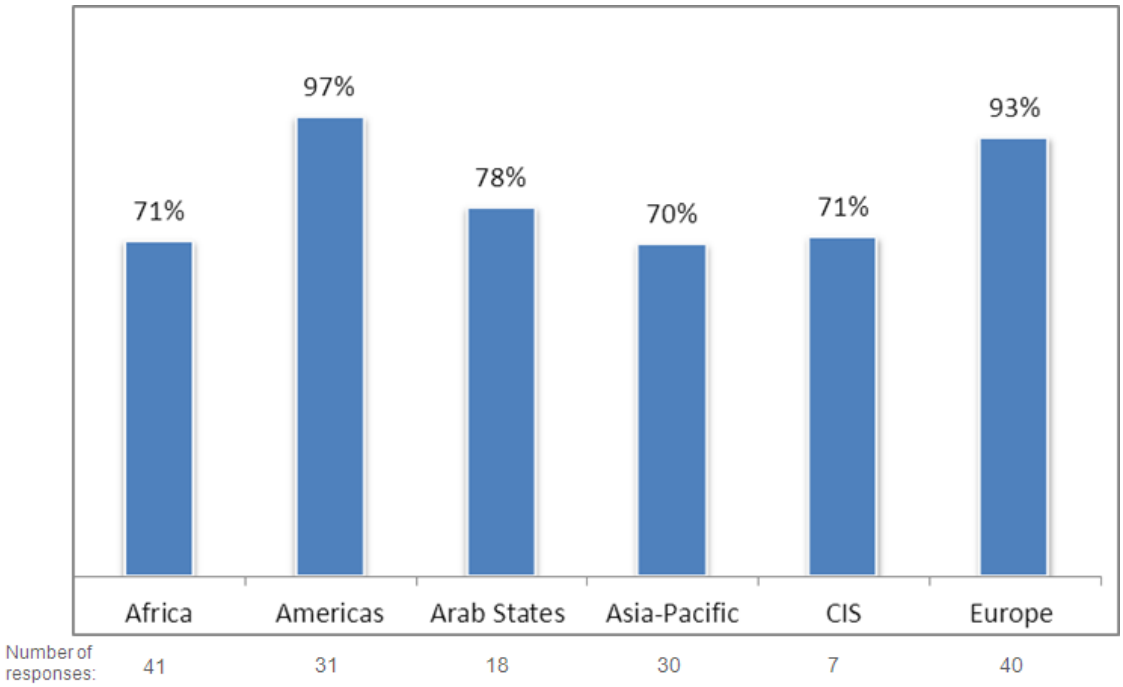
In the United States**,** 2010 saw a landmark report from the FCC in its *National Broadband Plan.*[18] Issues discussed in the Plan included the need for: greater transparency in spectrum allocations; incentive mechanisms to reallocate or repurpose spectrum; more spectrum made available within the next 10 years; and expanded opportunities for innovative spectrum access models such as unlicensed use. Efforts in spectrum reform took on greater significance in June 2010 with a Presidential Memorandum entitled "*Unleashing the Wireless Broadband Revolution.*"[19]

The United States example is instructive for several reasons. First, it shows that spectrum matters in the United States have been raised to a higher level of visibility and significance in the context of planning for the future.. Second, the time context to consider for planning and regulatory activity was recognized to be over a long term—a period of 10 years. Third, the demand for spectrum for new wireless services is very significant (estimated at an extra 500 MHz) and calls into question existing allocations and the justification and efficiencies of current approaches to fulfilling spectrum needs. Fourth, the demands for commercial and Government use of spectrum need to be comparatively assessed and prioritized, given the limited availability of spectrum.

As part of the U.S. initiatives, the Department of Commerce's National Telecommunications and Information Administration (NTIA) has released a number of reports.[20] The most report recent addresses the repurposing of government spectrum in one of the bands entitled "*An Assessment of the Viability of Accommodating Wireless Broadband in the 1755 – 1850 MHz Band*".[21] Here, the NTIA concludes that a repurposing of all 95 MHz is possible. However, the extent to which the spectrum can be made exclusively available to commercial interests—and in what timeframe—requires further discussions between agencies and the industry. Possible solutions include partial clearing scenarios and a phased approach to commercial auctions and entry. Some federal systems might need to remain in the band indefinitely. Thus, negotiation is the favored way forward, rather than fiat. This has also been the favored way in the United Kingdom for many years**.**

As the previous examples illustrate, transparent access to relevant information by all stakeholders is an important way to ensure greater recognition of the importance of spectrum. A general measure of transparency amongst countries is provided by the ITU as a result of a questionnaire over whether a country makes publicly available information on spectrum (e.g. regulations, a spectrum management table, and spectrum fees).[22] The responses are shown in Table 2 in regional summary and these indicate an encouraging situation.

Table 2: Spectrum information made available, percentage of country responses by region, 2011



Source : ITU World Telecommunication/ICT Regulatory Database

3.3 An inventory of spectrum needs

An inventory provides substantive evidence of spectrum needs and should involve demand and supply considerations and most likely an active database to track spectrum use. The inventory allows for a review and justification of spectrum needs for individual radiocommunication services: which will involve metrics covering the technical, economic and social efficiency of the use of spectrum. As such, inventories can also be useful in determining where spectrum is underutilized or where it might be possible to reallocate spectrum for new uses. This aggregation of potential demand for spectrum is an exercise which is now common amongst many countries as they try to dimension the challenge of spectrum into the future.

Spectrum needs cover many industries and user communities. The ITU-R considers spectrum usage and demand for different services in its work within the Study Groups leading up to World Radiocommunication Conferences (WRCs) and Radiocommunication Assemblies (RAs). This work can also serve as a useful reference for services that need to be accounted for in a National Spectrum Plan, helping to lay out uses and allocations, on a primary and secondary basis.

In the United States, the FCC's National Broadband Plan also gives consideration to methods for ongoing measurement of spectrum utilization and a triennial assessment of spectrum allocations. In Australia**,** the regulator - ACMA[23] - provides an annual rolling 5-year forecast of spectrum demand drivers, the top spectrum projects over the 5-year period and specific work plan priorities over 2012-2016 in the current version. These are followed up with open consultative processes on the itemized projects as the year proceeds.

Europe is currently in the process of conducting an inventory of spectrum uses over the range 400 MHz to 6 GHz, with a view to putting focus on the *supply side* of spectrum provision and efficiency of spectrum use.[24] Functional characteristics will be matched by efficiency metrics, and the program will depend critically on a transparent and compatible pan-European ECO Frequency and Information System database.[25] Spectrum man-

agement agencies throughout Europe will cooperate and improve national databases and inventories, which currently exist in Denmark, Finland, France, the Netherlands and the UK.

Canada has also implemented a stocktake of the current use of spectrum across the range of services in Canada, and commissioned a study of future demand up to 2015 for radio spectrum in Canada.[26] One interesting feature of the study from Canada is its categorization of Scenarios. One scenario is a *wireless only* solution to broadband demand, which, whilst it may be of more academic interest to Canada, could well be the scenario of greatest interest to developing countries where wireless solutions will prevail. In this scenario, there is rapid progression to higher levels of wireless communications. The range of demand across the scenarios is 300 – 500 MHz by 2015. The other two scenarios comprise a more balanced fixed and wireless provision with the differences being the rates of uptake.

3.4 The importance of a National Spectrum Plan

Organizing spectrum to be available in a timely fashion to meet developing needs involves long term thinking as part of the national strategy. As mentioned, a National Spectrum Plan should be a widely consulted document with a horizon of at least 5 or 10 years. Once established it can be publicly "rolled over" through forecasts and consultation on an annual basis for updates as technology and markets evolve. This assists transparency and orderly spectrum allocation by the regulator, and allows spectrum marketing proposals to be discussed progressively. Longer timeframes allow appropriate and meaningful milestones to be built in.

Sweden has a well-designed Spectrum Strategy proposal[27] summarized in Box 2.

Box 2: Spectrum Strategy Proposal: Sweden

- **Inventory phase**: demand and supply (today and out to 2022), followed by
- **Analysis phase**: a review of frequency bands and evaluation of current and potential usage of spectrum, followed by
- **Implementation phase**: involving review or phasing out of current usage of spectrum; together with license conditions; assignment options; and finally assignment

Source: NPTA Sweden

These efforts will be supported by principles and tools to optimise the public welfare, together with efficient instruments for spectrum management, and efficient technical rules for licensees. The consultation referred to in Figure 2 has a number of considerations and is not confined to just the National Spectrum Plan. It also refers to other separate consultations over the market proposals for spectrum, and even further to the broadest of consultation on spectrum in a wider policy environment.

For regulators and policy makers seeking to develop a National Spectrum Plan that will allow them to better match spectrum supply and demand—and make more spectrum available for broadband uses—a number of policies can be implemented. For example, a Report to the United States Congress[28] notes that there are currently three key policy tools for increasing the availability of spectrum for wireless broadband:

- allocation of additional spectrum
- re-assigning spectrum to other users (with compensation)
- opening up spectrum for unlicensed use

Other policy options considered include:

- sharing of network infrastructure
- changing the cost structure of spectrum access
- more spectrum efficient technologies, and
- sharing spectrum.

Box 3: Categories of future spectrum needs

Aeronautical Mobile : voice and data communications necessary for the safety and efficiency of aviation

Broadcasting : intended for direct reception by the general public on AM, FM and digital systems

Fixed Services: between a fixed transmitter and one or more fixed receivers

Land Mobile: terrestrial services between base stations and mobile stations, or directly between mobiles

Maritime : communications for safety and efficiency of maritime military, civilian, and search and rescue

Radiodetermination: to obtain position, velocity or other characteristics of an object

Satellites : enabling international communications or large coverage areas or rapid deployment

Science Services: for Earth and space station data transfer for processing

Wireless Access Services : terrestrial connections for a user to a core network Internet or other provider

Emerging Technologies : adoption of future developments

Source : ACMA Australia 5-year Spectrum Outlook

A dynamic concept of spectrum sharing arises from a progression from static channel allocation approaches to those for network-centric technologies typical of responding to the instantaneous character of Internet-type services. Spectrum-sharing techniques include geolocation databases, smart antennas and cognitive radio and may lead to dramatically different ways of managing a nation's spectrum resources.[29]

A comprehensive National Spectrum Plan should account for all required services – for example – as summarized in Box 3. Specific applications are contained within these categories of service (i.e., public safety systems are provided under the Land Mobile service). Areas of spectrum scarcity and how to place a value on the quite different uses of spectrum (commercial vs non-commercial and emerging vs. existing services) is an increasing challenge which confronts both the policy-maker and the regulator who must manage spectrum allocation in practice. This is a delicate balancing act.

In the United States, for example, the FCC National Broadband Plan sees the need to make spectrum available for the development and evolution of new technologies. This need is foreseen to be met partly by freeing up a new, contiguous nationwide band for unlicensed use. Also, finalization of rules for the use of TV white space spectrum[30] was made possible by innovative databases and cognitive radio techniques, and on a licensed or unlicensed basis. "Opportunistic" or "cognitive" technologies - which generally do not require a license and which are at a pre-commercial stage - may significantly increase the capacity of spectrum in the future by sharing available spectrum dynamically without disrupting incumbent, licensed users.

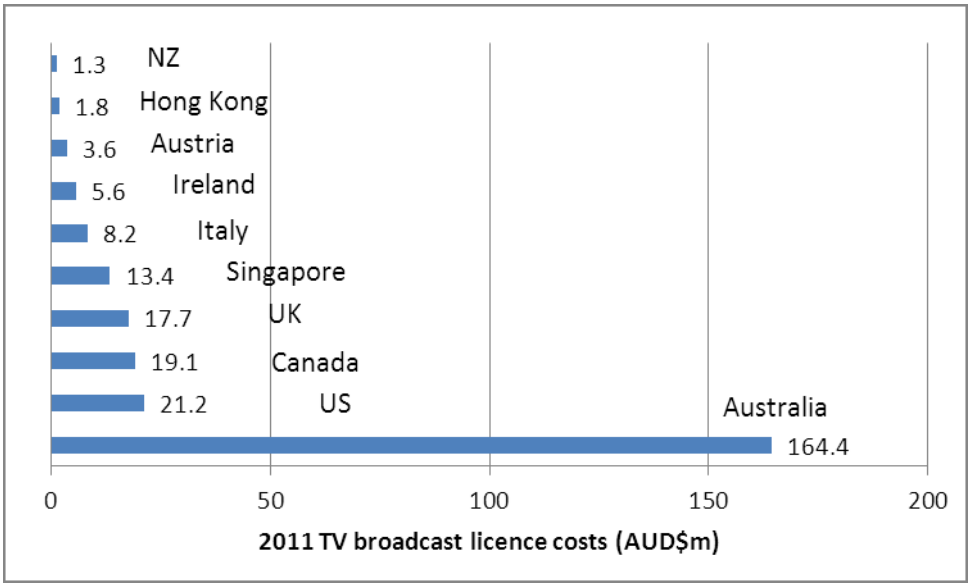
As policy-makers and regulators seek to promote radio services and manage spectrum efficiently, it will be important to recognize the international context within which decisions are made. A National Spectrum Plan should be consistent with agreements reached at WRCs and RAs as those agreements provide the certainty to implement radiocommunication services in a harmonized and standardized way. To accommodate special circumstances, countries can insert footnotes to the regulations allowing differing national allocations.

Importantly, the ITU has begun a significant work programme that is designed to identify additional spectrum that could be used for mobile broadband services. The agenda for the 2015 WRC, which guides much of the Study Groups' activities, includes Agenda Item 1.1 in the Land Mobile category which is –

'to consider additional spectrum allocations to the mobile service on a primary basis and identification of additional frequency bands for International Mobile Telecommunications (IMT) and related regulatory provisions, to facilitate the development of terrestrial mobile broadband applications in accordance with Resolution **233 (COM6/8)WRC-12**'

A recent Inquiry into Convergence[31] in Australia examines the fundamental change brought about by convergence and puts forward recommendations for a new principles-based policy framework that should reduce compliance costs and increase certainty and flexibility whilst ensuring that services continue to meet expectations. The Inquiry was partly informed by reports from the ACMA on "broken concepts" and "enduring concepts."[32] One issue that arose during the Inquiry was the matter of charging for the use of broadcasting spectrum. It was shown that commercial TV and radio broadcasters in the broadcasting services bands are subject to licence fees calculated as a percentage of gross earnings, with 9 per cent for television and 3.25 per cent for radio in 2011. Four other countries have a similar approach to TV broadcast license costs: New Zealand, Singapore, Austria and Italy, whilst New Zealand (which has a dual fee structure), Canada and the United Kingdom have charges determined by a market-based mechanism. Licence cost comparisons are as follows in Figure 3.[33]

Figure 3: Comparisons of TV Broadcast License Costs



Source: 20. Australian Government. "Convergence Review : Final Report". March 2012. www.dbcde.gov.au

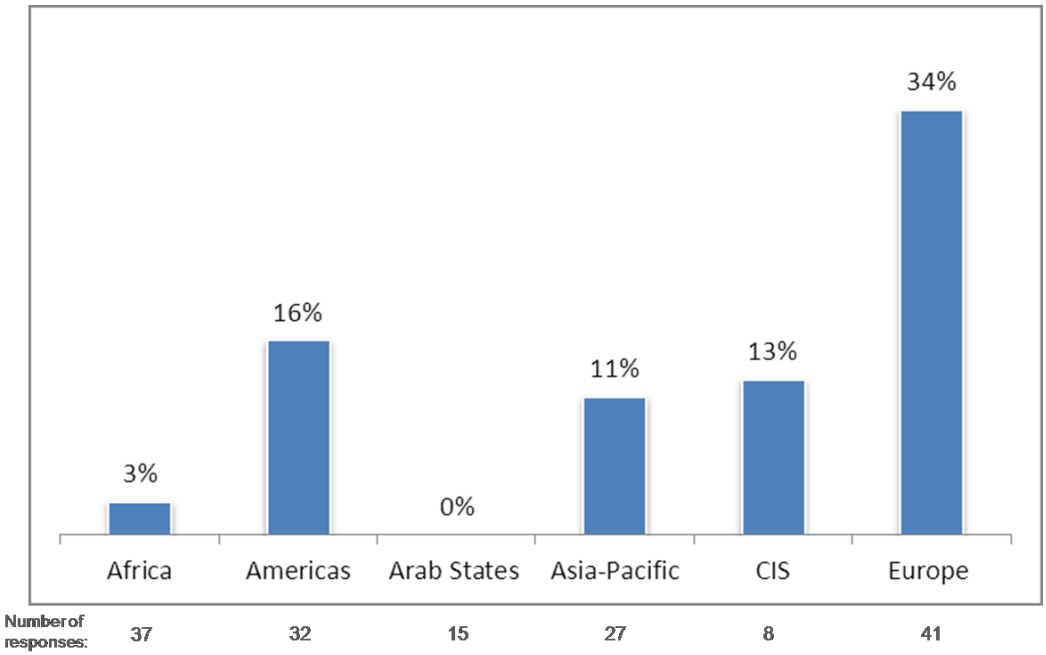
The recommendation to the Australian government on this particular matter tracks the initiative of the UK, noting that, because convergence is eroding the boundaries between broadcasting, voice communications and data transmission, spectrum allocation should as far as possible be based on spectrum management resources, not content. In addition, the regulator should develop methods to value spectrum (see below) and derive an appropri-

ate license fee in consultation with existing broadcasters. This would allow a non-discriminatory and affordable approach to licensing.

As policy makers and regulators seek to develop a National Spectrum Plan, one area that shows a division of thinking in spectrum policy amongst countries is the licence-exempt model. Whilst somewhat dated, the World Bank's InfoDev program in 2003 estimated that only 41 per cent of developing countries had rules for licence-exempt bands compared with 96 per cent of developed countries.[34] This may have undesirable consequences by dissuading new technologies from coming to market in developing countries, especially considering the leap-frogging potential they may offer to those countries.

Secondary trading of spectrum is another area of contrast, as shown in ITU statistics and data on which countries allow this.[35] This information is summarized by region in Table 3. It shows that countries in Europe are much more involved in secondary trading of spectrum, and are reaping the benefits that this brings in administering spectrum, whilst other regions have generally not adopted such approaches.

Table 3: Spectrum (secondary) Trading, percentage of country responses, 2012



Source : ITU World Telecommunication/ICT Regulatory Database

3.4 A market-based approach for assignment of spectrum

In an effort to speed up spectrum decision-making and ensure that spectrum is put to its most efficient and highest-valued use, policy makers and regulators have begun to develop market-based policies to supplement or even supplant slow, bureaucratic processes. Such approaches, which include market-oriented and flexible-use policies are increasingly viewed as an important means to promote convergence and increase broadband diffusion.

A recently released ITU report addresses market-based spectrum management policies and identifies a framework based on market-oriented and flexible-use policies as an important means to promote convergence and broadband diffusion.[36] In designing auction and tender rules for IMT spectrum, for example, the report recognizes that regulators can achieve various public policy goals such as enhancing coverage, and providing service to rural areas, as well as generating revenues for the government. However, the latter should not result in the creation of

barriers for spectrum assignment via excessive pricing. The report also notes some best practices for market-based and flexible-use spectrum management, as summarized in **Error! Reference source not found.**.

Box 4: Best practices for market-based and flexible-use spectrum management

- Adopt auctions as the mechanism to award spectrum use rights for commercial mobile services and set out transparent rules for the award and licensing process, including a clear understanding of what rights and obligations winners will be subject to (e.g. coverage obligations).
- Auction a wide range of frequency bands, in both higher and lower bands (i.e. above and below 1 GHz) since higher bands tend to be suited more for urban areas, while lower bands allow for more efficient coverage of rural areas.
- Initiate and complete spectrum auctions as quickly as possible, with the potential of conducting multi-band auctions, in order to allow license winners to speed up the deployment of mobile services, particularly mobile broadband.
- Ensure that new and existing spectrum licenses are technology - and service-neutral by setting minimal technical usage conditions on licenses, and consider adopting rules for unlicensed use and/or expanding spectrum available for unlicensed use.

Source: ITU, "Regulatory Impact of Convergence and Broadband for the Americas". Connect Americas Summit, Final Draft, 2012

Flexible-use policies include technology neutrality—which allows an operator to use any technology (or wireless standard) to provide a given service. This allows the operators to evolve and adapt their networks using the latest technology to best meet their customers' needs (i.e., the market helps drive technology choices). Overly prescriptive requirements that mandate the use of a particular technology in a particular spectrum band are increasingly seen as harmful to innovation and stifling increases in efficiency.

A growing number of regulators are introducing market-based mechanisms such as in-band migration, spectrum sharing and spectrum trading to distribute spectrum in an effort to meet the demand for fresh spectrum both for 3G and 4G services quickly and efficiently.[37] A substantial number of regulators, however, still rely heavily on administrative assignment and beauty contests to award spectrum licenses. In the African continent this approach is quite common. Uganda, for example, has made several bands available for mobile services using a first come - first served approach. It did not conduct an auction, even though auctions are allowed, because policymakers felt that an auction was unnecessary in the circumstances. In South Africa, ICASA created a hybrid assignment system involving a first stage "beauty contest" to pre-qualify bidders. But the regulator had some difficulty designing an auction system and finding a qualified auctioneer to run it. Cameroon, Ghana, and Nigeria are looking to develop "4G" service provision through turnkey arrangements with operators.

With respect to spectrum used for commercial purposes, the last two decades have seen many countries move from a prescriptive form of spectrum management to greater reliance on market forces and a lighter form of regulation of industry.[38] This has occurred for example in the United States, Canada, Europe, Australia, New Zealand etc. Market-based mechanisms include auctions, public tenders, and subsequent trading of licenses after award. Currently, nearly one half of countries worldwide use auctions as a primary way of assigning spectrum for the most popular mobile broadband services.[39]

In the United States, which has been using auctions for more than a decade, a major new element of policy is the (eventual) use of voluntary "incentive auctions"[40] for which the FCC now has legislated authority. This type of auction is intended to facilitate the movement of spectrum currently dedicated to one commercial purpose (such as TV broadcasting) to another, higher-valued use (e.g., mobile broadband).

An essential part of an auction process is a well consulted and comprehensive auction manual, which provides transparency to potential bidders. The manual also provides the vehicle for clearly explaining government objectives such as competition expectations, or spectrum caps, rollout obligations, or requirements, including infrastruc-infrastructure sharing.

Canada provides a typical example of a spectrum policy framework built around these concepts.[41] Canada will generally apply an auction mechanism when demand for spectrum is expected to exceed the available supply and government policy objectives can be met fully through use of an auction. An auction will generally not be used in bands designated for priority service (such as where systems are vital to national sovereignty and defence, law enforcement, public safety and emergency services).

Auction licensees are usually given the maximum flexibility to adapt to changing consumer demands, and the technologies they may offer. Spectrum policies are also pro-competitive, following two guiding principles :

- restricting market participation, based on existing market power and potential anti-competitive effects, and
- spectrum aggregation limits, again based on competition concerns.

New Zealand has also been a leader in moving its commercial spectrum management approach from its historical administrative assignment process under the radio licence regime to the management rights regime. The central guiding document summarizing policy in New Zealand,[42] whilst dated 2005, was somewhat prescient in the opportunities and tensions foreseen in commercial mobile and broadcasting technology developments in the future. The document contained observations on convergence, and the potential need for a comprehensive audit (equivalent to the inventory concept introduced earlier) to identify inefficient utilization to resolve a perceived shortage of commercial spectrum, and for achieving social and cultural objectives. As these examples show, a market-based approach is a common, even necessary element of a National Spectrum Policy. In practice this would comprise a combination of techniques involving administrative allocation methods, market-oriented assignment methods, and license-free operation in proportions which reflect national needs and priorities. Table 4 provides some insight into the popularity of the various techniques used to achieve public policy goals in a recent study of the Americas.[43]

Table 4: Various spectrum management techniques from the Americas

SPECTRUM MANAGEMENT TECHNIQUES	COUNTRIES
Specific coverage obligations	Colombia, Chile, Brazil, Costa Rica, Peru
Use of spectrum caps	Argentina, Brazil, Chile, Colombia, Mexico, Peru
Spectrum trading rights	USA, Mexico, Chile, Uruguay
Flexible use spectrum policies	Argentina, Brazil, Chile, Colombia, Peru, Uruguay, USA, Venezuela
Development of incentive auctions	USA
Development of "Unlicensed" or "license-exempt" rules	USA, Canada, Brazil, Argentina, Chile, Colombia, Costa Rica, Panama, Paraguay, Uruguay, Venezuela.

Source: Regulatory Impact of Convergence and Broadband for the Americas". Connect Americas Summit, July 2012, ITU

The role of economics: efficient management of spectrum

As policy-makers and regulators seek to balance competing interests, it will be important to clearly indicate how the different uses of spectrum will be evaluated in the context of larger national communications and economic goals. Many governments are turning to market-based valuation methods to help them manage spectrum more efficiently.

The terms "highest value use" and "total welfare standard" have gained traction in economic evaluation of spectrum. However, whilst conceptually straightforward, this is a very difficult issue. A problem lies in establishing "value" on a comparable basis in a diverse user environment. Spectrum that will be used purely for commercial activity is relatively straightforward; comparisons can be made to past auctions, for example. The question often asked, though, is whether and how value should be ascribed to safety of life services, or the use of spectrum for scientific pursuit, or for experimentation with new technology, or the use of spectrum in defence of a country, etc.

With regard to repurposing spectrum, the United Kingdom has employed Administrative Incentive Pricing (AIP) for commercial and government spectrum to signal market value to spectrum users so that they have the incentive to ensure optimal use of their spectrum.[44] This approach has had its intended impact on government spectrum holders – the military in particular. Here, spectrum costs are now included in business cases for major programs, long term spectrum need plans are developed, and some unneeded spectrum has been transferred to other uses.

Significant effort has been expended to develop an economic estimation of the value of spectrum, and this still remains the most viable approach for commercial applications of spectrum pricing and marketing. An economic base of thought also provides the best starting point for comparable valuation of non-commercial applications of spectrum. It is extremely unlikely, for example, that any other methodology other than market forces (or a proxy such as AIP) will be used to distribute 3G and 4G spectrum, at least in countries where spectrum access is constrained and the marketing processes allow contemporary auction techniques for doing this.

However, as indicated in an ITU report on valuation of the spectrum, there are still no easy answers for comparing values among spectrum bands that continue to be used by different kinds of (commercial and non-commercial) users.[45]

It is suggested that a broader perspective may need to be taken into consideration for evaluating the social value of spectrum – the value of spectrum used for non-profit-making enterprises such as weather prediction, scientific inquiry, emergency responses or national defence. Proxies may, however, exist indirectly, for instance in unlicensed bands through observing input costs to service development.

In general, governments have no mechanism (other than general taxation) to "charge" citizens for spectrum used in the interests of the common good. Until this disconnect is resolved, spectrum value will continue to have multiple meanings - one for making money, and one for making policy.

Despite this, some progress is being made. In the United Kingdom, the use of AIP by Ofcom may widen to applications beyond Defence. Tools involve a gradual introduction of taxation, coupled with starting points assisted where possible by intrinsic and extrinsic factor analysis, and using the concepts of opportunity costs and marginal costs where feasible. Moreover, current work by Marcus[46] and Marks[47] addresses the different forms of efficiency and metrics in the use of spectrum. This is part of a European spectrum inventory exercise, and should lead on to better solutions for comparing dissimilar users.

According to the studies, the different forms of efficiency involve:

- technical efficiency
- economic efficiency, and
- social efficiency

No single metric can fully capture efficiency (in the use of spectrum) in any of these dimensions, and an efficiency metric must be understood in the context of the application for which it was designed.

The EC vision is that data on economic and social values will be evaluated for all bands (in the range 400MHz to 6GHz) using metrics for economic *and* social efficiency. In this way, bands under significant pressure will be identified and policy options proposed to improve spectrum efficiency.

Marks points out that there are no precedents for the metrics approach envisaged and data may be incomplete. However, she expects indications of opportunities for significant improvement in the efficiency of use resulting from the analysis undertaken, and this should assist regulators with the difficult exercise of meeting demand for spectrum.

3.5 A strategy of international and regional engagement

The enormous changes occurring in mobile broadband and the accompanying evolution of spectrum policy are international in scope. It is therefore critical to have a strategy of engagement in regional and international considerations to the greatest extent possible.

At the international level, the ITU provides a common venue where all Member States can participate in the work of allocating spectrum for new uses and developing standards and plans that maximize the harmonized use of the spectrum resource. As the top level of the spectrum allocation process, the ITU thus plays a critical role in promoting harmonization among the regions of the world—ensuring that services can coexist with each other, while minimizing interference.

The work of the ITU-R sets much of the stage for international harmonization and collective guidance on regulatory and technical matters, ranging from the WRCs to the Working Parties within individual Study Groups that pursue the technical basis for the evolving wireless world - both terrestrial and satellite. The ITU has been particularly active in addressing mobile broadband issues. More information on ITU-R IMT mobile broadband studies is given in Box 6.[48] The ability to efficiently accommodate demand for spectrum and contain interference to acceptable levels depends critically on these studies, which were set in motion by WRC-12. The ensuing ITU-R Reports and Recommendations will form an essential basis for the development of national regulations.

Box 5: IMT work plans in ITU-R resulting from WRC12 decisions

Many of the spectrum regulatory tools and techniques (such as sharing criteria, antenna technology advances, software defined and cognitive radio, radio network architectures), to efficiently accommodate new technology and service advances will be studied in ITU-R Study Groups during the next 4 years, culminating in inputs to the ITU World Radiocommunication Conference to be held in 2015 (WRC-15). At WRC-15, new spectrum allocations will be considered with a view to incorporating agreements into the Radio Regulations (which have treaty status), and attendant Resolutions and Recommendations. Back-to-back with this will be the Radiocommunications Assembly (RA-15) which deals with non-treaty technical matters from Study Groups, and which may produce technical output documents of a voluntary nature. Some of these considerations may flow into WRC-15.

In association with these meetings is the Conference Preparatory Meeting (CPM) which meets twice between each WRC. CPM-15 first met immediately following WRC-12 and amongst other things organized the detail and timing of the work activity of the ITU-R Study Groups with regard to WRC-15 Agenda Items. The second meeting of CPM-15 will meet approximately 7 months ahead of WRC-15 in order to evaluate and catalogue the alternative solutions (or methods) to satisfying each agenda item. These alternatives come from the Study Groups, and are then presented to the WRC for its consideration.

WRC-12 (and the following CPM-15) was instrumental in setting up an additional and important activity on "IMT-Advanced" through a Joint Task Group (JTG4-5-6-7) which will progress its work on identifying spectrum for broadband applications and sharing studies towards the next CPM-15 Meeting.

JTG 4-5-6-7 is important because it captures much of the intersecting interest (and conflict) in the spectrum needs of the bourgeoning terrestrial mobile broadband sector and the existing services. The elements for study by the JTG are contained under Agenda Items 1.1 (see Section 2.2 earlier) and accompanying Item 1.2 for WRC-15, which are explained in an ITU-R Circular Letter.

The IMT studies to be conducted before WRC-15 should assist regulators in identifying the spectral efficiencies (and hence the actual spectrum needed) that should be expected as a result of advances in modulation techniques, antenna designs, offloading between different radio networks, coding efficiencies etc. These studies will also indicate potential candidate bands that may be used for the next generation of broadband services.

Source : ITU.

Engagement at the regional level is also critical for ensuring that spectrum is most efficiently utilized. Regional organizations are important venues for developing policies that will promote harmonization among neighboring countries. In addition, regional preparations for the WRC and RA Meetings provide a convenient way for many countries to stay abreast of developments in efficient use of spectrum. A series of preparatory meetings hosted by regional bodies also allows neighboring countries the opportunity to dialogue on border issues and to share similar experiences and promote harmonization. These opportunities also create a context for the ongoing refreshment of the National Spectrum Plan and associated forecasts.

Border coordination between individual countries addresses geographic overlaps and potential interference scenarios. Agreed signal/power levels need to be coordinated. These levels should reflect ITU-R outputs, which represent an agreed international technical basis and which can be drawn on during negotiations.

Further development of national policies and regulatory solutions that encompass the broad social, economic and technical considerations are benefitting from regional cooperation. The significance of this work has been pointed out from within Europe in pathfinding efforts there.

Box 6: Wireless Broadband Master Plan Pilot Project

A recent ITU presentation points out a key assumption that shared wireless access permits lowering of the costs of access in an easier way than fixed networks. Upgrades to WBB are also simpler, and consumers can buy services on an incremental (often pre-paid) basis. The presentation also stated that it is unlikely that for many emerging markets there will ever be fixed network deployment at a level comparable to developed countries. The WBB Master Plans are intended to address these issues and provide guidance.

Based on a survey of the circumstances in 18 countries in the Asia Pacific, four countries were chosen for a WBB Master Plan pilot project: Myanmar, Nepal, Samoa, and Vietnam. Important observations have been made based on the pilot projects (see Reference 30). The goals of affordable universal WBB services that address the "digital divide" in emerging countries, and the effective use of regulatory tools to achieve a key policy objective, will be met if:

- competition and market structure is optimised ahead of revenue raising;
- ample spectrum is made available and its use is flexible;
- technology innovations are able to be deployed;
- infrastructure is not duplicated and there is service competition on that infrastructure;
- prices (if regulated) should take into account the market and changes driving that market; and
- universal service schemes are efficiently delivered and well targeted.

Source: Sameer Sharma. ITU Regional Office for Asia and the Pacific, International Training Program. "Wireless Broadband Master Plan : Introduction, Survey Results and Outcomes". 2-4 April 2012, Hyderabad, India.

Pathfinding efforts are not restricted to developed countries. Solutions are also being developed to meet the specific circumstances of developing countries. Under the joint partnership of the ITU and the Korean Communication Commission, for example, the *Wireless Broadband Master Plan* project was launched in Q2 2011 (see Box 7). The aim is to assist selected developing countries in the Asia Pacific region to develop their own wireless broadband master plan in order to provide for broadband supported services and applications that are affordable and comparable to those in developed countries. In essence, the goal is to address the "digital divide" by utilizing wireless broadband (WBB) technologies.

On a broader harmonization front, the GSMA has released a report on the importance of harmonized allocation of spectrum on a regional basis in the 700 MHz bands a result of the digital dividend.[49] The report estimates that the adoption of harmonized spectrum for mobile broadband in the Asia-Pacific region could generate up to US$1 trillion in GDP growth between 2014 and 2020. The GSMA reports that Japan and Papua New Guinea are likely to be the first countries to hold spectrum auctions in the band, while Australia and New Zealand are expected to be the next batch of countries to open the spectrum to mobile operators. Within the Asia-Pacific region, most countries have heeded the harmonization lesson, and only Malaysia and China remain currently undecided on the 700 MHz band.

The consequences of a non-harmonized approach can be significant. The United Kingdom and Spain, for example, were early movers in digitizing their broadcast services in order to free up 800 MHz digital dividend spectrum. This was accomplished in advance of regional harmonization. Both countries were subsequently faced with the need to redeploy some channels so as to harmonize with the rest of Europe. In the United Kingdom, this resulted in up to 350million pounds in redeployment and interference mitigation costs.

4. Conclusions

The first section of this paper set the scene for an assessment of spectrum policy making and regulation in an environment in which there is increased pressure on the scarce resource of spectrum, arising especially from the need to service mobile broadband and the phenomenal increase in data traffic expected in the future. The greater inclusiveness of spectrum management in broader industry and economic activity, including being an integral part of national broadband planning means that the modern spectrum regulator needs to be more broadly aware of the industry and market atmosphere and developing issues which are outlined in the section 1. This leads to the notion of the "third generation regulator".

Spectrum policy has high-level principles that are durable in nature. Section 2 summarizes these principles as :

- Facilitate broadband deployment.
- Promote transparency.
- Ensure technology neutrality.
- Apply flexible use measures.
- Ensure affordability.
- Make spectrum available on a timely basis.
- Manage spectrum efficiently.
- Level the competitive playing field.
- Harmonize (International and Regional) policies.
- Take a comprehensive approach to promoting broadband access

More dynamic change with time is associated with implementation of these principles. This leads to contemporary best practice, the elements of which include:

- wider recognition, visibility and accountability of the spectrum function;
- a taxonomy of spectrum needs;
- a National Spectrum Plan and rolling annual consultation;
- a Marketing Program for allocation of spectrum; and
- a strategy of international and regional engagement.

Best practice is expressed in implementation of stable high-level principles, and is demonstrated through pathfinding examples that are embedded within this report.

Regarding whether National Spectrum Policy measures up to best practice, this can be evaluated with a series of considerations or tests. For example, do the initiatives –

- Encourage regional and international harmonization of spectrum?
- Promote efficient use of spectrum?
- Balance public and commercial interests?
- Promote greater competition?
- Provide flexibility in use of spectrum for different users and needs?
- Encourage and reward use of new and efficient technologies?
- Utilize the latest spectrum management principles?
- Demonstrate international cooperation?

REFERENCES

1. 4G Americas : White Paper "New Wireless Broadband Applications and Devices: Understanding the Impact on Networks". May 2012.
2. The World in 2011. ITU ICT Facts and Figures.
3. Gary Schwartz. "the Impulse Economy : Understanding Mobile Shoppers and What Makes Them". Atria Books. October 2011.
4. Cisco : VNI Mobile Forecast Highlights, 2011 – 2016. www.cisco.com/web/solutions/sp/vni/vni_mobile_forecast_highlights/index.html.
5. Guillermo Escofet, Informa Telecoms & Media. "Mobile Content and Applications Report". May 15 2012.
6. Tellabs Study. "Mobile Operators Profitability Challenged within Three Years". Feb 2011. http://www.tellabs.com/news/2011/index.cfm/nr/142.cfm
7. Google/Ipsos. "Our Mobile Planet : Understanding the Mobile Consumer". May 2012. www.thinkwithgoogle.com/insights/tools/our-mobile-planet-tool.
8. ict regulation toolkit. ITU infoDev. Module 2 : "Competition and Price Regulation". www.ictregulationtoolkit.org
9. Administrative Circular CA/201. ITU Radiocommunication Bureau. 19 March 2012. "Results of the first session of the Conference Preparatory Meeting for WRC-15 (CPM-1).
10. GSR11 "Best Practice Guidelines on Regulatory Approaches to Advance the Deployment of Broadband, Encourage Innovation and Enable Digital Inclusion for All". Colombia October 2011.
11. GSR5 "Best Practice Guidelines for Spectrum Management to Promote Broadband Access". Yasmine Hammanet, Tunisia. November 2005. See also http://www.itu.int/ITU-D/treg/Events/Seminars/2003/GSR/WSIS-Statement.html for broader ramifications.
12. Spectrum Policy in the Age of Broadband :Issues for Congress. Linda K. Moore, Congressional Research Service. 21 June 2012.
13. FCC National Broadband Plan, Chapter 5: Spectrum. March 2010 http://www.broadband.gov/download-plan/
14. Presidential Memorandum, USA, June 2010. "Unleashing the Wireless Broadband Revolution". http://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution
15. U.S.Department of Commerce. March 2012. "An Assessment of the Viability of Accommodating Wireless Broadband in the 1755 – 1850 MHz Band" http://www.ntia.doc.gov/files/ntia/publications/ntia_1755_1850_mhz_report_march2012.pdf.
16. FCC Order on unlicensed operation in the broadcast TV bands. November 2008. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-260A1.pdf
17. John Alden, Freedom Technologies. Report to ITU-D, April 2012. "Exploring the value and economic valuation of spectrum". www.itu.int/broadband.
18. World Bank InfoDev Report. November 2003. "The Wireless Internet Opportunity for Developing Countries". www.infodev.org/en/Publications.24.html
19. Five Year Spectrum Outlook 2012-2016 : *The ACMA's spectrum demand analysis and strategic direction for the next five years.* Australia 2012. www.acma.gov.au
20. Australian Government. "Convergence Review : Final Report". March 2012. www.dbcde.gov.au
21. ACMA. "Broken Concepts : *The Australian communications legislative landscape*" August 2011 and "Enduring Concepts : *Communications and media in Australia*" November 2011. www.acma.gov.au
22. European Commission Workshop. "Inventory and review of spectrum use : Assessment of the EU potential for improving spectrum efficiency". Brussels, May 2012.

23. J.Scott Marcus, WIK Consult-GmbH. "Inventory review of spectrum use : Preliminary Findings". Ibid.
24. Philippa Marks, Plum Consulting Ltd. "Inventory review of spectrum use : Evaluating the Economic and Social Efficiency of Spectrum Use". Ibid.
25. Lena Liman, Swedish Post and Telecom Authority. "Spectrum strategy work in Sweden". Ibid.
26. Government of Canada. "SPFC – Spectrum Policy Framework for Canada". June 2007. www.ic.gc.ca/spectrum
27. Red Mobile/PA Consulting, 2012. "Study of Future Demand for Radio Spectrum in Canada 2011-2015. www.ic.gc.ca/spectrum
28. ict regulation toolkit. ITU infoDev. Module 5 : "Radio Spectrum Management". www.ictregulationtoolkit.org
29. Sameer Sharma. ITU Regional Office for Asia and the Pacific, International Training Program. "Wireless Broadband Master Plan : Introduction, Survey Results and Outcomes". 2-4 April 2012, Hyderabad, India.
30. Scott Minehane. Ibid. "Wireless Broadband Master Plan – II".
31. Ministry of Economic Development, New Zealand. "Review of Radio Spectrum Policy in New Zealand". 2005.
32. Marianne Treschow. "Spectrum Policy in Sweden". Private communication.
33. KCC Annual Report. March 2011. See http://eng.kcc.go.kr
34. KCC Plan for 2011.
35. Ofcom "Spectrum Review Framework : A consultation on Ofcom's views as to how radio spectrum should be managed". November 2004. http://stakeholders.ofcom.org.uk/consultations/sfr
36. Ofcom "SRSP: The revised Framework for Spectrum Pricing: Our policy and practice of setting AIP spectrum fees". December 2010. http://stakeholders.ofcom.org.uk/spectrum/spectrum-pricing/
37. Ofcom "Appendix A (to SRSP consultation document): Our current practice in setting AIP fees". Ibid. March 2010.
38. Regulatory Impact of Convergence and Broadband for the Americas". Connect Americas Summit, July 2012. ITU.
39. Main Characteristics of a National Spectrum Policy. Mercy Wanjau, Kenya Communications Commission. Private Communication.

[1] The paper was edited by David Wye, TMG.

[2] See Reference 7.

[3] Trends in Telecommunications Reform 2012. ITU-D.

[4] www.pyr.com. June 2012.

[5] http://www.ericsson.com/au/res/region_RASO/docs/2010/ericsson_50_billion_paper.pdf

[6] See Reference 1.

[7] See Reference 2 and www.http://www.itu.int//ITU-D/ict/statistics/index.html

[8] See Reference 4.

[9] See Reference 6.

[10] See pbc@budde.com.au Newsletter 31/7/2012.

[11] An important source of regulatory advice comes from the ITU's *Telecommunications Regulation Handbook,* which is divided into several modules. Module 2 (Competition and Pricing – Reference 8) was significantly re-written in 2011 and this section summarises some of the new lessons. Module 5 is also important.

[12] These attempts include considerations in GSR05 of best practice guidelines, the ITU Handbook of Spectrum Management, Module 5 of the ITU infoDev ICT Regulation Toolkit,and the work of ITU-R Study Groups (see for instance current work in ITU-R SG1 WP1B, Temp Docs 3, 5 and 6).

[13] When they were last examined in detail within the GSR community.

[14] See Reference 11.

[15] See Reference 10.

[16] See the GSR11 Best Practice Guidelines on regulatory approaches to advance the deployment of broadband, encourage innovation and enable digital inclusion for all, www.itu.int/bestpractices

[17] Rate of return (regulation)

[18] See Reference 13.

[19] See Reference 14.

[20] The NTIA administers federal government- used spectrum, whilst the FCC has responsibility for commercial and other uses.

[21] See Reference 15.

[22] ITU ICT Eye : http://www.itu.int/icteye

[23] ACMA is the Australian Communications and Media Authority

[24] See Reference 22.

[25] EFIS(ECO Frequency Information System) is the tool to provide harmonised availability of information regarding spectrum use in Europe. 42 CEPT countries are represented in EFIS.

[26] See Reference 26.

[27] See Reference 25.

[28] See Reference 12.

[29] See also ITU Trends 2008.

[30] See Reference 16.

[31] See Reference 20.

[32] See Reference 21.

[33] As at the time of writing the USD and AUD were almost on a par.

[34] See Reference 18.

[35] Spectrum (secondary) Trading. ITU ICT Eye : http://www.itu.int/icteye

[36] See Reference 38.

[37] As presented in ITU Trends 2012.

[38] See http://www.itu.int/itu-D/treg/publications/bbreports.html

[39] ITU Telecommunication/ICT Regulatory Database, www.itu.int/icteye

[40] These involve compensation to an incumbent for relocation or displacement in order to allow higher value use of the spectrum.

[41] See Reference 26.

[42] See Reference 31.

[43] See Reference 38.

[44] See http://www.itu.int/itu-D/treg/publications/bbreports.html

[45] See Reference 17.

[46] See Reference 23.

[47] See Reference 24.

[48] http://www.itu.int/ITU-R/index.asp?category=information&rlink=rhome&lang=en

[49] www.mobilebusinessbriefing.com/articles/apac-spectrum

INTERNATIONAL TELECOMMUNICATION UNION

GSR 2012 Discussion Paper

International Mobile Roaming Services: A Review of Best Practice Policies

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 19 October.

TABLE OF CONTENTS

1 INTERNATIONAL MOBILE ROAMING SERVICES: A REVIEW OF BEST PRACTICE POLICIES

Author: Dimitri Ypsilanti, Senior ICT Expert

1. Introduction

This paper provides a review of policy and regulatory initiatives taken to reduce the costs to users of international mobile roaming services (IMRS). It builds on the ITU's earlier work, in particular the 2008 Global Symposium for Regulators discussion paper[1], recommendations from ITU-T and analysis by the Organisation for Co-operation and Development (OECD) on this issue in addition to regional initiatives, such as by the European Union, the African Union and the Arab Regulators Network. The aim of the paper is to suggest best practice solutions to ensure that in the long term sustainable competition will reduce IMRS prices.

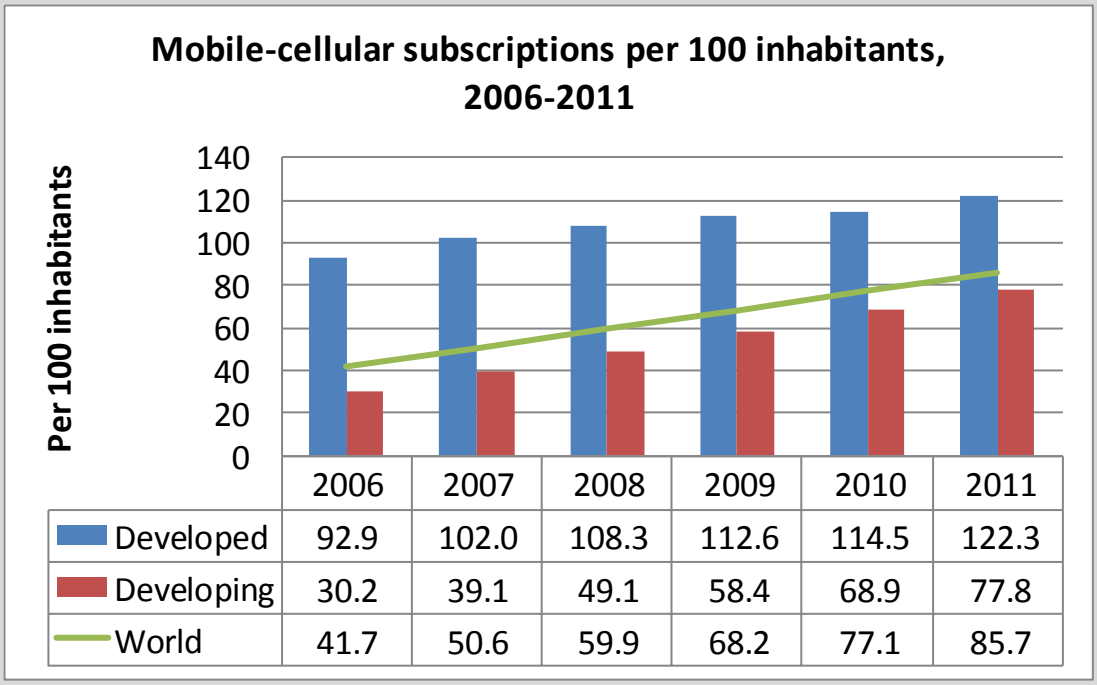
1.1 Mobile devices are becoming the main tool for communications

The high prices charged for international mobile roaming services have emerged in recent years as an important telecommunication policy and regulatory issue. Across the OECD countries it has been estimated that roaming prices on bilateral routes vary up to eight times (i.e. the cost of the same service for subscribers visiting each other's country and calling home) and up to 20 times more expensive for an international roamer to make a call home than for a local mobile user, in that country, to make an international call to the roamer's home country.[2] The European Union has estimated that retail roaming prices are, on average 118% higher than the estimated underlying costs.[3]

Finding solutions to high mobile roaming prices has also been difficult to resolve for a number of reasons. First, users in a country usually choose their service provider on the basis of the best prepaid offer or post-paid monthly mobile subscription package available for their particular consumption requirements - international mobile roaming charges are not normally advertised as part of this package although they are included in this package. Second, even if users are aware of the prices charged by mobile service providers for international roaming (and they are usually not), roaming is not a major consideration for them since in volume terms domestic calling, messaging and domestic mobile broadband access constitute the bulk of their mobile activity. Most users only become aware of international mobile roaming prices when travelling internationally. Third, when travelling, a mobile user cannot usually choose his/her international roaming service provider - they have to rely on their national provider. Finally, authorities from the country of origin of international travellers have no authority to control and regulate the wholesale prices set for international mobile roaming in a visited country.

While the issue of high IMR prices is not new, it has taken on increased importance in the last few years. A major reason for this has been the increasingly important role played by mobile services in economic and social transactions resulting from the significant growth in mobile subscriptions in developed and developing countries over the last decade. Recent ITU data show significant growth in mobile subscriptions (Figure 1) in particular in developing economies. In addition, significant technological change is shifting subscribers from 2G to 3G mobile technologies in some markets and from 3G to 4G in other markets. A key part of these changes is the increasing use of smartphones by subscribers and the shift to data communications.[4] Figure 2 shows the rapid development of mobile broadband subscriptions at the global level.

Figure 1: Mobile subscriptions per 100 inhabitants (2007-2011)

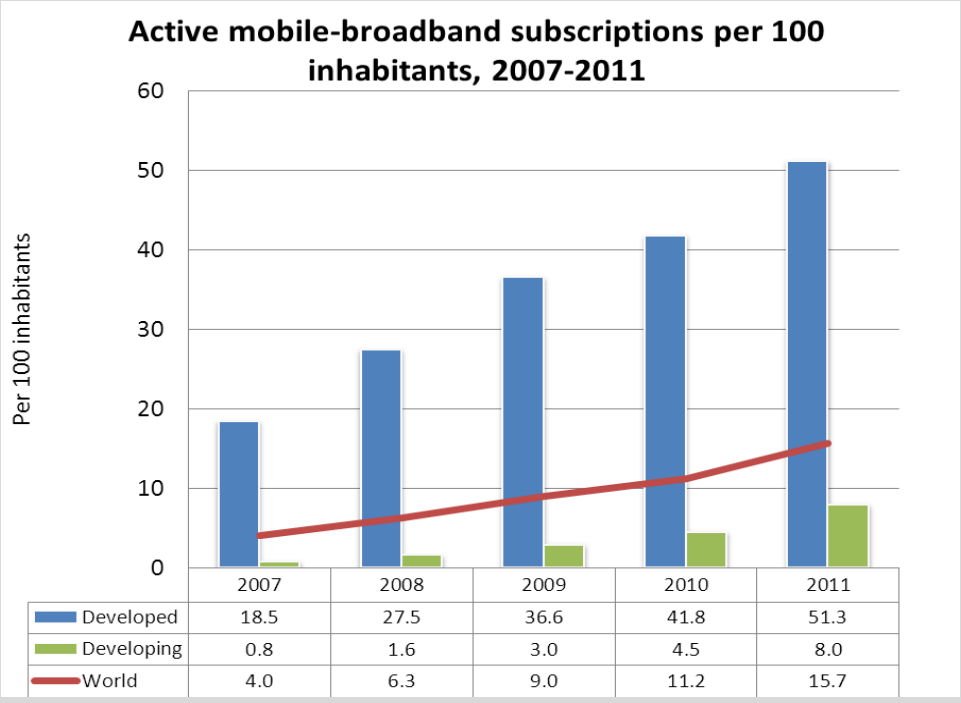


	2006	2007	2008	2009	2010	2011
Developed	92.9	102.0	108.3	112.6	114.5	122.3
Developing	30.2	39.1	49.1	58.4	68.9	77.8
World	41.7	50.6	59.9	68.2	77.1	85.7

Note: The developed/developing country classifications are based on the UN M49, see: http://www.itu.int/ITU-D/ict/definitions/regions/index.html

Source: ITU World Telecommunication /ICT Indicators database

Figure 2 : Mobile broadband subscriptions per 100 inhabitants (2007-2011)



	2007	2008	2009	2010	2011
Developed	18.5	27.5	36.6	41.8	51.3
Developing	0.8	1.6	3.0	4.5	8.0
World	4.0	6.3	9.0	11.2	15.7

Note: The developed/developing country classifications are based on the UN M49, see: http://www.itu.int/ITU-D/ict/definitions/regions/index.html

Source: ITU World Telecommunication /ICT Indicators database

The development and rapid global diffusion of the Internet and related applications and services has transformed business practices in economies and changed the communications behaviour of users, both business and consumers. This transformation has increased innovation and improved productivity in many industry sectors, created new economic activities and expanded market reach of many firms, in particular small and medium enterprises. This transformation has led to the rapid growth of data communication which can be expected to expand significantly as broadband networks increase capacity through fibre to the home technologies, as new technologies such as cloud computing become more commonplace and as the range of applications widens.

Smartphones, and the related development of services and applications for these phones have significantly expanded the use of mobile data communications in national markets and mobile data services are increasingly being used by subscribers when roaming internationally. The demand for mobile Internet access is expected to continue to expand rapidly as smartphones continue to diffuse and other terminals, such as tablets, and portable computers become more commonplace.[5] Mobile voice communications is being overtaken at national and international levels by the use of SMS, data access, access to emails using mobile phones and the use of a wide range of mobile applications. Many of these applications update automatically, require location data, etc., and in so doing generate more mobile data traffic. Subscribers also use their mobile terminals to access social applications and are storing personal content on cloud applications.

As these applications become commonplace, their use is expanding to international travellers increasing the demand for international roaming services. The expected shift to mobile payment services, use of mobile applications for airline tickets/boarding passes and other near field applications will also generate domestic as well as international traffic. At the same time a number of new data applications have developed for international users (maps, translation information, tourism information, location services, etc.). Mobile operators, faced with declining average revenue per user in mobile voice markets, as a result of competition in domestic markets and as users are migrating from using voice services to other messaging applications, are placing emphasis on developing new applications and services. Subscribers who use these new applications and services on a daily basis in their home country tend to continue to do so when travelling.

In many cases the use of these mobile services and applications by users travelling internationally has led to situations of "bill shock" because of insufficient knowledge by users on prices and billing practices.[6] This has resulted in media and political pressure to tackle the problem of high international mobile roaming prices.

Almost all countries now have more mobile than fixed subscribers. In many economies there has been a trend in the reduction of fixed lines with users (including families) relying only on mobile phones. In developing economies, where in the past connectivity was based on expanding fixed lines, this has changed with the emphasis now on mobile communications. These trends are likely to continue given, as indicated by ITU data, that access to mobile networks is now available to 90% of the world population and 80% of the population living in rural areas.[7] In short, the pressure to resolve the issue of high IMRS prices will increase.

An important mobile wireless growth area is machine-to-machine communication. This term includes devices that are connected to the Internet using a variety of fixed and wireless networks and communicate with each other.[8] *IMS Research* estimates that shipments of cellular modules for M2M will reach over 100 million by 2015.[9] A large number of these modules can be expected to be mobile across borders and hence could be subject to international roaming charges. Examples could include M2M devices used in the tracking of international cargo, in automobiles or trucks which cross borders, in consumer devices such as e-books or medical devices. Although the data traffic per device may be small, the eventual volume of devices which may cross-borders can result in high costs for business and act as a barrier to the development of new applications, services and productivity growth.

1.2 Growth in international travel

Separate, but concurrent with the explosive development of the Internet, mobile markets and ICT technologies in general, there has been a considerable expansion in worldwide trade and foreign direct investment as the global

economy has become more open.[10] Open markets have also led to a greater integration of national economies with the development of global supply chains.[11] In most continents regional integration is developing and there are numerous free trade arrangements that have merged either bilaterally or among several countries in a region. These developments have strengthened economic and social ties, have led to a higher intensity of business travel among these countries and growing tourist travel. According to some estimates business travel is responsible for one-third of the growth in world exports over the last decade.[12] Business travel has been one of the major factors behind the growth of international mobile roaming services.

The opening up of economies to foreign direct investment has also stimulated the development of tourist industries in those countries. Developing economies quickly recognised the beneficial impact of tourism for economic growth.[13] International tourism, according to the World Tourism Organisation generates USD 1.2 trillion equivalent to 30 percent of the world's exports of services.[14] Travellers want to have reliable and cheap communications with their home country and increasingly rely on mobile applications to assist them in their international business and in facilitating their tourism plans. As noted above new mobile applications, in many cases developed by the visited country, target tourists resulting in the increased use of mobile data services.

The development of a range of mobile applications for business, tourism, and eventually payments will be constrained if international mobile roaming prices remain high and the opportunities for visited countries to develop tourism services and for users (business and consumers) to take effective advantage of smart mobile phones will be limited. The problem of high international mobile roaming service prices is a global issue but the probable impacts will weigh more heavily on developing economies in that users from those countries are facing, relative to their incomes, higher international mobile rates.

2. The Regulatory Challenge in IMRS

Questions regarding high prices and lack of effective competition in IMRS markets are not new. The International Telecommunications Users Group raised this as an issue in 2000 and it was subsequently discussed at the ITU's Study Group 3.15 In 2002 the European Union recognised that the wholesale IMRS market could be susceptible to ex-ante regulations and should be reviewed by national regulatory authorities.16 17 These early efforts did little to resolve the issue. However, efforts to resolve the issue of high IMRS prices have accelerated in the last few years. These efforts have ranged from private sector initiatives taken by mobile service providers or other service providers using alternative calling technologies and by government/regulatory initiatives either through bilateral discussions, regional initiatives, efforts by international organisations (ITU, OECD, WTO), and unilateral efforts. Progress has been made. However, it has been slow and has focused to a large extent on pushing prices down through regulatory measures rather than finding ways to introduce longer term solutions which could result in effective competition in IMRS markets and reduce prices.

2.1 The regulatory challenge[18]

Wholesale charges

All mobile wireless operators charge a wholesale interconnection rate (mobile termination rate) at the domestic level. These charges are what other operators pay (fixed or mobile) for delivering a call to mobile wireless providers. In effect, the terminating operator has a monopoly on call termination for their subscribers since it controls access to the specific subscriber being called. Termination rates provide a significant source of revenue for mobile operators so that there is little incentive to reduce these rates which also implies that larger mobile operators benefit more from above-cost rates. This also implies that above-cost termination rates result in a subsidy by subscribers of one network at the expense of another network. The termination rates faced by call originating service providers impacts directly on the retail prices originating operators can charge and the flexibility they may have in structuring retail offers. There is also a strong correlation between the volume of outgoing minutes on mobile networks and the termination rate.[19]

The perception by telecommunication regulators that high domestic mobile termination rates negatively impact on competition, innovation and consumer welfare in mobile markets has led to increasing intervention in this market in order to set wholesale termination rates. Although a number of mobile service providers have argued that reducing revenues from interconnection charges would lead to higher prices in other parts of the mobile market (the so-called "water-bed effect"), there is no evidence that in a competitive market this has occurred.[20] On the contrary, in many countries where the mobile termination rate has declined to low levels operators have started to provide innovative pricing packages such as unlimited national, international calls, unlimited SMS and unlimited mobile Internet access.[21]

The mobile termination framework at the international level is similar to domestic frameworks with the exception that it is much harder to regulate. Mobile network operators (MNOs) in country *A* have to pay a wholesale mobile termination rate to an operator in country *B* in order to deliver a call to one of their customers visiting country *B*.

The MNOs in country *A* also have to pay an operator in country *B* if one of their customers in country *B* wishes to originate a call back to their home country or to a subscriber in country *B*. Table 1, taken from the ITU's 2008 GSR discussion paper on international mobile roaming[22] illustrates the main elements of IMRS cost structures. These cost elements are mobile origination, mobile/fixed termination, international transit and roaming specific costs. Other costs elements incurred by a customer who is roaming in another country are signalling and billing and transit. Of these cost elements the most important by far are mobile origination and termination charges. The OECD noted that the

"*...major contributor to high retail charges is the wholesale rates charged by foreign operators. Where information is available the wholesale rate makes up around three quarters of the retail rate. Wholesale roaming charges are frequently in excess of USD 2 to USD 3 per minute and sometimes are more than USD 4 per minute*."[23]

The Body of European Regulators of Electronic Communications (BEREC) in reviewing the performance of prices caps in the European Economic Area highlighted that "... a sizeable margin remains between the average wholesale and retail prices. While the difference between average non-group wholesale and off-net retail rates has narrowed in relative and absolute terms in the past year, it remains significant (with retail representing a 429% or €2.097 margin over the per minute wholesale rate in Q2 2010, and 428% or €1.539 in Q2 2011).[24]

The wholesale roaming rates, for GSM network, are determined by Inter-Operator Tariffs (IOTs) which provide a non-discriminatory tariff - known to all GSM Association (GSMA) members - and which provide the benchmark for negotiating wholesale rates. The final outcome may as a result of negotiations differ from the IOT level for a particular operator since it may take into account volume of traffic, and traffic balance. The wholesale rate determines to a large extent the retail rates the MNOs in country *A* charge their customers for international roaming. Roaming agreements follow a framework defined by the GSM Association, which provide standard terms for international roaming agreements (STIRA). These guidelines apply only to operators that have an operating licence (i.e. mobile network operators) and as a result can be members of the GSM Association (effectively this excludes mobile virtual network operators and Network Service Providers).[25] Indications are that this may change in the near future.

The regulator in country *A* may be in a position to regulate the margin imposed on international mobile wholesale rates but, in itself, this would be insufficient to bring about a significant reduction in IMRS prices. The wholesale prices in country *B* are clearly outside the scope of jurisdiction of the regulator in country *A*. In effect, just as in national mobile markets where the terminating operator has a monopoly on call termination for their subscribers since they control access to the specific subscriber being called, in international markets the service operator in country *B* controls access by country *A*'s subscriber when that subscriber roams in country *B*. Similar to national markets, the access market for the purposes of international mobile roaming is not contestable.[26]

National telecommunication regulators could regulate mobile origination charges that their national MNOs charge foreign MNOS and the termination charges faced by foreign MNOs, but to do so usually falls outside of their mandate to ensure that their citizens benefit from a competitive national telecommunication market. The only incentive that a national regulator in country *A* has to reduce the origination and termination charges its MNOs charge foreign MNOs is if this provides a benefit to its national citizens. This situation differs significantly from national roaming where regulators can set wholesale rates if necessary or, as India decided in 2012, to effectively abolish national roaming charges. Residents of country *A* only benefit from lower international roaming wholesale charges to service providers from country *B* if wholesale roaming charges to mobile service providers from country *A* are lowered in country *B*.[27]

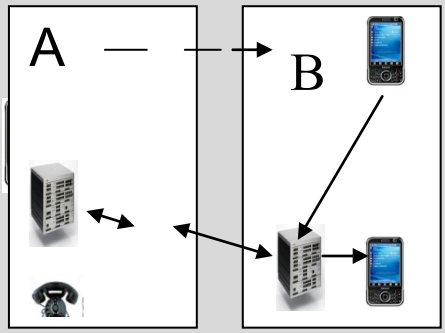
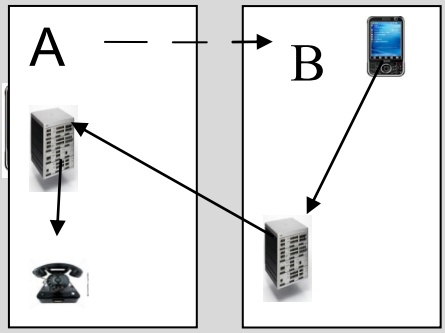
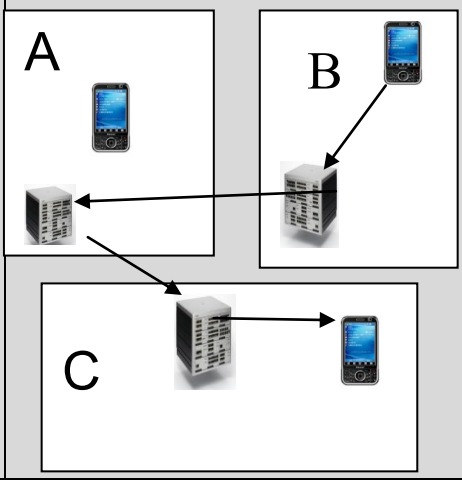
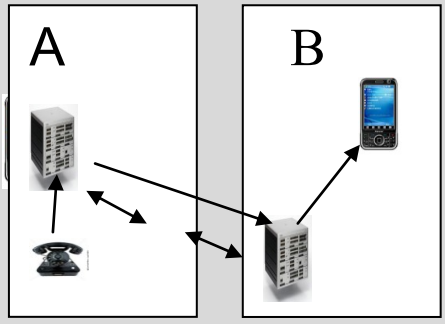
There is a question as to whether action should be taken only against wholesale rates and allow the lower rates to be reflected through the market on retail rates, or to take action on both wholesale and retail rates simultaneously. Taking action only against wholesale rates assumes that the market is working sufficiently well to pass on price reductions to end users. However, as noted above, there is very little competition at the retail level so that the incentive to pass on lower wholesale rates is probably quite low and even with some competition would probably take a much longer period to be reflected in retail charges. Taking action at both the wholesale and retail levels at least has the advantage of ensuring that consumers obtain benefits rapidly.

Retail charges

The telecommunication regulator of a country could determine that the retail rates for IMR paid by national subscribers are too high. A study undertaken for Australia found that the average roaming margins for Australian operators are approximately 3.2 times higher than domestic margins.[28] However, there is a limit on what actions can be taken. National operators could be required to reduce their retail rates, but the only part of these rates they have direct control over is the margin they are imposing on wholesale rates. Margins may be high and regulators may require that domestic service providers inform them of these margins. Reducing these margins may lead mobile service providers to try and obtain better wholesale rates from their counterparts in other countries although they have very little negotiation power.

Given that the main cost components which affects IMRS prices is the wholesale rate, the longer term solution is to find ways to reduce this rate while ensuring that reductions in wholesale rates are passed on to the retail market. Reviews of experiences in the European Union following the imposition of price caps is that prices declined to meet the requirements of price caps, but on average did not decline below the caps. If a regulatory initiative is taken which only imposes wholesale price regulation, it would seem necessary that retail prices should be monitored to determine whether they are reduced to reflect wholesale reductions. If retail prices remain sticky then it would be necessary to impose retail price regulation in addition to wholesale price regulation.

Table 1: Main international mobile roaming services and their cost structures

Call type	Cost elements	Illustration
Call inside a visited Country A traveller from country A goes to country B and makes a call to a subscriber of country B.	Mobile origination in country B + [National transit in country B] + Mobile termination in country B + Roaming-specific costs + Retail-specific costs	
Call from a visited country to the home country A traveller from country A goes to country B and makes a call back home to a subscriber in country B.	Mobile origination in country B + International transit + Mobile or fixed termination in country A + Roaming-specific costs + Retail-specific costs	
Calls from a visited country to a third country A traveller from country A goes to country B and makes a call to a subscriber in country C. Note that country C may or may not be in a region where international roaming prices are regulated.	Mobile origination in country B + International transit + Mobile or fixed termination in country A + Roaming-specific costs + Retail-specific costs	
Receiving a call in a visited country A traveller from country A goes to country B and receives a call from **either of the countries**	Mobile termination in county B + International transit + Roaming specific costs + Retail specific costs	

Source: Taken from "International Mobile Roaming Regulation - An Incentive for Cooperation", http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR08/discussion_papers/international_roaming_web.pdf

The regulator in country *A* may be in a position to regulate the margin imposed on the international mobile wholesale rates but, in itself, this would be insufficient to bring about a significant reduction in IMRS prices. The wholesale prices in country *B* are clearly outside the scope of jurisdiction of the regulator in country *A*. In effect, just as in national mobile markets where the terminating operator has a monopoly on call termination for their subscribers since they control access to the specific subscriber being called, in international markets the service operator in country *B* controls access by country *A*'s subscriber when that subscriber roams in country *B*. Similar to national markets, the access market for the purposes of international mobile roaming is not contestable.[29]

National regulators could regulate the mobile origination charges that their domestic MNOs charge foreign MNOS and the termination charges faced by foreign MNOs, but to do so falls outside of their mandate to ensure that their citizens benefit from a competitive national telecommunication market. The only incentive that a national regulator in country *A* has to reduce the origination and termination charges its MNOs charge foreign MNOs is if this provides a benefit to its national citizens. This situation differs significantly from national roaming where regulators can set wholesale rates if necessary or, as India decided in 2012, effectively abolish national roaming charges. Residents of country *A* only benefit from lower international roaming wholesale charges to service providers from country *B* if wholesale roaming charges to mobile service providers from country *A* are lowered in country *B*.[30]

There is a question as to whether action should be taken only against wholesale rates and allow the lower rates to be reflected through the market on retail rates, or to take action on both wholesale and retail rates simultaneously. Taking action only against wholesale rates assumes that the market is working sufficiently well to pass on price reductions to end users. However, as noted above, there is very little competition at the retail level so that the incentive to pass on lower wholesale rates is probably quite low and even with some competition would probably take a much longer period to be reflected in retail charges. Taking action at both the wholesale and retail levels at least has the advantage of ensuring that consumers obtain benefits rapidly.

2.2 Transparency

The level of wholesale charges is the key issue facing policy makers for IMRS charges, however the need to sensitise consumers and provide greater transparency is also important. While initiatives which increase transparency for consumers may only have a small and longer term impact on lowering IMRS rates they can help protect consumers from "bill shock" and may provide the information and incentive for users to try alternatives when roaming internationally. Consumers do not choose their service provider on the basis of international mobile roaming prices charged by these providers. They choose their service provider on the basis of a package of voice, messaging and data services and related prices i.e. the demand elasticity for subscriptions and call packages is considered much higher than for international mobile roaming. As argued by WIK " [a]*t current levels of usage demand elasticity, it is rational for MNOs to take high markups over the wholesale IOT for mobile voice roaming. The marketplace for mobile voice roaming is unlikely to organically correct itself under current conditions.*"[31]

Indeed, in most cases consumers are not aware of roaming prices when they enter into a contractual arrangement with a mobile service provider and, in some cases, depending on the country and service provider they need to specifically request international roaming as an option before travelling. Seldom are roaming prices made transparent to the consumer when subscribing to mobile services.

Regulatory initiatives which increase transparency for users are important in allowing users to better manage their usage of mobile roaming, understand the implications of roaming on their bills and can help reduce bill shock. However, it should not be expected that increasing transparency will, on its own, play a large role in significantly reducing prices faced by consumers when travelling.

A regulator in country *A* may have limited scope in reducing the wholesale mobile origination and termination charges set by foreign MNOs, but there is scope in facilitating alternate calling procedures in country *A*.[32] This could be through policies based on network neutrality, for example, ensuring that VoIP applications (sometimes referred

to as over the top providers), such as Skype, Fring, Viber, can be downloaded and used on mobile and other portable terminals. Policies on network neutrality can, in this context, complement policies on international mobile roaming.[33]

Providing information to consumers on alternate calling procedures for IMR can also help empower consumers. Providing this information is difficult in that each of the alternatives has positive as well as negative characteristics. The number of alternatives also change fairly rapidly, many are specific to roaming between two countries only and their prices may be quoted for the visited country only. It is, therefore, a difficult challenge to maintain a data base on these alternatives.

Interconnection has been viewed as a fundamental requirement in telecommunication markets in order to create conditions of competition. However, it has been recognised that, while necessary, interconnection on its own is not sufficient to create effective competition. What is important in order to compete is equal access, in other words interconnection should be available on the same terms and conditions for competing carriers as the providing carrier provides for its own services. The ability to provide services by a carrier to its customers should not be constrained by another carrier's control of facilities or supplementary services. This notion of interconnection on an equal access basis has become a fundamental tool for telecommunication regulators. However, in the context of international mobile roaming a telecommunication service provider needs to attain access to networks of operators in other countries on equal access terms. There is a fairly wide agreement among telecommunication regulators at the global level that national interconnection rates need to be regulated, at least until sufficient competition emerges in relevant markets. The same arguments should normally apply to international mobile interconnection (roaming) rates.

Taxation

Governments need to recognise that they are also responsible for higher IMRS retail prices through their tax policies. Some countries tax inbound and outbound roaming, some only tax outbound roaming while some do not tax inbound or outbound roaming. Taxation can increase prices significantly as the GSMA has noted in the case of Latin America.[34] The taxation of international telecommunication services are also covered by the International Telecommunication Regulations, namely section 6.1.3 which states: "*Where, in accordance with the national law of a country, a fiscal tax is levied on collection charges for international telecommunication services, this tax shall normally be collected only in respect of international services billed to customers in that country..*"[35] The OECD in examining IMRS prices noted that "*... it may be the case that in applying tax to the total bill many OECD countries are taxing the taxes applied in foreign countries through the wholesale rates charged to roamers*."[36]

2.3 Empowering and protecting consumers

Consumers have benefited significantly from competition in telecommunication markets through lower prices, more choice and better quality of services. Competition has also played an important role in the development and diffusion of new technologies and services which have also benefited consumers. Competition in the telecommunication sector has developed mainly though supply side measures, however, an important role can be played by consumers themselves in enhancing competition through demand side choices.

For this to occur it is necessary to ensure that consumers are empowered by providing them with better information and more flexibility in making choices in the market. In this context a number of measures are required: improving transparency of prices; minimising costs of switching services; facilitating timely, easy to use and effective settlement of consumer complaints. With such measures in place consumers themselves can help create more effective competition in the market.

As already noted, consumers, when subscribing to mobile services, do not pay much attention to international mobile roaming prices, nor are these prices generally brought to their attention or explained to them. Increasing

transparency is necessary at the domestic level since this provides them with sufficient information to make choices with regard to service providers. Transparency in the context of IMR provides consumers with a more limited scope to make choices since they are already tied to a mobile service provider. The choice then is to find alternative calling procedures or to limit their usage when travelling, roam silently (turn off their phones), disabling functionalities on their phones (e.g. data roaming), purchase local SIM cards (effectively losing their local phone number), using WiFi where available for calls or other messaging applications.

The challenge for policy and regulation is to ensure that consumers have full information on IMR prices when they first enter into a mobile contract, that they understand the potential expenses they may face when roaming, that they can keep up to date with IMR prices, have an understanding on how to technically manage their phones to avoid unwanted charges when roaming.

2.4 Facilitating competition

It is important that solutions to high international mobile roaming charges create conditions of effective competition in the longer term. Measures which help reduce wholesale or retail prices are of course important and provide an immediate benefit to consumers, but such measures do not necessarily lead to a long-term solution. Price caps were usually used by telecommunication regulators as a transition mechanism in the process of creating market competition and would normally be reduced in scope and impact as competition developed, and eventually abolished. In national telecommunication markets price caps were accompanied by other regulatory measures aimed at fostering market entry and developing competition. In the case of international mobile roaming unilateral measures cannot be used to create competition. It is therefore necessary to explore bilateral or multilateral approaches to obtain a solution, which is lasting, to deal with high international mobile roaming prices.

When countries began to move from national telecommunication monopolies toward competition, the regulatory bodies essentially restructured markets so competition could develop. Similarly, when the International Satellite Organisations lost their monopolies, there was agreement among the signatories that those markets needed to be restructured. Similarly, the solution to high IMR charges also requires structural changes.

The introduction of new technologies in the IMRS market could result in structural changes in the IMRS market which create conditions to help create competition. For this reason it is important that policies and regulations do not place impediments to new technologies. Mention has already been made of VoIP and other applications that can be downloaded on smartphones which require enabling policies to allow their use by subscribers. However, there is no guarantee that such technologies will develop, will enter the market, or whether these will be close substitutes to IMRS and have an impact on competition. In a number of cases technologies that are marketed for subscribers to use when roaming are similar to the range of call-back procedures that were developed in reaction to the high accounting rates for international calls in the fixed market. That is, the high IMRS prices offer an arbitrage opportunity (such as VoIP services used at wireless hotspots) which put some downward pressure on prices, but not sufficient pressure to result in prices that would reflect those in a competitive market. There are other technologies which will remain once efficient prices are attained, but may remain only in niche or specialised markets. Nevertheless, it is important to ensure that new technologies that can be used by subscribers when roaming are developed and are encouraged to diffuse.

Proactive policy and regulatory changes are the only sure course of action to ensure that structural changes take place in the IMRS market but these need to be co-ordinated at minimum at the bilateral level, or the regional level, but preferably at the international level. Such policies need to be multifaceted. Consumer empowerment is important, but on its own will not lead to longer term solutions. Ensuring the use of competing technologies is also important but require policies, such as those ensuring network neutrality, that allow the use of applications which have a potential to act as substitutes for IMRS (e.g. VoIP applications using mobile terminals). However, the most important policy initiatives are those that change the structure of the wholesale IMR market. This market has been identified as being primarily responsible for high international retail roaming prices.

There are two main structural measures that can be used and they are mutually compatible and complementary. The first is that countries agree (at the bilateral, regional or international level) to provide access to the MNOs in their country by mobile virtual network operators from other countries at the same terms of conditions as national MVNOs. This implies that the MVNOs can obtain access to the networks of MNOs at national interconnect charges, and offer IMR services. This has two implications. Many countries do not yet allow MVNOs - they would need to do so and, secondly, this implies that the IOT system used by GSMA needs to be changed.[37] Although not a preferred option, MVNOs could be limited to providing only roaming services. The second structural measure is to decouple (unbundle) international mobile roaming services from the bundle of services offered by mobile operators (MNOs or MVNOs) so that users, if they so choose, can when roaming use a competitive supplier of IMR services (the choice can be made either when they initially subscribe to a mobile phone service or before leaving their home country). It is likely that such structural changes will lead to the emergence of regional and perhaps global MVNOs and, in many cases, especially at regional levels, the MVNOs would have close ties with MNOs. These two solutions provide a means of developing sustainable competition in the IMR service market without the need to maintain prolonged price regulation. There are, of course, technical issues involved in implementing structural changes some of which can be complex.

The section below summarises a number of bilateral initiatives that are being discussed to reduce IMRS prices (both wholesale and retail in most cases). It is encouraging that a large number of regional bodies have recognised that high IMRS charges have negative economic and social implications for their region and are examining ways to reduce these high charges. In a number of regional bodies the concern has been at the political level which has helped provide an impetus to find adequate solutions. Finally, as discussed below, there is a possibility that the World Trade Organization' s General Agreement on Trade in Services (as it applies to telecommunications) could be used as a tool to help introduce structural changes in the IMRS market and through this process reduce IMRS charges.

However, in most bilateral and regional discussions are aimed at reducing prices *per se* rather than finding a more permanent solution to high IMSR prices. The exception is the EU's Regulation III (see below in section 3.3) which from 2013 will begin to introduce measures which will lead to structural changes in the market.

3. A Review of Business and Regulatory Initiatives

Although IMRS prices still remain well above costs, they have declined since the early 2000s as a result of market initiatives taken by operators in response to several factors. Increased political, consumer (and media) awareness in recent years, often linked with cases of "bill shock" has imposed pressure on the market to lower retail IMRS prices. Partly, price declines can also be attributed to pressure from governments and regulatory initiatives. Some competition, although imperfect, has emerged as a result of technological change and has helped impose some pressure on the industry to reduce prices.

Examples of developments on the business side include the development of technologies which direct roamers to specific networks in foreign countries. This has allowed mobile network operators which have some affiliation with foreign operators to reduce retail rates. However, such traffic directing technologies have also created difficulties for smaller MNOs in trying to instil some competition in IMRS markets. The other market development which has played a larger role in putting downward pressure on retail IMRS rates has been through on-net pricing. This has led some MNOs with large international footprints to provide improved roaming prices (e.g. Vodafone, Orange, Telefonica, Zain).

A growing trend in response to consumer and regulatory pressure is for IMR service providers to offer fixed price or flat rate packages for roaming which are valid for short periods. Flat rate pricing is emerging in particular for data roaming. While such commercial offers are important in reducing retail prices for consumers, they are often not sufficient to introduce effective competition in the retail IMRS market.

3.1 Technological solutions

A number of technological solutions have developed aimed at providing users a by-pass solution to high IMR charges. Table 2 provides an overview of the advantages and disadvantages of a number of substitutes.

None of these provide a complete substitute to international roaming but can, in some cases, help reduce charges either for outgoing calls back to the country of origin, make calls in the visited or to a third country, receive calls or for messaging. In some cases substitutes mean that the subscriber does not have access to their domestic mobile number, or they may be required to find a free WiFi hotspot which can be difficult where knowledge of a foreign language is required. WiFi hotspots, for example, may be suitable for outgoing calls but not incoming and by definition are not mobile. For data roaming WiFi offers a close substitute but limits the use of applications which need, for example, location information. Other options can be complex for users or impose search costs on users. Technical issues, including the requirement to have a Smartphone, a tri-band phone, or an unlocked SIM card may also restrict the use of substitutes.

As already noted, changes in technology have also introduced some competition at the margin in the retail IMRS market. For example, the ability to use services such as Skype or Wi-Fi with Smart phones allow consumers to bypass high IMR charges but require access to hotspots. The availability of dual-SIM cards provides users with an alternative calling procedure to by-pass high IMR charges but also requires users to subscribe to a second service provider and to purchase a terminal which supports dual-SIM cards. Software solutions which integrate the home SIM card with a SIM card purchased in the visiting country avoid the need to have a dual-SIM card phone. Many of these technical solutions are for users who are technically knowledgeable and well prepared before embarking on international travel. The use of SIM cards with multi-IMSI numbers have also been suggested as a potential technical solution.[38] This would allow a user to choose a different operator for local mobile services and international mobile services. Such technical choices also raise a number of questions. For example, would the second operator be the cheapest for all visited destinations. If the user is a frequent visitor to a second country then a dual-SIM card solution or dual-IMSI may provide a solution. To most users these solutions provide added complexities.

Some examples of close substitutes include Interfone, a Danish company, which is marketing an overlay chip for GSM phones, which when a subscriber dials an international number or roams internationally takes over the call providing savings to users. [39] Gentay, a company specialising in the communication needs of the maritime industry launched in 2012 a global roaming SIM card using multi-IMSI[40] technology and offering worldwide connectivity for voice and data at local rates.[41] Multiple numbers can also be incorporated on the SIM cards to reduce the cost of incoming calls. HolidayPhone[42] provides a temporary SIM card with a call package that includes receiving 3 hours of calls on the users home number, making 2 hours of calls to the users country and 1000MB of mobile Internet access. The package purchased by the user is specific to the country visited and the SIM is a prepaid card from the visited country (the company provides prepaid SIM cards for 17 major tourist destinations. Flexiroam (Malaysia) supports roaming in 200 countries but the subscriber needs to purchase a local SIM card in the visited country and requires a mobile phone with call forwarding functionality.[43]

Table 2 : Advantages/disadvantages of International Mobile Roaming substitutes

SUBSTITUTE	ADVANTAGES	DRAWBACKS
GLOBAL MVNOs – GLOBAL SIM CARDS – REGIONAL SIM-CARDS	Local calls at local rates Price reductions (use of call-back)	No incoming calls to the customer's usual number[64] Lack of brand recognition
PURCHASING A LOCAL SIM-CARD	Local calls at local rates	No incoming calls to the customer's usual number Language barriers
DUAL SIM CARD HANDSET AND SERVICES	Retention of domestic provider	No incoming calls to the customer's usual number Availability of handsets SIM-lock
VoIP SUBSTITUTES (mobile or WiFi network)	Inexpensive over low-cost Wi-Fi access	No incoming calls to the customer's usual number[65] Data roaming charges VoIP application lock or surcharge (mobile handsets) Specific handset or laptop necessary[66]
HOTEL TELEPHONES – PAYPHONES – CALL SHOPS		No incoming calls to the customer's usual number No mobility Cost
INTERNATIONAL CALLING CARDS	Inexpensiveness	No incoming calls No mobility/some nomadicity Language barriers
USE OF SMS	Perfect substitute of domestic SMS	Weak substitute (no voice calls) High price compared to domestic SMS
SATELLITE ROAMING	Global coverage	No incoming calls[67] High prices/limited handset availability
VoIP SUBSTITUTES (fixed network)	Inexpensiveness	No incoming calls to the customer's usual number
EMAIL	Inexpensiveness More flexibility (longer text, file exchange)	No incoming calls Very weak substitute Lack of real-time communication

Source: OECD, DST/ICCP/CISP(2009)12/FINAL, International Mobile Roaming Services: Analysis and Policy Recommendations, Paris 2010.

Roamline, an affiliate of KPN, the Dutch incumbent fixed and mobile carrier, offers a global mobile roaming data roaming service which requires the subscriber to pre-purchase a SIM card which can be used in 130 countries and is charged on a per use basis.[44]Roam Mobility, based in Canada offers roaming for Canadians visiting the United States. It has teamed up with T-Mobile in the US and provides a US number to customers and unlimited calls and text to Canada and the US for a fixed per day charge.[45] Transatel, a French based company, offers to European roamers a multi-IMSI SIM card with embedded local numbers in 5 countries so that local calls in the visited country are made

at local rates and outgoing international calls are also at local rates.[46] Singtel's GlobalDial 121 provides customers with a call-back service.

The range of service providers offering roaming is quite large. Some have links with established operators and some mobile operators, recognising customer dissatisfaction with high prices, are trying to satisfy customer demand for cheaper roaming but making available alternative services.

Regulators can also help in stimulate these solutions by, for example, providing information to users on alternative solutions. More important, however, regulators should ensure that there are no obstacles to the take-up of alternative technologies. For example, many mobile operators have prevented users from downloading *Skype, Whatsapp,* or similar VoIP services which would help bypass high charges. For GSM phones regulatory initiatives, such as allowing subscribers to unlock their phones and use the SIM cards of alternate providers and from operators in visited countries, are important to take advantage of substitutes.

The different alternatives are useful for the experienced traveller or traveller that has some knowledge of roaming and the charges involved. Many of these near substitutes require prior awareness and prior knowledge by users before they leave their home country. Most consumers only become aware of roaming charges once they have left their home country. Despite a range of near substitute technologies it does not seem that they have had a significant impact either in terms of attracting customers or on prices in IMRS markets. An analogy can be made with call-back providers who provided international telephone service in the early stages of market opening in the international long distance voice market when accounting rates between countries, and as a result international calling retail rates, were extremely high. Call-back technology provided a close alternative to international voice calls, but the technology was insufficient to create competition in that market and change the accounting rate system which was in place. The creation of competition in that market required the opening of national markets to competition allowing direct access by national service providers to foreign markets so they could terminate cross-border calls locally.

3.2 Business initiatives

African mobile operators have been leaders in reducing and eliminating international mobile roaming charges in particular Zain (formerly Celtel) which in 2006 inaugurated *One Network* eliminating IMRS charges for its customers in Kenya, Tanzania and Uganda (i.e. customers paid domestic rates for outbound calls when roaming and were not charged for incoming calls).[47] The *One Network* expanded during 2007 to cover 6 more countries in Africa.[48] By the end of 2007 Zain claimed that *One Network* served "*400 million people across 12 countries now connected across Africa in one borderless mobile network covering an area more than twice the size of Europe*".[49] [50] Subsequent expansion of ZAIN also covered the MENA region.

The fact that ZAIN had licences in contiguous countries was an important factor supporting the development of *One Network* as was the liberalisation of international gateways in the countries where ZAIN operated. *One Network* subscribers can make calls to their home country and send SMS at prices applicable in visited countries and receive incoming calls from their home country for free. However, the elimination of roaming charges applied only to traffic which was retained on the Zain network i.e. on-net calls. Nevertheless, given the rapid expansion of the company across the African continent the benefit to customers was significant.

By creating disruptive competition Zain created pressure resulting in a number of other African operators offering cheaper IMRS to neighbouring countries or to countries where they had a footprint usually following the Zain model by providing subscribers with free incoming calls and SMS in visited countries and paying prices in the visited countries for outgoing calls. For example, Glo annonced in May 2012[51]a roaming service (UniWorld) offering a uniform local tariff for prepaid and postpaid subscribers in Nigeria, Benin and Ghana. Orange created a zone of West African countries in 2007, comprising Guinea, Guinea Bissau, Ivory Coast, Mali and Senegal and Vodacom provides roaming in six African countries with free incoming calls for IMRS and outgoing calls charged at the price of

visited countries. In contrast, in Europe where several companies have a fairly extensive cross-border footprint prices were reduced but never eliminated.

Digicel which is active in a number of Caribbean countries launched a service in 2011 which, for USD27 provided for 7 days unlimited roaming on a Digicel network which included incoming calls, unlimited calls to the home country, unlimited text messages to Digicel numbers and unlimited data access. As for offers in other areas this was facilitated by Digicel's presence in those countries where it had licences. PCCW (Hong Kong) mobile provides a "All-in-one Roaming Passport (Day Pass)" covering 53 countries. In contrast to other packages KDDI of Japan has offered a limited package to its users by providing Wi-Fi access for smartphones across 100 countries.

Operators in the European Economic Area have reduced IMRS prices as a result of the price caps imposed by the EU and some have introduced new packages aimed specifically at roaming. T-Mobile in the UK has also introduced a roaming option limited to data. This provides users with a fixed data allowance when roaming which stops the data connection once a certain limit is reached. At the regional level companies such as Telefonica has launched a standard pan-European data roaming tariff. Smartphone customers can now use 25 MB for internet access anywhere across the 27 European Union member states for EUR 2 per day. The tariff targets mobile customers on Movistar or O2 networks. The Pan-European tariff, launched in Germany in May 2012, will be available mid-2012 to O2 and Movistar customers in Spain, the UK, Ireland, Czech Republic and Slovakia. Vodafone (UK) launched a service in 2012 allowing customers to use their standard UK tariff plan for an additional £3 a day. Any excess charges are also billed as if the user was in the UK. In contrast Meteor Ireland announced in 2012 that it would abolish roaming charges in Europe enabling consumers to pay the same charges for calls and texts, but not mobile data charges, as when they are at home. T-Mobile US, taking advantage of its European footprint as well as the lower data roaming prices in the EU has introduced a plan providing its American business customers with unlimited data roaming for USD50 a month.

Elsewhere, many other mobile operators have reduced prices in many cases as a result of regulatory pressure rather than legal requirements. For example, Etisalat reduced calling charges for its UAE customers travelling within the Gulf Council Countries (GCC) by up to 26 per cent in early 2012 following a request by GCC officials to the regions MNOs. In April 2011 Singapore and Malaysia announced a progressive reduction of roaming rates (up to 30 percent for voice and 50 percent for SMS) following Ministerial pressure and in June 2012 Singapore and Brunei announced that they would begin in 2013 to jointly reduce roaming rates.

In May 2012 China Telecom began a novel prepay service by launching a UK MVNO (CTExcelbiz) which markets prepaid packages for China Telecom customers in the UK. The service also provides a local Chinese number which friends and family in China can use to call a China Telecom roamer in the UK. China Mobile is also offering discounted data roaming rates to their customers for voice calls and data access when they are roaming internationally in key business destinations. For example, China Mobile's data roaming price for its customers when they are in the US is the equivalent of $1.50 MB significantly lower than what US operators are offering their customers when roaming in China. The company has also indicated that it would become an MVNO in the USA, with plans for entry into France and Germany. MTN (South Africa), in March 2011, began providing free incoming calls and SMS for both postpaid and prepaid customers travelling in the South and East Africa (SEA) region (countries where MTN has market presence). Tele2 (Sweden) is marketing a VoIP application allowing its customers to make and receive calls outside of Sweden at the price of a normal mobile voice call.

The increased media attention as well as political attention to high IMRS prices has played an important role in many regions in reducing retail prices. A lesson from ZAIN and others is that lower prices can result when a network operator has access to foreign markets. In these cases access was available because these companies had a MNO licence. Clearly this is not generally an option given that a limited number of MNO licences are made available in most countries because of spectrum limitations as well as the cost of building a network. As a result the MVNO option suggested previously is necessary, an option that China Telecom seems to be following.

GSMA

The GSMA, in June 2012, obtained agreement among 24 (of 800) members to enhance transparency for customers when roaming. This initiative is limited to data roaming and includes sending SMS to customers to remind them of data roaming charges when they arrive in a foreign country, implementing a data spending limit and sending alerts when that limit was reached and temporarily suspending data services when the limit was reached.[52]

3.3 Initiatives by International Organisations

ITU

Early work by the ITU on IMR charges was noted above. More recently, ITU-T Study Group 3 approved in September 2012 a new Recommendation ITU D.98 on Charging in International Mobile Roaming Service [53]. Section 4 of this Recommendation contains principles for lowering IMR rates including empowering consumers (section 4.1), market-based solutions (section 4.2) and regulatory intervention (section 4.3).

The main recommendations, which are non-binding, are highlighted in Box 1.[54] In addition, a new supplement to ITU-T Recommendation D.98 was proposed and will be studied by Study Group 3.

Box 1: ITU Recommendation D.98 Charging in International Mobile Roaming Service

Empowering consumers

1. transparent information on IMR retail rates and structure before users roam internationally
2. usage alerts when users start to roam
3. warning alert when a certain cost has incurred
4. roaming cost caps
5. special user protection measures for inadvertent roaming in border regions
6. user choice of visiting network

Market-based solutions

1. provision of roaming pricing plans which fit different users
2. support substitutes like local SIM cards, and provision of IMR by other means
3. regional and interregional cooperation
4. cooperation of mobile operators to lower wholesale tariffs.

Regulator intervention

This section of the Recommendation states:

" regulators and policy makers, taking into account specific national or regional conditions, may introduce regulatory interventions on international mobile roaming service tariffs for the benefit of users by encouraging competition. Possible interventions may include a range of regulatory measures such as usage alerts, bill caps, tariff caps and pre-selection."

Source: ITU, Telecom Standardization Bureau, new Recommendation ITU-T D.98, Charging in International Mobile Roaming Service, www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=3?.

The ITU's World Conference on International Telecommunications 2012 (WCIT-12), which meets in December 2012, will review the International Telecommunication Regulations (ITRs) where the international treaty that is the basis of today's connected world will be reviewed. The ITRs were agreed in 1988 at the World Administrative Telegraph and Telephone Conference in Melbourne, Australia, and came into force in 1990. The ITRs set out principles for ensuring that networks can connect with each other smoothly, and that international services will be offered in a fair and efficient manner. Within this context, proposals have been made to add provisions to the International Telecommunication Regulations (ITRs) to ensure transparency of end-user prices for international mobile services, and that rates are cost-based. Improved cooperation is needed to achieve effective solutions and make bill shock a thing of the past.[55]

OECD

The Organisation for Economic Co-operation and Development (OECD) began work on roaming in 2008 by examining roaming retail prices for voice and SMS and providing a preliminary assessment of policy issues. This report found that roaming prices were excessive in the OECD area compared to underlying costs or compared to the retail price of a domestic mobile call plus an international call from the fixed network.[56] This was followed up by a report on providing an analysis of potential policy recommendations.[57] A report on data roaming prices was carried out over 2010-11 which analysed pricing data for data roaming (including for laptop use) and used the data to estimate total expenditures for several mobile roaming usage patterns. Most OECD operators have optional data plans available (usually daily, weekly and monthly plans). Information to users is facilitated somewhat in that operators categorise countries by zones and provide a single price for each zone.

Following this work a non-binding set of measures was adopted by the OECD in February 2012 (OECD Council Recommendation)[58] which put forward a series of measures that policy makers could use to raise consumer awareness and protection, ensure lower prices and encourage effective competition. The main points of the Recommendation are highlighted in Box 2.

Regional Initiatives

Perhaps one of the earliest regional initiatives on international mobile roaming was a *Report from the Nordic competition authorities* in 2004.[59] The report recommended that "... *analyses* [of international roaming markets] *take into account that price regulation can unduly distort market development and that technological development in itself might lead to effective competition on the markets shortly*."[60] Although there has been progress in technologies since 2004, this has been insufficient to lead to effective competition in the IMR market.

European Union

The European Union had been concerned with high intra-EU IMR prices for a number of years. In 2003, the Commission decided that the international roaming market should be considered as a relevant market. This eventually led in June 2007 to the adoption of a regulation on international mobile roaming. The EU Roaming regulation was adopted in 2007 and introduced caps on roaming prices within the EU ("Eurotariff") and imposed certain information obligations on operators. The Eurotariff set maximum prices for phone calls made and received while travelling within the EU. Revised rules were adopted two years later reducing roaming prices for voice calls even further as well as imposing caps on SMS prices. An additional requirement as of July 2010 was aimed at reducing "bill shock" by introducing a cut-off mechanism once data roaming bill had reached 50 euros and operators were required to send an SMS message once subscribers had reached 80% of the agreed limit.[61]

Box 2: OECD Council Recommendation

The OECD Recommendation encourages governments to:

- promote awareness about the cost of roaming services and the availability of substitutes;
- promote transparency of information provided to customers by international roaming providers regarding the use and billing of roaming services;
- promote transparency of information provided to customers by international roaming providers regarding the use and billing of roaming services;
- provide information to data roaming customers on the risk of automatic and uncontrolled data roaming connections and downloads and explanations about how to switch off these connections; agreed financial limits, beyond which data roaming transmission would be stopped, unless the customer follows an indicated procedure: personalised notifications when data roaming services have reached a certain proportion of an agreed financial limit;
- remove barriers that may prevent smaller players from competing with larger players to offer roaming services, in particular by forming trans-national alliances;
- In removing such barriers, Members should pay due attention that they do not protect inefficient operators, and that these alliances do not in fact reduce competition.
- encourage discussions with industry about the transparency of (headline or non-discounted) Inter-Operator Tariffs (IOTs) for IMR services to inform future or current regulatory proceedings and consider collecting data on wholesale roaming rates and publishing benchmarks of aggregate rates that preserve commercial confidentiality;
- remove barriers that prevent mobile virtual network operators to have access to local wholesale mobile services for the purpose of offering roaming services and ensure that mobile virtual network operators benefit from possible regulated wholesale roaming rates between operators in different countries when purchasing wholesale resale roaming in the home country;
- if it is determined that market dynamics are insufficient to produce reasonably competitive wholesale prices, authorities are encouraged to regulate wholesale roaming prices, including by reaching bi- or multi-lateral agreements between countries, as appropriate, and/or through the introduction of price caps based on commonly established principles;
- if market dynamics are insufficient to generate competition, consideration should be given to implement retail price regulation to protect customers from paying excessive prices for using roaming services;

Source: OECD, 16 February 20102, Recommendation of the Council on International Mobile Roaming Services, Paris.

On 30 May 2012 the Council of the European Union approved international roaming Regulation III, which became effective on 1 July 2012, when Regulation II expires. [62] The new regulation will remain in force for 10 years. Its provisions (see Box 3) builds partly on earlier provisions. Some of the existing provisions, which only applied to intra-EU roaming, will be extended to apply to roaming outside of the EU. Several significant changes, which are

structural in nature, have been introduced, namely that customers will be able to choose a separate provider of roaming services after 2014 and that operators will be required to provide access to other operators for the purposes of providing roaming services at prices which are published as a reference offer following predetermined guidelines. The latter provisions are the most crucial.

Whereas the prices caps that were imposed by the European Union have helped place downward pressure on prices they have not created the conditions for competition. The new provisions by providing cross-border access are essentially treating regional roaming as an interconnect service and by facilitating the creation of cross-border MVNOs in the European Union area the provisions are laying down conditions which will eventually facilitate the development of competition.[63] It is worth noting that the EU used as a benchmark to set regulated roaming prices the mobile termination rate benchmark. It is also worth highlighting the important reductions that are being imposed on retail prices and wholesale prices that indicate the extent to which these prices diverge from cost-oriented prices which would be offered if IMRS markets were more competitive.

Box 3: Main provisions of the EU Roaming Regulation III[64]

- The price-cap system for retail prices is extended to cover data transmission roaming services, (data euro-tariff) applicable to data communications within the European Economic Area (EEA) with a value that does not exceed the maximum price set in the new regulation. Limit is EUR 0.70 per megabyte as of 1 July 2012, changing to EUR 0.45 per megabyte on 1 July 2013, and to EUR 0.20 per megabyte on 1 July 2014;

- New reductions on the maximum limits that were set for the voice euro-tariff and the SMS euro-tariff. The voice euro-tariff, which was limited to EUR 0.35 per minute, will change to a maximum limit of EUR 0.29 per minute on 1 July 2012, and this limit will fall to EUR 0.24 per minute on 1 July 2013, and to EUR 0.19 on 1 July 2014. The maximum limit of the SMS euro-tariff will fall from the current EUR 0.11 per SMS to EUR 0.09 per SMS on 1 July 2012, to EUR 0.08 per SMS on 1 July 2013, and to EUR 0.06 on 1 July 2014;

- After 1 July 2014 mobile service customers will have the possibility to sign up for alternative mobile services within the EEA, separate from their national mobile operator. After 1 July 2014 customers will have the right to change their roaming provider at no cost, within 3 working days of concluding a deal with a new roaming provider;

- After 1 January 2013 mobile network operators will be obliged to satisfy all reasonable requests by other operators to access their networks in roaming and to publish a reference offer considering the specific guidelines to be published by the Body of European Regulators for Electronic Communications (BEREC);

- The obligation, previously in force, for operators to automatically provide their customers - via a messaging service - with basic personalized information about the roaming tariffs for voice, data or SMS communications when they enter another EEA country, now also applies when customers enter countries outside the EEA;

- The obligation, previously in force, for roaming operators to offer their customers, free of charge, a service providing information on the accumulated consumption of roaming data and which guarantees that the accumulated expenditure on that service does not exceed a specific monetary limit (EUR 50 by default) after which the service is no longer provided, now also applies when the customer travels outside the European Union (with some exceptions, established in the Regulation).

Source: http://ec.europa.eu/information_society/activities/roaming/regulation/archives/current_rules/index_en.htm

By 2013 the structural measures will begin to be implemented and while there will certainly be some technical challenges they should be no more burdensome than, for example, local loop unbundling were for fixed PSTN operators. Again, as in the case of LLU there is bound to be a learning period for operators as well as regulators.

In examining developments in Africa where ZAIN, MTN and others have made significant steps to reduce roaming charges, the question arises why this has not happened in Europe where a number of operators (e.g. Orange, Vodafone, T-Mobile, Telefonica) have licences (or are part share-holders) in a number of EU countries. Smaller operators in Europe are not in a position to emulate Zain since in most European countries no further MNO licences are available and in any case the costs would be excessive for them. Clearly the solution would be to provide these companies with licences through MVNO agreements so that there is an opportunity to create competition in the IMRS market. This is what the new EU Regulation III is aimed at.

AREGNET and GCC

The Arab Regulators Network, AREGNET, was given the responsibility by Ministers to follow-up on a 2005 report which examined international mobile roaming prices in the region and found them to be excessive relative to domestic mobile prices. The work of AREGNET[65] focused on developing a 'glide-path' for wholesale rates (IOTs). The wholesale rates were based on retail prices for similar calls in each country and a 30% mark-up was added to derive suggested retail prices. Despite the concern for high IMR prices agreement could not be reached on the AREGNET proposal. Ministers of the Gulf Co-operation Council, however, agreed in 2008 to follow-up on the AREGNET proposals and reached agreement on a formula to determine retail and wholesale rates using price caps with reductions in prices staggered over 2010 and 2011. The GCC roaming working group is examining how to impose price caps on SMS, MMS and data roaming charges.[66]

Following a decision of the Ministerial Committee of the Gulf Cooperation Council (GCC), taken in February 2012, to introduce maximum prices cap for all mobile operators within the region, the GCC agreed to reduce prices for roaming amongst its six countries. In this context, Bahrain's Telecommunications Regulatory Authority (TRA) has issued an instruction to all mobile operators to implement reduced tariffs for international calls made to GCC countries while roaming in GCC countries. Bahrain's TRA reduces 75 per cent roaming tariffs across GCC.67

The closer economic ties between GCC countries including a commitment to economic integration, much like the EU, facilitated the success of the GCC relative to AREGNET. The GCC agreement, which is in the form of a Memorandum of Understanding, foresees that other countries may join but need to have adequate provisions to enforce the agreement.

CRASA[68]

The Communication Regulators' Association of Southern Africa set up a Regional Alliance Task Team (RATT) in 2008 to examine the problem of high IMR charges and subsequently commissioned a study published in 2010 and which put forward a number of short term goals for SADC's consideration.[69] These included regular roaming data collection, multilateral cost reduction measures and roaming hubbing, increased transparency and consumer protection and price control by agreement. Some of these have been implemented by the RATT in particular greater IMR price transparency through SMS notification when travelling, collection of comparable roaming price data by regulators, setting and notifying users of bill limits. Ongoing work is underway to examine the underlying costs of roaming in the Southern African Development Community.[70]

The Economic Community for the West African States (ECOWAS) has undertaken important initiatives in developing regional roaming arrangements.71 These have been undertaken through intra-operator agreements which allow roaming subscribers to receive free calls when roaming and pay local rates for outgoing calls. The arrangements however are not generalised in that they only cover specific networks and do not apply completely to all ECOWAS countries. Regional roaming has been facilitated by the fact that several operators have a regional

footprint (Orange Zone, Zain One, and One World) but also because of close co-operation between the regional telecommunication authorities.[72]

In Africa, the African Union has also examined the possibility of affordable roaming tariffs through regulation.73 In this context the Commission put forward a number of proposals including:

- require transparency for roaming tariffs
- develop a single web site showing roaming tariffs
- co-ordinate and adopt common regulations which are obligatory
- try and obtain common acceptable rules among the African mobile operators

The breakdown of IMR charges in many parts of Africa developed largely by the fact that operators had licences in contiguous countries and also through effective co-operation between regional regulatory associations. This provides an important lesson which is that competition can work if a mobile operator is willing to break the mould (such as Celtel/Zain) but only if the conditions allow this to occur. The crucial factor has been that operators had licences in several countries in the region.

APEC TEL and Asia Pacific Telecommunity

APEC Ministers first discussed the issue of IMR in 2008 followed up by further analysis in APEC TEL. Emphasis was placed on developing guidelines to protect consumers and in 2010 APEC TEL produced "Guidelines for the Provision of Consumer Information on International Mobile Roaming" which put forward best practice suggestions on providing IMR information to consumers.74

The guidelines suggested the types of information that should be provided to consumers, how to provide this information as well as the need to provide information on alternative technologies to consumers. The Asia Pacific Telecommunity International Mobile Roaming Working Group developed guidelines for regulators and the for operators aimed at enhancing transparency of information. 75 The Guidelines for Regulators to Provide Information on International Mobile Roaming (IMR) Services is aimed at suggesting what type of information regulators should make available to the public including informing consumers of the high cost of IMRS, providing information on alternatives to IMRS services and that regulators should have a dedicated page on their website on IMRS issues with the following information.

A similar set of Guidelines for Operators to Provide Information on International Mobile Roaming (IMR) Services emphasised similar requirements to improve transparency by providing subscribers with information. The guidelines also put forward suggestions for reducing "bill shock". They also suggested that operators provide subscribers with information highlighting differences in charging structures between IMRS services and domestic mobile services, and how subscribers can deactivate part or all of the IMRS services. The Guidelines also suggested that home operators may choose to adopt zonal charging for IMRS service, under which the same rate would be applied to a set of countries that fall under the same zone and inform subscribers as to which countries are covered by zonal pricing.

The APT also suggested that regulators should examine whether regulatory barriers exist in their countries which could create obstacles to potential substitutes for IMR services and should also take steps to educate subscribers as to the available substitutes they could use to reduce the cost of roaming.

Box 4 summarises the main features of these guidelines.

ASEAN

The ASEAN Telecommunications and IT Ministers have, as their goal, a roaming policy where users that roam across the 10 member countries pay the same charges as in their home country. The ASEAN Telecommunication Regulators' Council (ATRC) adopted a *Record of Intent* aimed at strengthening co-operation in telecommunications regulations, focusing in particular, in the short term, on lowering intra-ASEAN roaming charges. In 2011 ASEAN

Ministers issued a Joint Ministerial Statement at the 11th ASEAN Telecommunications and IT Ministers Meeting welcoming this initiative.[76] Reducing roaming charges in the region has also been highlighted in the ASEAN ICT

Masterplan 2015 (AIM2015).[77] Progress has mainly been through bilateral agreements (see below). More recently, Indonesia's Minister indicated support for a "roaming-free" Asian region.[78]

Box 4: APT Guidelines for Regulators and for Operators

Guidelines for Regulators :

1. A plain description of IMR services;

2. A prominent notification that using IMR services may be significantly more expensive than using domestic mobile services;

3. That IMR charges may apply to the following activities undertaken on a mobile phone while travelling overseas:

- making and receiving calls

- receiving and retrieving voicemail messages

- sending and receiving SMS messages and multi-media messages

- using mobile data services, including but not limited to browsing the internet, sending and receiving emails;

4. Before their departure, consumers are highly encouraged to obtain from their mobile service providers the detailed information of IMR charges applicable to their visited countries, and should take note of the following:

(e) whether there would be any difference in charges among different mobile networks in the visited country, and remind consumers that they may manually select the designated network under the "manual" mode of the network selection when travelling in the visited country

5. Hyperlinks to the web pages of individual operators dedicated for IMR-related information; (Regulators should work with their operators to ensure that their operators have followed the "Guidelines for Operators to Provide Information on IMR Services" when providing information on their websites;)

6. Information of various types of alternatives to IMR services, including but not limited to a description of how these alternatives are used, their advantages and limitations, etc.;

Guidelines for Operators:

1. Operators are recommended to provide clear, accurate and easy to understand information on IMR services to customers;

2. Customers should be informed that in general IMRS is significantly more expensive than using their national mobile services;

3. Subscribers should be informed that, when roaming, they may be paying for making and receiving calls and SMS messages as well as using mobile data services including email;

4. Operators are recommended to inform subscribers of different charging structures for IMRS compared to national services;

5. Customers should be provided with inform on how to deactivate all or some IMR services;

6. Customers should be notified by SMS messages when they roam outside their home country through SMS that IMR charges will apply;

Source: Asia Pacific Telecommunity, International Mobile Roaming Working Group Working Group Report , 15 May 2012, at http://www.apt.int/sites/default/files/2012/05/APT_IMR_Working_Group_Report_Final.pdf

South Asian Association for Regional Cooperation (SAARC)

The 2008 SAARC meeting of the Heads of State of the SAARC, in 2008, urged that mobile roaming tariffs in the region be reduced viewing this as an important step to stimulate regional trade. The Colombo Declaration they adopted stated that:[79]

"The Heads of State or Government observed that an effective and economical regional telecommunication regime is an essential factor of connectivity, encouraging the growth of people-centric partnerships. They stressed the need for the Member States to endeavour to move towards a uniformly applicable low tariff, for international direct dial calls within the region,"

Latin America

A number of bodies in South America have been dealing with roaming including those focused mainly on telecommunications (Regulatel and CITEL), and those dealing with regional economic integration (MERCOSUR, CAN and IIRSA).[80] A number of projects have been undertaken in the different bodies dealing with cross-border roaming in the region. IIRSA began examining roaming prices in 2008 and followed up with a workshop later in that year.[81] Its work is aimed at prompting a competitive roaming market in the region and improving costs, quality and coverage in the context of a South American Roaming Cross-border Agreement[82]. The project was also aimed at improving regional co-ordination by the regulators from participating countries to facilitate the development of regional roaming. CITEL has also put forward proposals to increase transparency on IMRS charges in the region.

The Caribbean

The Caribbean Community (Caricom) in a *Draft Regional Information and Communication Technology (ICT) for Development Strategy, Telecommunications Services Sector* of 2010 suggests several challenges relevant to roaming that the region should take-up including establishing a single mobile numbering plan for the region and removing mobile roaming charges and remove mobile termination for data and voice.[83] CARICOM will begin in 2013 to undertake a study on the "*Development of a Regional ICT Space for CARICOM countries*" which includes as a module an examination of new regulations for mobile roaming charges.

3.4 Bilateral Initiatives

There have been a number of bilateral initiatives to reduce cross-border roaming charges usually taken between neighbouring countries that have close trade, tourism ties or population links. In many cases the agreement to move forward on reducing IMRS charges has taken place at the political level but there may be a need to provide statutory power to regulators/ministries to enable agreements to be implemented and enforced. In certain cases political pressure on the incumbents in the two countries involved may be sufficient to reduce charges. For bilateral agreements to be effective there are a number of elements which may be required. These would include the methodology used to reduce prices and a decision on whether only wholesale prices or wholesale and retail prices would be targeted. A decision on whether reductions in prices will be "one-off", or take place in steps over time and whether this will be based on a cost model or agreement on a " glide path". Good co-ordination is also required between regulators of the two countries involved. Consideration also needs to be given to whether structural measures will also be implemented to ensure that bilateral arrangements lead to longer term competition allowing the eventual phasing-out of regulatory measures.

To be effective a bilateral agreement would require that country *A* agrees to require its MNOs to reduce origination and termination charges faced by MNOs in country *B* if these charges are also reduced for the MNOs from country *A*. Retail charges for IMRS would not necessarily have to be similar in bilateral agreements although it would be expected that, following the reduction in wholesale charges, that retail prices would decline. Wholesale charges would be similar unless there are well defined cost differences between the two countries.

Examples of bilateral agreements some of which are underway and others under discussion include:

- **Singapore and Malaysia** were the first ASEAN countries to take action on IMR prices through an agreement entered into by the regulators in the two countries.[84] The regulators agreed to implement a number of measures which increased transparency for consumers. In addition they agreed that consumers would have the option of capping their data roaming usage. Price reductions of up to 30% for voice calls and 50% for SMS were agreed to beginning in May 2011 for roaming services in Singapore and Malaysia and phased in over time. The agreement covered both wholesale and retail prices. The two regulators have also agreed to continue examining what actions to take to reduce mobile data prices and MMS and video calls.

- **Brunei Darussalam and Singapore** have agreed to reduce roaming rates for mobile voice calls, SMS and data roaming charges by the first quarter of 2013. As part of the agreement both the wholesale inter-operator wholesale charges and retail charges will be reviewed.[85]

- **Brunei Darussalam and Malaysia** have agreed to discuss the reduction of roaming rates but no announcements have been made to indicate whether there is progress although it would be expected that such an agreement would reflect decisions taken between Brunei and Singapore and Singapore and Malaysia..

- **Australia and New Zealand** issued a joint report[86] in 2010 which reviewed mobile roaming between the two countries and recognised that prices, both wholesale and retail, were high and transparency for users was inadequate. The report concluded with a potential list of possible actions that could be taken to reduce IMR prices. The report examined the pros and cons of a number of measures. Those measures viewed as having some potential included rerouting technologies for outgoing calls viewed as reducing wholesale charges, improving transparency through a centralised website showing the roaming rates of all national operators, SMS on arrival in the visited country and SMS after a roaming charge has been incurred in the visited country showing the price of the communication. Billing caps were also put forward as a suggesting for controlling charges for users. The potential for price controls, on either wholesale or retail or both, was also raised in the discussion paper. Further solutions raised was to mandate wholesale IMR services to any home network (Australian or New Zealand) upon request and using MVNOs to offer inbound services to foreign MNOs. Other potential structural solutions discussed were unbundling mobile roaming services. The report recognised that there could be a need for harmonisation in legislative provisions between the two countries in order to implement certain recommendations. Following this report (which had the status of a discussion paper) the Ministers of the two countries agreed in 2011 to undertake a full market investigation into trans-Tasman mobile roaming. Australia and New Zealand have a Free Trade Agreement which covers the telecommunication sector and which was being reviewed over 2012 as an option to be used to put in place a bilateral agreement on IMR.

- **Finland-Russia and Poland-Russia** have international mobile roaming agreements**.** Russia had initially sought to have an EU-Russia agreement but this effort was not successful. Israel had similarly tried unsuccessfully to join the EU agreement and had suggested to the EU that it widen its proposed roaming area to include any county that would harmonise its regulations on a reciprocal basis. According to Israel his was rejected on the grounds that the EU could not enforce its regulations outside Europe.[87] Russia has opted to try and follow a bilateral approach with border EU countries. The intent of the Polish-Russia discussions in 2011-2012 was to enter into a Memorandum of Understanding between the operators of the two countries and the Ministries. Although the MoU was agreed to by the Polish operators and the two Ministries the Russian operators did not sign. The MoU was only valid until the end of 2011 and has not been renewed. Furthermore, the Russian authorities do not have the authority to require their operators to adhere to an MoU. The situation with respect to discussions between Finland and Russia, also during 2011-2012, has been similar to that between Poland and Russia. The fact that the Russian authorities do not have the legal power to implement an agreement which would lower the wholesale roaming charges of their operators has meant that, despite the desire of the Russian authorities, that discussions are at an impasse.

The role of cross-border and trade agreements

Domestic ICT regulators do not have any jurisdiction over wholesale rates for international mobile roaming charged by operators in foreign countries. As such, some form of cross-border co-operation is required which could be at the bilateral, regional or international level. Clearly, a global agreement would be the preferred way forward, but may be the most difficult, and will unlikely be the most rapid given the number of countries involved. While a number of regulators wish to move ahead with bilateral or regional agreements, there is a concern, as discussed above, by some that trade negotiators will be reluctant to allow such initiatives arguing that a bilateral or regional agreements may have to be opened up to third parties as part of *most favoured nation* obligations.[88] [89]

Bilateral IMR service agreements, which have only begun to be implemented, have not to date been challenged by other countries in the context of the GATS MFN commitments. In the case of a bilateral agreement it may be possible for third countries to request their operators obtain the same treatment in the two countries that have a bilateral agreement. This could lead to a WTO dispute procedure. However, it should be noted that the IMRS bilaterals are unlikely to have an impact on third countries.

Where a Free Trade Agreement exists between several countries a bilateral agreement between two countries covered by that agreement may provide a "free-ride" to operators from a third country. The benefits from the bilateral need to be examined relative to the costs of providing that " free-ride". If the economic and social links between the bilateral partners is high then the benefits are likely to outweigh any costs.

By allowing third countries to join bilateral agreements on IMRS and adhere to the same principles as the initial partners would also help to reduce the risk of disputes. The OECD in its policy paper argued that bilateral agreements should be open to all countries that were willing to reciprocate and take action against their operators wholesale rates, citing the framework developed (but not agreed to) by AREGNET, which was in the form of a MoU, as one example which could be used.[90]

The World Trade Organization's (WTO) Basic Telecommunications and Reference Paper makes no explicit mention of international mobile roaming services (or for that matter mobile services).However, commitments in the context of market access and national treatment include cross-border supply, consumption abroad and commercial presence. At an informal Symposium on International Mobile Roaming held at the WTO in March 2012 there was discussion (but no conclusion) as to whether the Basic Telecommunications Agreement applies to wholesale international roaming services and whether this would imply that there was a requirement to offer non-discriminatory terms and conditions for interconnection.[91] A 2004 WTO report[92] "*Mexico – measures affecting Telecommunications services*" which was released by a Panel examining the dispute between the United States and Mexico regarding provisions in Mexico's domestic laws and regulations on telecommunications stated that:

There is no reason to suppose that provisions that ensure interconnection on reasonable terms and conditions for telecommunications services supplied through the commercial presence should not benefit the cross-border supply of the same service, in the absence of clear and specific language to that effect. Since the GATS deals specifically with international trade in services by four modes of supply that are considered comprehensive, it would indeed be unusual for interconnection disciplines not to extend to an obvious and important mode of international supply of telecommunications services – cross border.[93]

The Panel argued that cost-orientation also should apply to domestic and international interconnection and that the domestic rates provided a benchmark for international interconnection

4. Proposed Best Practice Recommendations

International mobile roaming prices have declined over the last few years and there have been improvements in many markets through increased transparency and access to alternate technologies which, while not perfect substitutes, provide a means for mobile subscribers to reduce their bills when roaming. Nevertheless, from the many studies carried out across the different economic regions, the evidence indicates that the IMR market is one characterised by market failure leading to a general conclusion that it is highly unlikely that high international mobile roaming prices will be corrected through market forces. If this is the case regulatory initiatives will be required.

There are costs to regulations as well as benefits. In the case of IMR services the costs are imposed on regulatory bodies as well as mobile network operators. On the other hand there are benefits in correcting market inefficiencies, in particular by reducing the net economic loss to society resulting from inefficient prices. Certain countries are concerned, especially those that have a large number of foreign tourists, that they will experience a loss in foreign exchange revenues. It is more likely that as prices fall for voice, messaging and data, that foreign tourists will begin using these services more intensively resulting in the longer term to higher foreign exchange revenues. For those countries that have moved toward greater economic integration it is evident that high IMRS prices are an obstacle to such integration imposing a cost to business as well as consumers.

The issue of high IMRS prices (wholesale and retail) needs to move forward from debates, workshops, analysis, etc., toward more concrete implementation. There has been progress and the background work has been extremely useful in providing all the main elements to move toward more concrete actions. The European Union has moved forward in implementing change and there has been progress in obtaining lower prices, but it has also been recognised that the solutions that have so far been used are not in themselves conducive to create in the long term competitive markets. The recent regulations adopted by the EU are likely to achieve this goal but there is a need to sort out the complexities of implementing these solutions.

Bilateral and regional initiatives are extremely important and help in the process of reaching a global solution to the problem of high prices. They should be encouraged to move forward. However, consistency in measures across regions is important. At present such consistency seems to be emerging. In the longer term it is clear that a global solution is required which can ensure that the IMRS market can develop effectively within a competitive framework. This may occur through the widening of some regional frameworks once they are established to encompass other regions. The OECD has put forward recommendations for its member countries[94] and the ITU developed a recommendation and is revising the current International Telecommunications Regulations Discussion, although informal, has begun at the WTO.

This section will build on section 3 by putting forward recommendations on best practice which could be followed at the international level, regional and national levels in order to develop a long lasting solution to reduce high international mobile roaming prices. The range of solutions is twofold. Solutions which provide more empowerment for users as well as improve transparency in the market and solutions aimed at developing effective wholesale and retail price competition in the international market for mobile roaming.

4.1. Transparency

Transparency in markets plays a fundamental role both in empowering users and in providing the relevant authorities with information in order to take appropriate decisions. Transparency can also be important for the market players to foster competition.

Empowerment for users

The choices that users (consumers and business users) make in international mobile roaming markets can be important in helping create some competition in this market and consequently helping in changing the behaviour of service providers in the market. Business users, in particular those from large companies that have a high volume of international mobile roaming business, are in a better position to negotiate with their mobile service providers more favourable IMRS prices, so that specific attention needs to be paid to consumers and to small and medium enterprise users. Empowerment is closely linked with increased transparency. Work by BEREC, AREGNET and the Arab Telecommunications and Information Council of Ministers, CRASA and the African Union, APEC and the APT, the Inter-American Commission for Telecommunications (CITEL), the ITU, the OECD, the EU, and a number of other regional organisations have all highlighted the need for increased transparency for subscribers and, to a large extent, these bodies have reached similar conclusions as to what is required to attain that goal. As competition develops in the IMRS market regulatory authorities may find that the market itself through the competitive process provides sufficient transparency. There is a consensus across continents that this is far from being the case at present.

Empowerment for users can be facilitated unilaterally by the competent authorities within a country and should, in practice, be easy to implement at the regional level.

Some best practices in this regard are outlined below:

- ✓ Users need to be informed when roaming that charges are higher than domestic charges and that there is a risk involved in adhering to the same consumption pattern that they use at home when roaming.
- ✓ Users should have easy access to the prices they will pay in visited countries.
- ✓ Users should be informed of international mobile roaming prices, including the structure of these prices, when subscribing to mobile voice and/or data services and the information should be easily found on the mobile operator's web site.95
- ✓ Simplicity and clarity of information is important since prices differ for incoming calls, outgoing calls to the home country, outgoing calls to the visited country, and data usage charges. In addition, charging practices may differ for IMR services as opposed to domestic services e.g. in the use of per minute or per second pricing or the use of peak/off-peak charging.
- ✓ Subscribers should be informed of how to disable handsets to prevent international roaming, for example, for data roaming. Many data applications on smartphones can lead to inadvertent roaming so information on how to disable such applications is important.
- ✓ When arriving at a roaming destination, users should be informed by SMS that roaming charges will be incurred and provided with information on those charges.
- ✓ Users should be able to choose a preferred visiting network and the prices on that network.
- ✓ Pre-determined limits (caps) could be applied on international mobile data roaming and users should be informed when they are close to attaining this limit. The default should be to disconnect data roaming when the limit is reached, although the option to exceed this limit should be available.
- ✓ Regulatory authorities need to ensure that users are protected from inadvertent international roaming in border regions.
- ✓ Regulators are encouraged to review (with their national taxation authorities) the tax treatment of IMR services imposed on their national users as well as foreign roamers to avoid double taxation and to ensure that tax treatment is consistent with international provisions, in particular the ITRs.

Price Regulation

The analyses and reviews of international mobile roaming that have been undertaken by all the international organisations, regional bodies and individual countries have reached a similar conclusion. That is, that retail prices for international mobile roaming are significantly high, have no linkage to domestic mobile prices and do not reflect costs. In addition, there is widespread agreement that a major reason for high retail prices are the underlying wholesale prices which come under the responsibility of ICT regulatory authorities in visited countries. There is also, to a large extent, agreement that a lowering of wholesale rates may not in itself be sufficient to lower retail

rates since market forces are weak in the international roaming market. These findings lead to the following conclusions for best practice regulation:

- ✓ wholesale price regulation of inter-operator tariffs is necessary to move to reasonable cost-based IMRS retail prices. Such regulation requires bilateral, or regional or international agreements.
- ✓ government authorities need to have legal power to enforce such regulation in particular to impose price controls.
- ✓ a number of models can be used to move to lower wholesale IMRS charges including price caps, cost models or using national mobile termination rates as a benchmark and reductions in charges would normally take place through pre-determined glide-paths.
- ✓ retail price regulation would be unnecessary if the decline in wholesale prices is passed on to the retail market. There is no clear evidence to indicate whether this would take place so monitoring would be necessary if regulators decide not to impose any retail price controls. The experience of the EU indicates that without retail caps declines in wholesale prices are not usually passed on to users.
- ✓ IMRS retail rate reductions should be avoided if they are not complemented by wholesale IMRS price reductions. Without wholesale rate regulation and wholesale price reductions, the flexibility to reduce retail IMR prices would be limited to a level which is likely to be unsatisfactory and could result in margin-squeeze especially for those operators, usually the smaller operators, that are not in a position to obtain lower wholesale prices in other countries.
- ✓ per second charging is the preferred means for retail pricing. This implies a similar pricing structure for wholesale prices but does not preclude the use of an initial flagfall charge.[96]

Price regulation should lead to lower IMRS prices but will not resolve the problem of market failure. However, in the absence of structural measures price regulation remains the best option to obtain reductions in prices of international mobile roaming. However, in the longer term it is not desirable to maintain price regulation so that consideration may have to be given to adopting structural measures so that long term competition in the IMRS market can develop.

Transparency of wholesale rates

Transparency is important at the wholesale level in addition to retail prices. In general, wholesale rates paid by a retail company in an industry are not known to competitors and there is a danger that if they are made public that the competitive process can be negatively affected. However, where there is no competition making wholesale rates known can help in creating competition. In the case of IMRS high wholesale rates have been determined as being at the core in explaining high retail charges so that the evolution of these charges is important to ensure that any policies regulators take are effective. In the case of the telecommunication sector it has been common practice by telecommunication regulators to make public wholesale rates (interconnection/termination rates) and this has helped drive the process of creating more effective competition. In the case of roaming the IOTs are transparent to the mobile operators but not to the regulators. Transparency of wholesale rates is therefore crucial if action to reduce them is taken and to enable regulators to monitor developments in the market so as to ensure that effective competition is emerging in the market.

Regulators may:

- ✓ have the authority to obtain wholesale IMRS rates charged by their national operators and share these rates when entering into bilateral or regional agreements.
- ✓ encourage the GSMA to publish headline (non-discounted) wholesale charges for international mobile roaming services (voice, SMS, mobile data).[97]

Substitutes

There are a number of potential substitutes which can be used by subscribers when roaming. As indicated above most are not perfect substitutes compared to a subscriber using their own terminal and domestic mobile

phone number. Nevertheless these substitutes can be useful in helping reduce the total charges a subscriber may face when visiting another country. Providing information on these substitutes, where to obtain them and their limitations can help empower users and instil some competition in the market. It needs to be recognised that it would be a difficult to maintain such a data base up-to-date.

- ✓ Regulators need to encourage the development and diffusion of substitutes to IMRS. They should ensure that operators do not prevent applications which can be used in roaming from being used on smartphones, laptops or other wireless devices.

- ✓ Regulatory/consumer authorities should provide a dedicated web site providing information on international mobile roaming substitutes including any drawbacks these substitutes may have.

- ✓ Regulators need to consider allowing the development of VoIP services and applications in their countries that can help in facilitating international mobile roaming services.

Regulators

One function of regulators is to require mobile service providers to be more transparent and to monitor that this is taking place. However, regulators themselves have an important role to play in the process of creating transparency and market competition.

In this context, regulators need to:

- ✓ encourage service providers to provide 'fixed' or 'flat' fee roaming services for mobile data roaming services which would allow them to better control their expenditure, understand the pricing structure and reduce the potential for "bill shock".
- ✓ encourage mobile service providers to structure their roaming charges on a zone basis so that it is easier for users to understand pricing structures.
- ✓ encourage operators to provide a data plan, with a spending limit, for roamers e.g. a per day/per week plan with a choice for the amount of data usage.
- ✓ require mobile operators to place a cap on data roaming and provide information when the user's usage is approaching the cap, allowing users to opt-out of the cap.
- ✓ require service providers to ensure that subscribers can obtain up-to-date information on their expenditures when roaming.
- ✓ set up a dedicated page on their web sites on international mobile roaming which provides up-to-date information on pricing and consumer related issues relevant to roaming.
- ✓ examine the potential to develop an independent "watchdog" type website at the international level on mobile roaming providing relevant information for users to consult.98
- ✓ pay to which either they or the relevant Ministry enters into.

4.2. Structural measures

There is a considerable consensus among government authorities that the dynamics of the international mobile roaming market are not conducive to the development of competition in this market and, as a result, there is a need to resort to structural measures in this market. In this context best practice would require the following measures:

- ✓ Where this has not occurred international gateways need to be liberalised.
- ✓ Subscribers should not be restricted from downloading applications on their terminal equipment that allow them to use alternative voice or messaging services when roaming.

- ✓ Separating (unbundling) the home and visited market. This implies that a subscriber can choose an international mobile roaming service provider before leaving the home country while maintaining an existing mobile number. This would be similar to the pre-selection process that was successful in creating competition in the fixed market for domestic and, in particular, international long distance.
- ✓ A complement to domestic unbundling of roaming service would be the concept of " local break out" for mobile data services allowing a visitor to choose a data service provider in the visited country to provide IMR services.[99]
- ✓ Creating international mobile roaming as a separate market implies that authorities allow domestic MVNOs to have access to network resources in the home market and agree with the authorities of visiting countries that these MVNOs have access to visiting country telecommunication markets on a non-discriminatory basis. This would allow MVNOs to have access to wholesale IMR offers.
- ✓ The international roaming service provider would need to have the capability to provide full international mobile roaming at a global level or at a regional level with significant country coverage.
- ✓ Bilateral agreements would need to be made open to third countries that agree to meet the same terms and conditions as the initial bilateral partners.

4.3. Bilateral, Regional and International agreements

Progress in resolving the high prices paid for the range of international mobile roaming services will only occur through appropriate bilateral, regional and/or international agreements. While the initial steps that are being taken in some of the bilateral and regional agreements are useful in lowering IMRS prices for users they will be insufficient to result in longer term competition in the market, that is competition which can be sustained without intrusive regulation. The EU Regulation III with its structural measures is moving toward a framework which will help such competition emerge. The earlier EU Regulation I and II were successful in lowering prices but clearly showed that, unless there was a desire to maintain continuous price regulation, steps were required to create conditions of competition in a market which was not contestable.

The WTO has taken an initial step in informally discussing international mobile roaming. Bilateral agreements and regional agreements should be encouraged but should be opened to other countries if they are willing, and able, to make the same commitments as the initial countries.

- ✓ Governments and/or government authorities which enter into bilateral or regional agreements to lower IMRS prices or eventually take structural measures to develop competition in IMRS markets need to ensure that they have the legal authority to enforce measures taken, monitor developments in IMRS markets and can enter into agreements with counterparts in other countries or at the regional level.

- ✓ Agreements need to be clear as to the responsibility of regulators, the methodologies to be followed and the data requirements for monitoring developments in IMRS markets.

The ITU can play an important role in developing and diffusing best practice regulation for IMRS among its members, and in particular acting as a forum to exchange experiences based on the lessons learned by those countries that have already moved forward and taken action to lower prices and develop competition in IMR markets.

ENDNOTES

[1] International Mobile Roaming Regulation - An Incentive for Cooperation, http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR08/discussion_papers/international_roaming_web.pdf

[2] OECD (2009), International mobile roaming charging in the OECD area, SAI/ICCP/CISP(2009)8/FINAL, Paris, 2009, http://www.oecd.org/dataoecd/41/40/44381810.pdf.

[3] See presentation by Peter Stuckmann, European Commission Information Society and Media directorate, EU Roaming Regulation - towards structural solutions, March 2012, Geneva, http://www.wto.org/english/tratop_e/serv_e/sym_march12_e/sym_march12_e.htm

[4] Smartphones are built around a mobile computing platform and support applications and provide Internet access.

[5] Cisco, for example has projected that global mobile Internet traffic will grow ten-fold from 2011 to 2016. See Cisco Visual Networking Index at http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html#~forecast.

[6] " Bill shock" refers to the negative reaction a subscriber has to receiving a high and unexpected request for payment from his/her company. As an example, see http://www.tgdaily.com/mobility-brief/59141-womans-200000-phone-charge-defines-bill-shock.

[7] http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2010.pdf

[8] See, OECD, Machine-to-Machine Communications: Connecting Billions of Devices, DSTI/ICCP/CISP(2011)4/FINAL, Paris 2012, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2011)4/FINAL&docLanguage=En

[9] http://imsresearch.com/news-events/press-template.php?pr_id=1875

[10] WTO data show nearly a threefold increase in world merchandise trade (in current prices) between 2000 and 2011

[11] The stock valuation of foreign direct investment during the 2000 and 2011 increased 3.4 times according to OECD data.

[12] See World Travel and Tourism Council *Business Travel: A Catalyst for Economic Performance* http://www.wttc.org/site_media/uploads/downloads/WTTC_Business_Travel_2011.pdf

[13] Tourism commitments have been made by over 125 WTO members, more than in any other services sector.

[14] *UNWTO World Tourism Barometer.*

[15] See ITU-T, COM 3-19-E, April 2002, Study Group 3, Contribution 19. INTUG argued that "... wholesale international mobile roaming charges are not cost-oriented and that home operators then add excessive charges before billing their retail customers. The wholesale prices are far from being cost-oriented. They are determined by administrative means, unrelated to costs and far from any competitive market." See also COM-R11-E, January 2003, REPORT OF THE FIFTH MEETING OF STUDY GROUP 3 HELD IN GENEVA FROM 9 TO 13 DECEMBER 2002, "The TAL Group fully supports the cost causation concept as the basis for determining rates for international traffic termination on mobile networks in all markets, and believes that in general, the costing elements are substantially the same for fixed line network termination and mobile network termination."

[16] Commission Recommendation On Relevant Product and Service Markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communication networks and services, http://ec.europa.eu/information_society/topics/telecoms/regulatory/maindocs/documents/explanmemoen.pdf

[17] In 1999 the European Commission decided to carry out an inquiry on international mobile roaming services recognising the problem of high charges -see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0382:EN:NOT

[18] An excellent technical description of international mobile roaming is provided in the 2008 GSR ITU paper, *op.cit*.

[19] For example, in the United States where Receiving Party Pays is used termination rates are very low resulting in very high volume of calls per subscriber. See Figure 6, OECD, Developments in Mobile Termination, DSTI/ICCP/CISP(2013/FINAL, http://dx.doi.org/10.1787/5k9f97dxnd9r-en.

[20] BEREC (the Body of European Regulators of Electronic communication notes that in reviewing the impact of price caps in the European economic Area on IMR charges that "[t]here are no clear indications that operators have tended to raise the prices of unregulated „Rest of World" roaming calls to make up for lost revenue due to the regulated price caps." Paragraph 1.12, International Roaming BEREC Benchmark Data Report January 2011-June 2011, BoR(11)51.

[21] For example, see www.free.fr

[22] op.cit.

[23] OECD (2009), *op.cit*.

[24] BEREC, op.cit., paragraph 1.23.

[25] The GSMA has indicated that they are in the process of allowing MVNOs to use standard documents such as STIRA

and presumably participate fully in the GSMA system.

[26] A contestable market is one where there is freedom of entry and exit in the market and the threat of competition is sufficient to keep prices low and prevent the abuse of monopoly power.

[27] If country *A* residents are not regular visitors to country *B* there is little benefit from declining IMRS prices in country *B*.

[28] Department of Broadband, Communications and the Digital Economy, Report of findings on: International Mobile roaming charges, June 2008, http://www.dbcde.gov.au/__data/assets/pdf_file/0005/86369/KPMG_Report_of_findings_on_International_Mobile_roaming_charges.pdf

[29] A contestable market is one where there is freedom of entry and exit in the market and the threat of competition is sufficient to keep prices low and prevent the abuse of monopoly power.

[30] If country *A* residents are not regular visitors to country *B* there is little benefit from declining IMRS prices in country *B*.

[31] WIK-Consult, Final Study Report, Study for the European Commission, Study on the Options for addressing Competition Problems in the EU Roaming Market, SMART 2010/0018, page 6, http://ec.europa.eu/information_society/activities/roaming/docs/cons11/wik_report_final.pdf

[32] See the background report to the ITU workshop on Origin Identification and Alternative Calling Procedures, March 2012 and summary report at: http://www.itu.int/ITU-T/worksem/oi-acp/index.html.

[33] The ITU reported (see background report in endnote 32) that at the end of that period 2004-2009 92 countries allowed VoIP while only 49 banned it outright; the remainder either had no regulatory framework for VoIP or allowed it only in a wholesale or restricted form while the number of countries "legalizing" VoIP doubled over the period, from 46 in 2004 to 92 five years later.

[34] GSMA, "Roaming Services in Latin America", Market and technical Approach, IIRSA Workshop, Bogota,

Colombia, 7 November 2008, www.iirsa.org/BancoMedios/Documentos%20PDF/tir_bogota08_medidas_tecnicas.pdf.

[35] International Telecommunication Regulations, http://www.itu.int/osg/csd/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf.

[36] OECD (2009). DSTI/ICCP/CISP(2009)8/FINAL, International Mobile Roaming Charging In The OECD Area, Paris, 2009.

[37] Moving away from IOTs would not in itself have an impact on the GSMA which plays an extremely useful role in other areas in terms of standardisation, helping developing economies improve their roaming capabilities and in facilitating billing, etc.

[38] IMSI or international mobile subscriber identity numbers are embedded on SIM cards and used to identify the subscriber.

[39] http://www.interfone.com/frontpage.php

[40] The International Mobile Subscriber Identity is a unique identification associated with a mobile user and used to send details of the mobile to the network including details of the mobile to the Home Location register or to the Visitor Location Register (when roaming).The IMSI determines whether a subscriber can use a particular network and used to obtain the subscriber's data.

[41] http://www.gentay.co.uk/newsandpr.php?category=News

[42] See www.holidayphone.com

[43] http://www.flexiroam.com/

[44] https://www.roamline.com/

[45] http://www.roammobility.com/

[46] http://www.transatel-mobile.com/

[47] See Sutherland, Ewan, International mobile roaming in Africa, Link Public Policy Research Paper No. 10, March 2010, http://link.wits.ac.za/papers/Sutherland-2010-mobile-roaming-africa.pdf

[48] In early 2010, Zain accepted an offer for the sale of all its Africa operations to Bharti Airtel which still operates the *One Network* in Africa.

[49] Zain Press Release at: http://www.zain.com/muse/obj/lang.default/portal.view/content/Media%20centre/Press%20releases/One%20Network%2012%20countries

[50] It should be noted that the percentage of population roaming in the *One Network* region compared to Europe is much lower as is the revenue generated by roaming relative to total moile service revenues.

[51] http://www.thenationonlineng.net/2011/index.php/business/infotech/48384-will-subscribers-get-cheaper-roaming-charges.html

[52] http://www.gsma.com/newsroom/gsma-launches-data-roaming-transparency-initiative/

[53] http://www.itu.int/en/ITU-T/studygroups/com03/Pages/results.aspx

[54] ITU-T, Draft new Recommendation ITU-T D.98, Charging in International Mobile Roaming Service, 16-20 January 2012, TD 227 Rev.2 (PLEN/3)-E.

[55] For more information on WICT12 and ITRs see: www.itu.int/en/wcit-12/Pages/default.aspxs, See the background paper on international mobile roaming at: www.itu.int/en/wcit-12/Documents/WCIT-background-brief10.pdf :.

[56] OECD (2009), *op.cit.*

[57] OECD (2009a), International Mobile Roaming Services: Analysis And Policy

Recommendations, DSTI/ICCP/CISP(2009)12/Final, Paris 2010.

[58]OECD, 16 February 20102, Recommendation of the Council on International Mobile Roaming Services, Paris 2012, http://webnet.oecd.org/OECDACTS/Instruments/ShowInstrumentView.aspx?InstrumentID=271&InstrumentPID=276&Lang=en&Book=False.

[59] Telecompetition, Towards a single Nordic market for telecommunication services, Report from the Nordic competition authorities, No. 1/2004, http://www.kilpailuvirasto.fi/tiedostot/telecompetition.pdf

[60] op.cit., page 10.

[61] Consumers can select a different cut-off limit or opt out of this bill shock safeguard entirely. Operators will be obliged to send a message (SMS, e-mail or pop-up message) to customers informing them of how much it will cost to surf the net via their mobile devices when they use roaming services in addition to the alert message warning customers when they have used 80% of their agreed limit.

[62] Regulation (EC) no. 717/2007 of the European Parliament and of the Council of 27 June 2007, amended by (Regulation (EC) no. 544/2009 of 18 June 2009).

[63] Allowing subscribers to choose an IMR carrier different to their domestic carrier is similar to carrier pre-selection which was introduced in the early days of competition in fixed networks. Pre-selection allowed subscribers to choose in advance an alternative carrier to carry their calls (usually long distance and international) without having to dial a special number of install specific equipment.

[64] See http://ec.europa.eu/information_society/activities/roaming/regulation/archives/current_rules/index_en.htm

[65] See, Ms Maitha Ali Jaffar, Telecommunications Regulatory Authority Sultanate of Oman, presentation at the IMR Symposium, Geneva, 22 March 2012, GCC International Roaming Regulatory Initiative, ww.wto.org/english/tratop_e/serv_e/sym_march12_e/presentation_%20maitha_jaffar.pdf

[66] ibid.

[67] http://arabnews.com/economy/article574768.ece

[68] See, http://www.crasa.org/

[69] Regulatory Impact Assessment Study SADC Home and Away, 23 April 2010, Ref. 15493-154, available at http://www.crasa.org

[70] See, Christian Mhlanga, presentation at the IMR Symposium, Geneva, 22 March 2012, A South African Perspective On International Mobile Roaming, www.wto.org/english/tratop_e/serv_e/sym_march12_e/presentation_mhlanga.pdf - 2012-03-29 -

[71] International Telecommunication Union, West African Common Market Project: Harmonization of Policies Governing the ICT Market in the UEMOA-ECOWAS Space Interconnection, 2004, http://www.itu.int/ITU-D/treg/projects/itu-ec/Ghana/modules/FinalDocuments/Interconnexion.pdf

[72] See Rupa Ranganathan and Vivien Foster, *ECOWA's infrastructure: a regional perspective*, The World Bank

Africa Region, Sustainable Development Unit, Policy Research Working Paper 5899, December 2011, " *The national members of the West Africa Telecommunications Regulators Association (WATRA) communicate regularly to keep abreast of telecom issues in the region and share information. The existence of this relatively developed institutional structure has helped to facilitate the roaming arrangements that are*

observed in the region.", page 59, http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2011/12/05/000158349_20111205145616/Rendered/PDF/WPS5899.pdf

[73] Commission de l'Union Africaine, Pré-étude de faisabilité pour le développement d'un programme pour la mise en place de tarifs de roaming abordables en Afrique, Synthèse, Juin 2011, http://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/Cotonou-12/pdf/Session6_1_Guellouz.pdf

[74] http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx

[75] APT Working Group Report, 15 May 2012, http://www.apt.int/sites/default/files/2012/05/APT_IMR_Working_Group_Report_Final.pdf

[76] See, Joint Ministerial Statement of the 11th ASEAN Telecommunications and IT Ministers Meeting and its Related Meeting with External Parties Myanmar, 9 December 2011, http://www.aseansec.org/25751.htm

[77] See *Evolving Towards Asean 2015*, Asean Annual Report, 2011-12,, http://www.aseansec.org/documents/annual%20report%202011-2012.pdf

[78] http://www.thejakartaglobe.com/tech/indonesia-wants-roaming-free-mobile-phone-coverage-in-asean-by-2014/537512

[79] See, http://www.slmission.com/statements/88-ministry-statements/109-colombo-declaration-of-the-15th-saarc-summit.html

[80] Regulatel is the Latin American Forum of Telecommunication Regulatory Entities (Foro Latinoamericano de Entes Reguladores de Telecomunicaciones) which created a Working group on Roaming in 2012. CITEL the Inter-American Telecommunication Commission**,** is an entity of the Organization of American States and the region's intergovernmental telecommunication advisory body. Mercosur, or Southern Common Market, is an economic and political agreement among Argentina, Brazil, Paraguay and Uruguay. CAN is the Andean Community (Comunidad Andina) which is a customs Union between Bolivia, Columbia, Ecuador and Peru. IIRSA is the Initiative for the Integration of the South American Regional Infrastructure created in September 2000 during a meeting of Presidents from the 12 official South American countries (Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Guyana, Paraguay, Peru, Suriname, Uruguay and Venezuela) aimed at the integration of the physical infrastructure in South America to promote economic growth throughout the region.

[81] http://www.iirsa.org/BancoConocimiento/R/roaming_suramericano/roaming_suramericano_ENG.asp?CodIdioma=ENG

[82] http://www.iirsa.org/BancoConocimiento/R/roaming_suramericano/roaming_suramericano.asp?CodIdioma=ESP

[83] http://www.gov.ms/wp-content/uploads/2011/02/Draft-RDdS-Nov-2010.pdf

[84] The Infocomm Development Authority of Singapore (IDA) and the Malaysian Communications and Multimedia Commission (MCMC).

[85] The Info-communications Development Authority of Singapore and the Authority for Info-communications Technology Industry of Brunei Darussalam were charged with examining roaming charges between the two countries and reaching an agreement with the operators on lower charges.

[86] See Trans-Tasman mobile roaming Discussion document May 2010, http://www.dbcde.gov.au/__data/assets/pdf_file/0008/127709/Trans-Tasman_mobile_roaming_discussion_document.pdf

[87] See Dr. Assaf Cohen, Widening the EU Roaming Zone, Vienna, April 23, 2008, http://www.moc.gov.il/sip_storage/FILES/5/1375.pdf

[88] *Most Favoured Nation(MFN) treatment is an obligation under the General Agreement on Trade in Services (Article II) which requires that a signatory accords "...* immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country*"(Article II, 1.). Common markets, customs unions, and free trade areas, however, are exempt from MFN provisions,http://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.*

[89] See for example, Sydney Morning Herald | July 18, 2011, **Hitch in bid to curb phone roaming costs** by Lucy Battersby, " FEDERAL [Australian Government] attempts to reduce global-roaming fees between Australia and New Zealand could be stymied by a free-trade agreement with the United States. The Department of Foreign Affairs and Trade is investigating if the introduction of price caps on mobile roaming fees will have an impact on the free-trade agreement with the US and agreements with Pacific countries. DFAT is concerned that under the US treaty Australian carriers may have to offer US visitors lower rates but Australians would not receive the same treatment there. Advertisement: Story continues below ''DFAT is working with the Department of Broadband, Communications and the Digital Economy on a range of issues in relation to international mobile roaming and Australia's international trade obligations,'' a departmental spokeswoman said.

[90] OECD (2010) op.cit., page 29.

[94] See OECD, Recommendation of the Council on International Mobile Roaming Services (C2012)7, Paris 2012, at http://webnet.oecd.org/OECDACTS/Instruments/ShowInstrumentView.aspx?InstrumentID=271&InstrumentPID=276&Lang=en&Book=False

[95] It needs stressing that many users (prepaid and postpaid) purchase a package of calls (e.g. number of hours) and would not necessarily be familiar with how much they pay per minute for their domestic mobile calls so that comparisons with domestic and international prices may be difficult for them. The use of per minute pricing for international mobile roaming charges in certain cases, instead of per second pricing, also increases the cost to users.

[96] Regulation I of the EU imposed for outgoing calls a per second billing interval after the 31st second and per second for incoming calls.

[97] Transparency of international accounting rates played an important role in fostering competition and reducing prices for international long distance calls in the fixed voice market.

[98] See APEC Guidelines, op.cit. APEC recognised the difficulty in maintaining such as site for the APEC members. At the International level this would be difficult.

[99] The EU Regulation III requires that, from July 2014, mobile operators in visited countries have the possibility to directly offer data roaming services to foreign roamers on their own networks.

GSR 2012 Discussion Paper

Blurring Boundaries:

Global and Regional IP Interconnection

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 19 October 2012.

TABLE OF CONTENTS

BLURRING BOUNDARIES: GLOBAL AND REGIONAL IP INTER-CONNECTION

Author: Dennis Weller, Senior Advisor, Navigant Economics

1. Introduction

The growth of the Internet since it was made commercially available in the early 1990s has been perhaps the most influential economic and social event of our time. The volume of IP traffic exchanged in 2010 was 1,200,000 times greater than in 1994.[1] This growth has been intensive: twenty households with average levels of Internet usage today generate more traffic than the entire Internet carried in 1994. Growth is also extensive, as broadband take-up has increased and the geographic reach of the Internet has expanded around the world. The Internet has created unprecedented opportunities for development, while at the same time challenging firms and governments by disrupting older business models and policy frameworks. Internet penetration, however, varies widely around the world, with much lower rates in developing countries (typically 10 times lower than mobile penetration rates).

The success of the Internet has been made possible by many factors, including the development of an efficient global market for connectivity through commercial agreements for the exchange of IP traffic. The basic model of peering and transit is now so well understood that the vast majority of peering agreements can be concluded on a handshake basis, without the need for a written document. The IP traffic exchange model has evolved over time to meet the needs of the Internet community. That process of adaptation is continuing today as new patterns of use drive structural change in the Internet ecosystem. This paper will review the current state of the market, and the forces that are likely to challenge it in the future.

As the Internet converges with, and displaces, older models of communication, the IP model of traffic exchange collides with the regulatory framework designed to promote policy goals in the traditional environment. This paper will examine the challenges faced by policy makers seeking to achieve those goals in the new environment, without interfering with the creativity, efficiency, and openness that has allowed Internet to deliver benefits to more than two billion users. Particular emphasis will be placed on the process of extending those benefits in greater measure to emerging economies through the development of the Internet ecosystem in-country and in-region.

2. Development of the IP market

2.1 Growth

From 1994 to 2010, the average annual growth in Internet traffic was about 140 per cent per year. Over the last five years of that period (1996-2010) traffic grew eightfold, or an average of about 50 per cent per year.[2] While the rate of growth has moderated, it is still remarkable for a system as big as the Internet has now become. For the period 2011-2016, Cisco forecasts that traffic will increase by a factor of four, to a total in 2016 of 1.3 zettabytes.[3]

As shown in Figure 1, Cisco predicts that that mobile data will be the fastest growing type of Internet traffic, at a compound annual growth rate (CAGR) of 78 per cent. By region, North America and Europe are expected to grow at 22 and 27 per cent, respectively. Traffic in the Asia-Pacific region, which is about equal to North America today, is forecast to grow at 31 per cent, and will thus be half again as great as that of North America by 2016. Other regions are forecast to make up ground through still faster growth.

Figure 1: Global IP Traffic, 2011-2016

IP Traffic, 2011–2016							
	2011	2012	2013	2014	2015	2016	CAGR 2011–2016
By Type (PB per Month)							
Fixed Internet	23,288	32,990	40,587	50,888	64,349	81,347	28%
Managed IP	6,849	9,199	11,846	13,925	16,085	18,131	21%
Mobile data	597	1,252	2,379	4,215	6,896	10,804	78%
By Segment (PB per Month)							
Consumer	25,792	37,244	47,198	59,652	76,103	97,152	30%
Business	4,942	7,613	9,375	11,227	13,130	7,613	22%
By Geography (PB per Month)							
North America	10,343	14,580	17,283	19,796	23,219	27,486	22%
Western Europe	7,287	10,257	13,026	16,410	20,176	24,400	27%
Asia Pacific	10,513	14,792	18,976	24,713	31,990	41,105	31%
Latin America	1,045	1,570	2,333	3,495	5,208	7,591	49%
Central and Eastern Europe	1,162	1,673	2,290	3,196	4,419	5,987	39%
Middle East and Africa	384	601	903	1,417	2,320	3,714	57%
Total (PB per Month)							
Total IP traffic	30,734	43,441	54,812	69,028	87,331	110,282	29%

Source: Cisco VNI,2012

2.2 Performance

The global market for IP connectivity has performed very well over time. It has produced lower prices, directed resources efficiently, called forth the investments necessary to keep up with the dramatic growth in traffic, and enabled the extension of the Internet to users around the world. The growth of peering, reductions in transit prices, proliferation of exchange points, and the development of content delivery networks (CDNs) have combined to reduce the cost and increase the quality of internet connectivity. If the connectivity necessary to carry the volume of traffic the Internet handled in 2010 were priced at the wholesale interconnection rates in effect in 1994, the global bill would be USD 16 Trillion, or slightly more than the GDP of the United States.

Prices for transit service have declined every year. Transit can now be purchased in larger markets for about two USD per megabit per month, depending on volume and other terms of the agreement, with some prices as low as USD 0.50. To put this into perspective, and to permit a crude comparison with price levels familiar in the traditional telecom space, these prices can be stated in the form of a per minute wholesale rate for the global transport and termination of voice traffic to any customer in the world. Even at the higher figure of USD 2, the voice equivalent would be about USD 0.0000008, at least five orders of magnitude lower than wholesale rates common in traditional telecom markets. This reflects in part the efficiency of IP networks, but also the fact that IP markets for the exchange of traffic have performed far better than those for traditional circuit-switched (TDM) traffic.[4] But transit prices also vary substantially by location and volume, reflecting differences in the weighted average distance the traffic must travel, scale economies, and market conditions in-region. These factors will be discussed in a later section of this paper, the experience of different countries will be reviewed, and best practices to address these challenges will be considered.

For a time after the telecom bubble burst in 1999-2000, some observers feared that the decline in transit prices was a temporary phenomenon driven by the excess capacity built up during the previous boom. It's now clear that these low prices are a long-term, sustainable trend that has been maintained for many years. As will be discussed below, investment has been forthcoming in recent years to build new Internet assets, including long-haul undersea cables.

2.3 Structure

The market for IP connectivity has evolved continuously over time, driven by changes in patterns of use (discussed below) and by the need to minimize costs and improve quality.

Peering. Through the continued expansion of peering**,** Internet Service Providers (ISPs) have disintermediated transit providers, reduced their transit expense, and increased their ability to deliver traffic directly to other networks.[5] The vast majority of Internet traffic now completes without touching any of the major backbone networks.

A recent survey of ISP networks gathered information about Internet peering agreements.[6] Responses were received from 4,331 different ISP networks, or approximately 86 per cent of the world's Internet carriers, incorporated in 96 countries, including all 34 members of the OECD and seven of the UN Least Developed Countries. Information was collected on 142,210 peering agreements.

The survey results indicate a highly developed market in which the terms of basic peering agreements are well known, and transaction costs are kept to a minimum. Only 698 of the agreements in the sample (0.49 per cent) were formalized in written documents. The other 141,512 (99.51 per cent) were "handshake" agreements in which parties agreed to commonly understood terms without creating a written document. Almost all of the agreements (99.73 per cent) had symmetric terms and were settlement-free. Only 374 agreements (0.27 per cent) included asymmetric terms such a compensation (or "paid peering") or minimum peering requirements imposed by one party on the other.

A surprising result of the survey was the prevalence of multilateral agreements, in which many ISPs meeting at an interexchange point (IXP) join a single agreement, rather than establish bilateral agreements with each of the other parties. The majority of the Autonomous System pairs observed in the sample were connected through multilateral agreements. The use of multilateral agreements can further reduce transaction costs. In some IXPs, a network is required to join the multilateral agreement as a condition of joining the exchange.

Figure 2: Probability of selection of a country of governing law; ten most likely and ten least-likely countries

Source: Woodcock and Adhikari

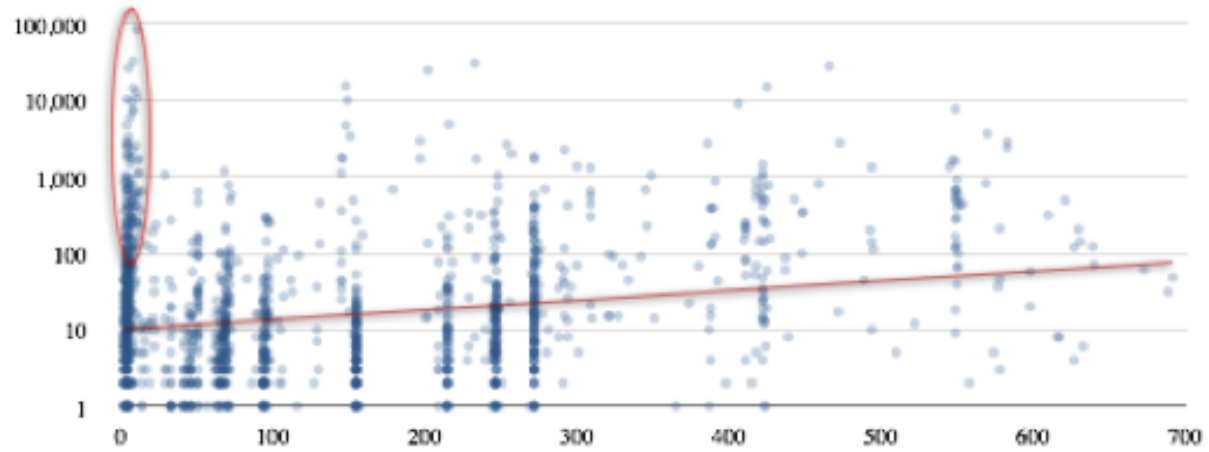
Peering agreements generally specify a country whose laws will govern in the event of a dispute between the parties. Within the sample, the country of governing law in every case was also the country in which at least one of the parties was based. In other words, unlike some other markets (such as ocean shipping, for example) there does not appear to be any "third party" country that attracts firms not incorporated there to employ its legal framework for this purpose. However, the data do show clear preferences, with some countries being more likely to be chosen if one of the parties is incorporated there, and others less likely. Figure 2 shows the ten countries with the highest probability of being chosen, and the ten least likely. In nearly every agreement in which one of the parties is incorporated in the US or Canada, that country is selected as the country of governing law. On the other hand, there are

some countries in which no agreements in the data set were selected for an agreement where one of the parties was incorporated outside this group, due to the the unattractiveness of their legal frameworks..

Networks may pursue different interconnection strategies. Figure 3 shows a distribution of the networks included in the survey, by the number of prefixes each network advertises (on the Y-axis) and the number of interconnection partners each network has reported (on the X-axis). The vertical cluster to the left of the Figure (circled in red) includes most of the large incumbent and global backbone networks. These large networks reach a wide universe of prefixes, but do so using a very limited set of interconnection partners. Outside this group, the red trend line on the Figure shows the number of interconnection agreements increasing as a network advertises more prefixes. These networks make increased use of peering to obtain the connectivity they need, and to reduce their reliance on transit. There is an interesting contrast between the older, "tier 1" networks, and large content-distribution networks (CDNs). CDNs that are comparable in size to the large tier 1 carriers have very broad interconnection arrangements, in terms of both the number and the geographic diversity of their interconnection partners. In this they follow the trend line on the Figure much more closely than do the Tier 1 carriers. This represents a clear difference in strategy, as well as the success that large CDNs have had in negotiating peering agreements with local access ("eyeball") networks. Finally, the other vertical clusters in Figure 3 represent multilateral peering agreements at large IXPs. The Hong Kong Internet Exchange, for example, has 144 participants.

Since peering and transit are substitutes for one another, as networks grow, as the price of transit falls, and as the costs of implementing peering arrangements change, these networks may adjust the amount of transit they buy, and "groom" their peering agreements, to roughly equate the cost at the margin of peering and transit in order to minimize their overall cost of connectivity. Both peering and transit are subject to scale economies. The cost of peering will generally fall as increasing volume allows the physical arrangements for peering to be utilized more efficiently. The cost of transit will generally fall with contract commitments for larger volume and a longer term.

Figure 3: Number of advertised prefixes (Y-axis) over number of interconnection partners (X-axis) per carrier



Source: Woodcock and Adhikari

Internet Exchange Points (IXPs). Two IP networks can meet and exchange traffic at any point they choose. However, by establishing a common point where multiple networks can meet it is usually possible to achieve greater scale and scope economies and reduce transaction costs. This is done through the use of IXPs.

When the Internet was first made commercially available it was very US-centric, and much of the traffic generated by European networks had to travel to the US to be exchanged, even if the traffic was addressed to a terminating point in Europe. This round-trip process, called "tromboning" adds cost and reduces quality by adding to the delay in transmission, or latency. As the Internet grew in Europe, and IXPs were established there, the need for tromboning diminished, and European IXPs became magnets for investment in Internet assets. Today, Europe has 137 IXPs, including seven of the ten largest in the world. Similarly, as Internet activity has grown in Eastern Europe, the center of gravity has moved eastward, with large IXPs in cities like Prague and Sofia. At the same time, a similar process was taking place in the more developed countries of Asia-Pacific.

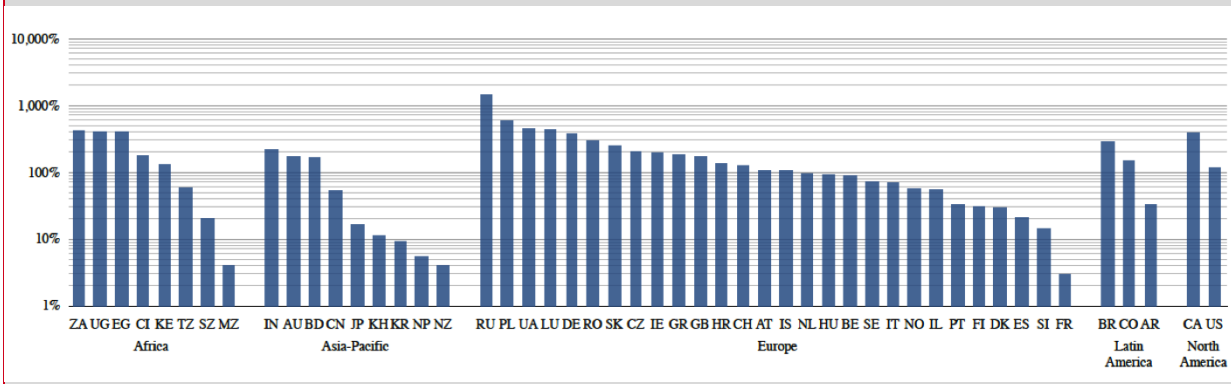
As the Internet has grown extensively in different regions around the world, this process of developing Internet resources and scale in-region has been repeated, with IXPs playing a key role. If there is not a convenient exchange point where traffic can be exchanged in-country or in-region, then traffic between two local subscribers may be tromboned to a distant exchange. For example, traffic within a Latin American country may be exchanged in Miami, or traffic local to a country in sub-Saharan Africa may be exchanged in Amsterdam.

The establishment of an IXP in-country or in-region can become part of a virtuous circle of investment and development of Internet assets. To the extent that local traffic can be exchanged at a convenient IXP, transit expenses can be reduced, and capacity on undersea cables can be used for long-haul traffic that needs it. Quality is improved when the route-miles the traffic must traverse, and the number of "hops," are reduced, thereby reducing latency. Research has shown that uptake of broadband and the usage of latency-sensitive applications, such as VoIP and video, increases when latency is reduced.[7] In this way, improvements in quality made possible by more direct routing can translate into increased domestic demand and revenues for ISPs and content providers.

The availability of a convenient domestic hub with access to domestic networks can also create incentives for global networks, CDNs, and content providers to establish a presence at the in-country ISP. Google, for example, has invested in caches to localize content in emerging economies. Similarly, domestic websites who have previously paid web hosting fees and transit to have their sites hosted abroad can save those costs, and increase quality, buy having them hosted locally. Having a convenient point nearby to drop off traffic may give domestic networks greater flexibility to optimize their routing and balance responsibility for transport costs when peering with international networks. By aggregating traffic at an IXP, participants may be able to negotiate better terms on larger purchases of transport services, and attract additional investment in domestic transport. Localizing the exchange of domestic or regional traffic at an IXP also protects those communications from the possibility of any interruption of service on undersea cables. Having a convenient point nearby to drop off traffic may give domestic networks greater flexibility to optimize their routing and balance responsibility for transport costs when peering with international networks. The development of Internet assets in-country can also encourage investment in complementary business development and investment in domestic access networks, IT-related businesses, and domestically-produced content. The availability of an IXP may also facilitate efforts by government to deliver services online.

An IXP cannot produce miracles by itself. For example, if participation in a domestic IXP is very costly, and domestic transport to reach that IXP is limited and expensive, then it may still be cheaper to trombone the traffic for exchange at a distant point. But an IXP can play an important role in a larger process of liberalization and market development.

Figure 4: Annualized percentage growth in domestic Internet Bandwidth production, grouped by region, 2005-2010



Source:Weller and Woodcock (2012), based on data from Packet Clearing House

At the other extreme, it is possible for a region to be oversupplied with IXPs, and some observers believe that this might be the case in Europe today. While having convenient points to aggregate and exchange traffic may reduce costs, as IXPs proliferate within a region it becomes more difficult for each of them to reach an efficient scale, resources are spent on transport links among them and ports for those links, and for any given network the cost of maintaining a presence at multiple IXPs may become burdensome. For similar reasons, in emerging economies where traffic volumes are initially low, it may be more useful to think in terms of regional IXPs where traffic from

neighboring countries can be aggregated and exchanged, and the development of regional, cross-border transport arrangements may be important to allow such an IXP to succeed.

IXPs, more than 350 in all, have now been created in many countries around the world.[8] Yet more than half the countries in the world still have no IXP within their borders.[9] Figure 4 shows the growth of IXPs in different countries, grouped by region. Domestic Internet bandwidth production is a measure of the aggregate cross-section capacity of the switching fabrics of the IXPs within each country. The annualized growth rates in that measure over the five years 2005-2010 range from less than 20 per cent to 1,470 per cent (in Russia). Several african countries, including South Africa, Uganda, and Egypt, grew at more than 400 per cent.

Content Delivery Networks. Over the last decade, a new category of service provider has developed on the Internet -- the content delivery network, or CDN. A CDN provides resources to enhance the quality of delivery for Internet content. The two main quality-enhancing elements are more direct routing, to reduce distance and the number of hops, and the caching of content close to the recipient of the content. Caching reduces latency by allowing frequently-accessed content to be stored nearby, and reduces transport costs by limiting the need to retrieve the content repeatedly from a remote source.

Stand-alone CDNs like Akamai and Limelight were early, and very successful, providers of these services. A 2009 study by Atlas Internet Observatory estimated that the top five "pure-play" CDNs -- Limelight, Akamai, Panther, BitGravity, and Highwinds -- represented 10 per cent of Internet traffic.[10] Total CDN traffic has increased from 20-30 per cent of the traffic on Internet backbones in 2010 to 35-45 per cent in 2012. Today it is more helpful to think of CDN functionality as a business in which many providers participate, including stand-alone CDNs, content aggregators like Google, backbone companies like Level 3, and local access providers including incumbent telcos and cable companies. Google self-provides CDN services on a very large scale, becoming in the process the second-largest network on the Internet. Netflix is one of the largest providers of online movies in the US, and is rapidly expanding into other countries. It has been a customer of CDNs like Akamai and Level 3 to deliver the billion hours of video it streams every month. In June of 2012 it announced its own CDN, called Open Connect, which already carries 5 per cent of its traffic.[11] YouTube, another large online video provider now owned by Google, has had a similar arrangement for some time. Recent acquisitions by backbone companies appear to have been motivated, at least in part, by the CDN businesses of the acquisition targets. This would include Level 3's purchase of Global Crossing, and Tata's purchase of BitGravity.

The rise of CDNs has been driven by, and has also supported, the change in the services provided over the Internet described in the next section. As the mix of services has shifted, and as those services as well as CDN functions have been supplied by different entities, the distinctions between backbone networks, access networks, and media companies have blurred. For example, Comcast's role in this universe has changed substantially in a short time. In 2007 it was primarily a local cable operator, lacking its own backbone facilities, mainly focused on residential video and broadband services and highly dependent on upstream transit suppliers. By 2009 it had become a major provider of voice services, a net exporter of traffic, the sixth largest network by traffic volume, and the largest user of IPv6 addresses on the Internet.

CDNs have, like the growth in peering, changed the topology of the Internet, flattening its structure, providing more direct delivery of traffic, and further disintermediating the providers of transit. While the market for Internet connectivity is often described as a hierarchical world with a rigid structure of Tier 1 and Tier 2 carriers, that picture is no longer accurate. As will be discussed below, the development of CDNs has set up an interesting process of negotiation to reset the terms of trade for the various parties along the value chain between content creators and local access networks. Through that process, the market for IP traffic exchange is beginning to generate answers to many of the questions raised in the debate surrounding net neutrality.[12]

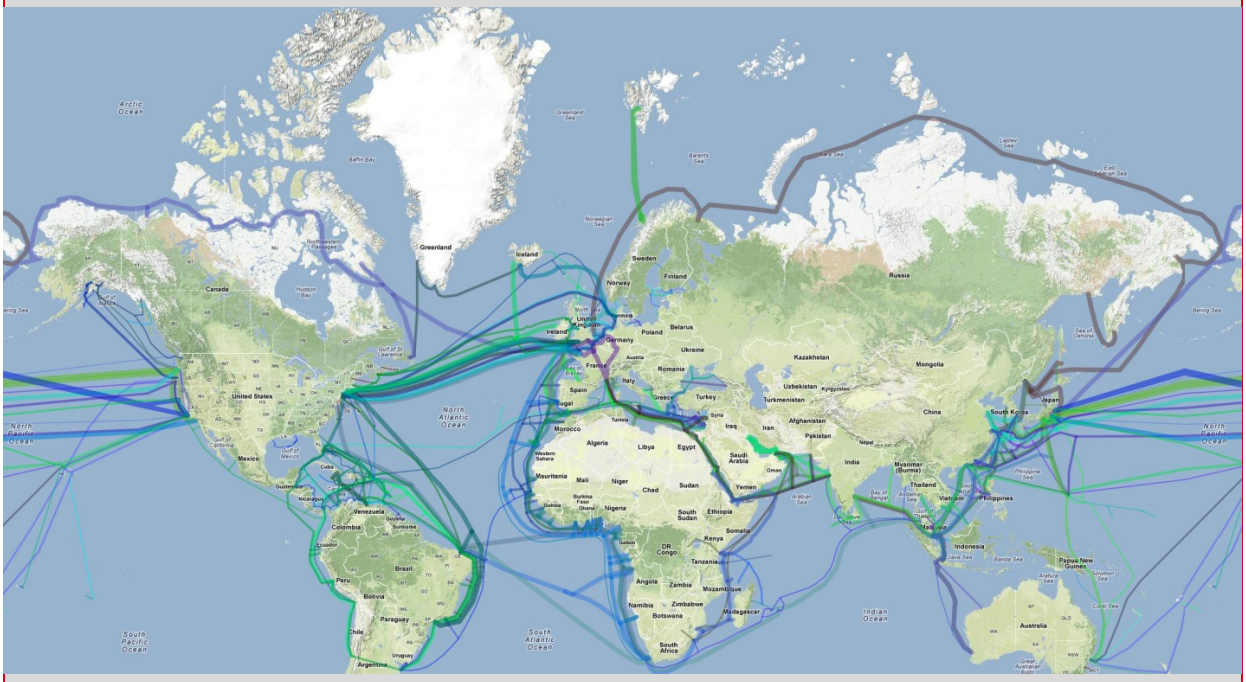
For emerging economies seeking to create a virtuous circle of investment and growth, CDNs present some new opportunities for partnership. The purpose of a CDN is to deliver content directly to the terminating access network. They therefore provide the transport to a point in or near the terminating network, thus covering what has been a significant cost for networks in developing countries. They provide alternatives to the transit providers, yet they are not in the transit business. Google, for example, does not seek, or accept, traffic from other networks. Its model is to peer with the terminating network, rather than to charge it for transit. The percentage of Google traffic delivered via direct peering increased from 30 per cent in 2008 to over 60 per cent in 2011.[13] The willingness of

large CDNs to peer with smaller networks, and to invest in caches in IXPs within developing countries, makes them potentially significant players in building a critical mass of Internet resources. At the same time, they represent a source of countervailing bargaining strength to offset the positions of incumbents in both developed and developing regions.

Investment in Internet facilities. In order to accommodate the rapid growth in Internet traffic, large investments in network facilities have been necessary. These include investments in routers, transport facilities, and switching fabrics in IXPs, and other things, in all regions. What is most interesting from a structural point of view has been the ongoing investment in long-haul facilities, particularly in undersea cables, around the world.

While the trans-Atlantic market had been well-served by cables for some time, the development of cable capacity across the pacific had lagged behind the growth of Asian markets, leaving them limited in capacity and route diversity. For many regions, such as Africa and Latin America, the limited availability of undersea cable capacity led to high rates, both for leased lines and for transit, a problem exacerbated in many cases by the tromboning of local traffic, which placed additional demand on the scarce resource.

Figure 5: Undersea cable routes, 2012

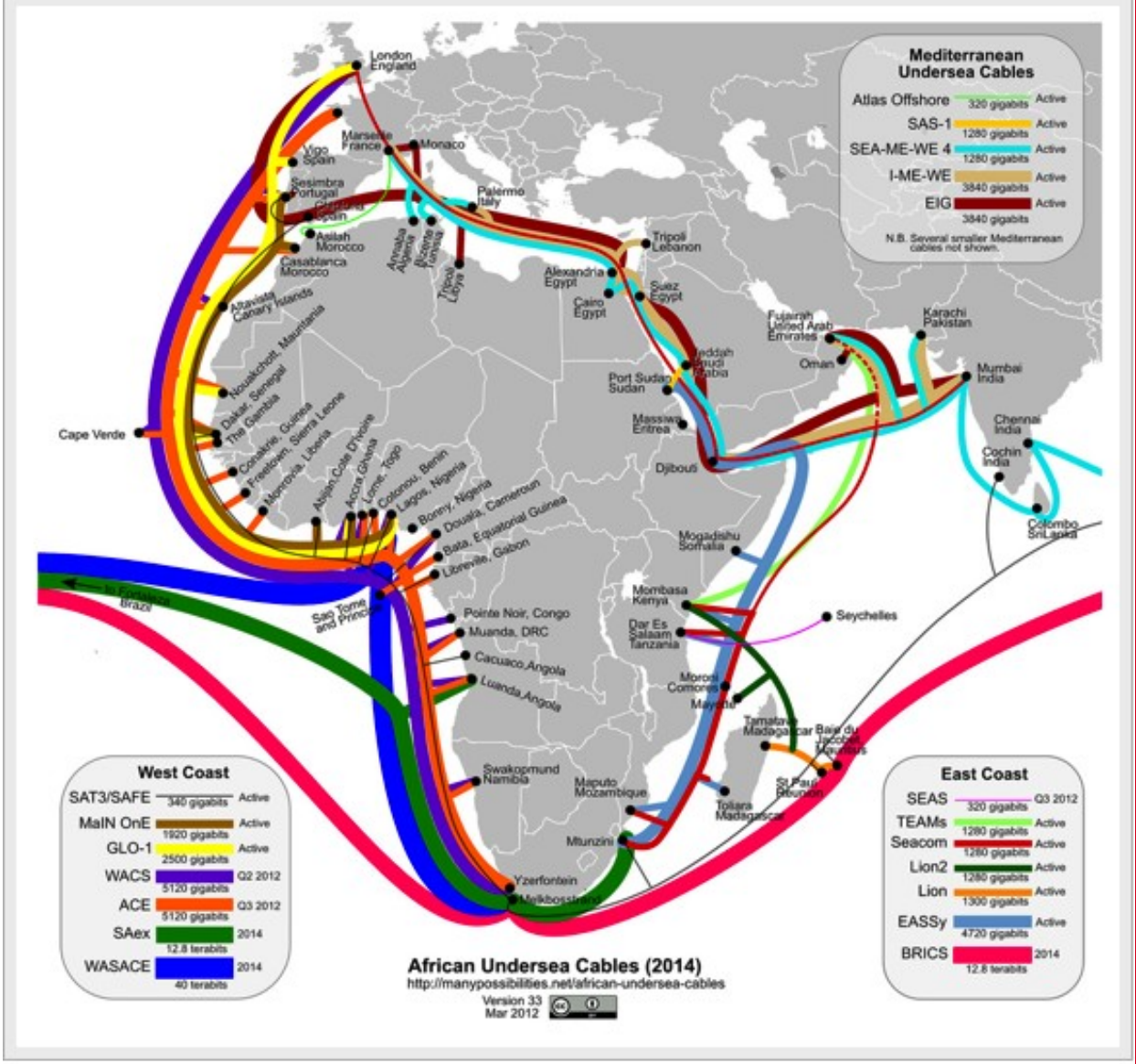


Source: Greg's Cable Map, http://www.cablemap.info

However, ongoing investment in new undersea cable projects, which has continued to a considerable degree even through the recent financial crisis, has begun to create additional capacity, route diversity, and competition in many regions. A global view of undersea cable routes is shown in Figure 5.[14] While much remains to be done, significant progress has been made which, together with other developments such as the creation of IXPs, has led to better performance in many markets. In 2010 and 2011, 19 new undersea cable systems representing an estimated investment of USD 3.7 Billion were deployed. Plans have been announced for 33 additional systems to be placed in 2012 and 2013, estimated to cost USD 5.5 Billion. Estimated construction costs for 2010-2013 by region are shown in Figure 7; note that the largest aggregate investment over the period will be around Africa.[15]

For example, the Trans-Pacific Express, the first new cable between the US and China in seven years, increased the available capacity between those two countries by a factor of sixty when it was completed in 2008. It now also reaches the Republic of Korea, Taiwan, and Japan. Several new cables have recently been, or will soon be, added to the existing capacity on both the east and west coasts of Africa, as shown in Figure 6.[16] As a result, the relative shares of the long-haul transport market in Africa are expected to shift from 45.6 per cent satellite, 54.4 per cent fiber in 2008 to 11.9 per cent satellite, 88.1 per cent fiber by 2014.[17] A new cable linking the US with Colombia and Brazil is scheduled to be deployed in the fourth quarter of 2012. Two additional cables scheduled in 2014 will also connect Brazil, Colombia, Panama, and the US.

Figure 6: African undersea cables (2014)

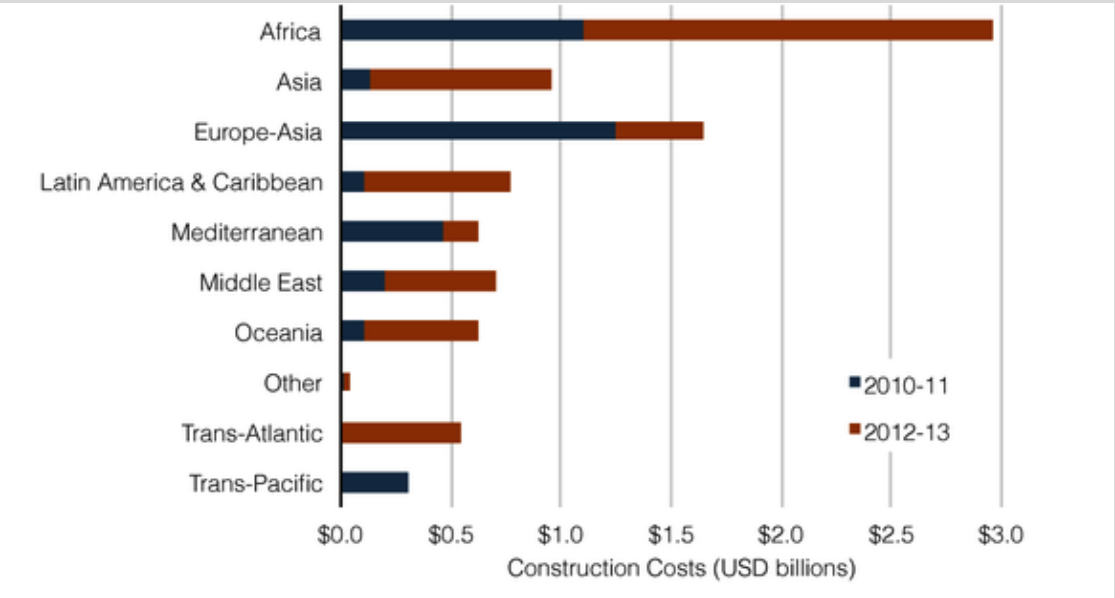


Source: http://manypossibilities.net/african-undersea-cables/

Although the Atlantic is already served by many cables, several new ones are scheduled to be laid over the next two years. One addresses an existing market, between New York and London. Owned by Hibernia Atlantic, when completed in 2013 it will reduce the route-miles between the two cities by 310 miles by following the shallow continental shelf, thus reducing latency by 5.2 milliseconds, a difference for which some business customers may be willing to pay a premium. Another new cable will link Brazil with Angola for the first time. In 2014 two additional Atlantic cables will be laid, one connecting Virginia Beach in the US with San Sebastian, Spain, the other between Brazil and Nigeria.[18]

This wave of new investment might have been difficult to predict a few years ago, given that existing cables still have spare capacity, or the potential to upgrade existing capacity, on many routes. One analyst has suggested that capacity constraints are not driving these projects. Rather, operators are interested in providing reduced latency and route diversity, and are attracted to enter those markets where margins have been relatively high in the past.[19] As this new competition enters those markets, they are driving down rates. The growth of the cable market has also brought much more diverse ownership, with participation from investors, telcos, and governments in developing countries as well as international carriers. This means that not only are there more cables and more capacity, but less monolithic control and more competition, not only among cables, but among different owners of capacity on a given cable.[20]

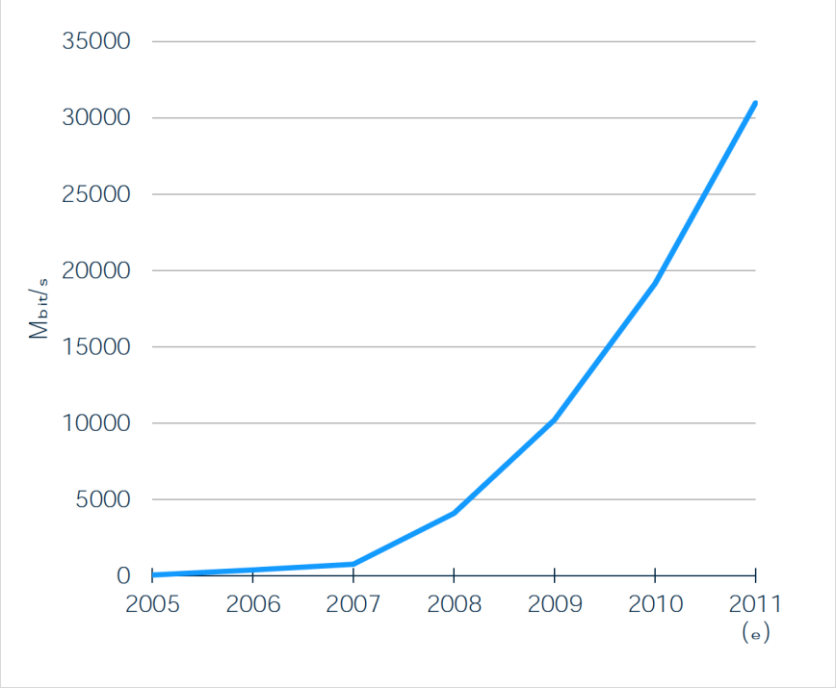
Figure 7: Submarine Cable Construction Costs by Region, 2010-2013



Source:Telegeography

Investment in long-haul capacity on terrestrial cross-border routes has been less spectacular than that in undersea cables, and in some areas has been limited by a lack of liberalization of cross-border arrangements. Nonetheless significant development has taken place. For example, the expenditure on cross-border terrestrial fiber in Africa in 2010 was USD 12 Billion. As Figure 8 shows, the total capacity of terrestrial cross-border routes in sub-Saharan Africa grew from 33 Mb/sec in 2005 to 30,960 Mbit/sec in 2011. These facilities are important to allow land-locked countries to reach the landing points for undersea cables, to handle regional traffic without tromboning, and to allow the development of IXPs as regional hubs.

Figure 8: International Internet bandwidth in sub-Saharan Africa supplied by terrestrial cross-border networks



Source: Africa Bandwidth Maps, 2012

3. Changing patterns of use

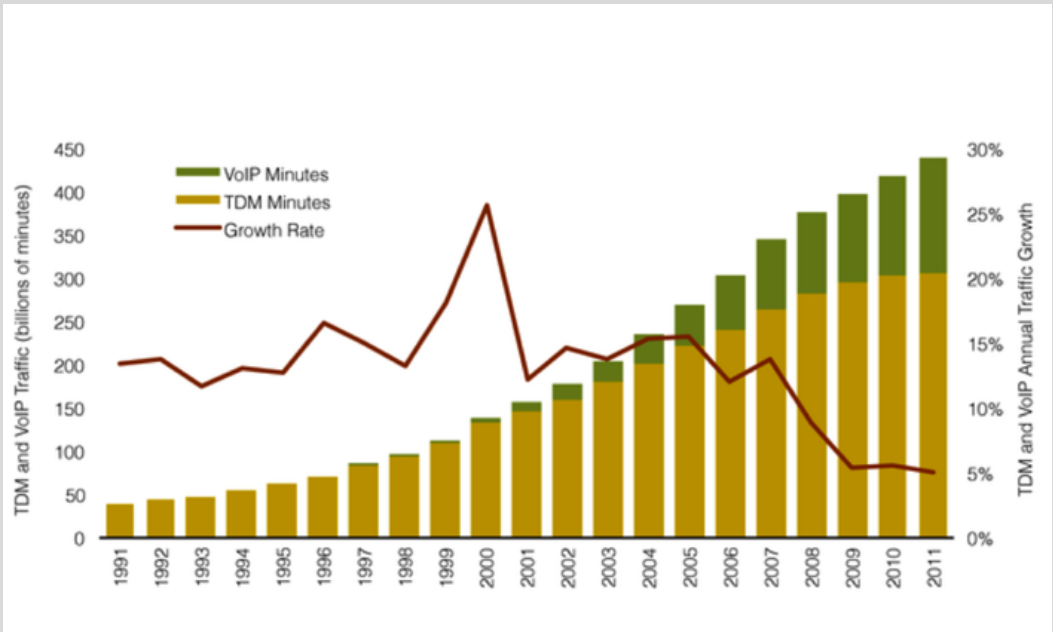
New trends in the way consumers, businesses, and institutions make use of the Internet have driven the structural changes discussed in the previous section. At the same time, the structural adaptations of the Internet ecosystem, such as the increased use of peering, the development of CDNs, and investment in new facilities, have made it possible for the system to support the new patterns of demand.

3.1 Decline and transformation of voice

For most of the history of communications, voice has been the primary offering, accounting for most of the revenue of the world's operators. Today, voice accounts for a small portion of the traffic carried on global networks. However, it still represents a significant share of carrier revenues. This share is likely to decline, for three reasons. Voice usage is declining, the price of voice service is being pushed downward, and the use of newer services is growing.

In developed markets, voice usage has peaked, and is in decline. A recent Nielsen survey in the US showed voice minutes of use declining across all age groups, especially among teenagers, falling 14 per cent in one year (2Q 2009-2Q 2010.) At the same time, the average teenager between the ages of 13 and 17 sent or received 3,339 texts per month -- more than six per waking hour (for teenage girls, the average is 4,050.)[21] Mobile voice usage had grown rapidly in the US and is still the highest in the world, but declined for the first time in 2010. In developing markets where mobile penetration is still increasing, total mobile voice usage may continue to grow for some time. The aggregate global volume of international calls is still increasing, but at a sharply declining rate. This is illustrated in Figure 9.

Figure 9: International call volumes and growth rates, 1991-2011



Source: Telegeography

The price of voice services is being driven downward by the shift to VoIP. Figure 9 shows the rapid increase in the percentage of International voice calling provided over VoIP. While most voice calling over mobile still uses circuit-switched technology, smartphone applications that facilitate VoIP calling are becoming more widely available. The rollout of 4G service using the Long Term Evolution (LTE) standard in many countries may spur a more rapid shift to mobile VoIP, since the greatly reduced latency of 4G systems allows them to support VoIP much more successfully than 3G systems could. The fact that many LTE systems will not sup-

port voice and data transmission simultaneously may also give consumers an additional incentive to avoid that constraint by turning voice into data.[22]

3.2 Video streaming and download supplants peer-to-peer

For years, carriers have been concerned that the growth of peer-to-peer (P2P) applications would overwhelm their networks. However between 2007 and 2009 the growth of P2P traffic slowed, and its share declined. Consumers have shifted their viewing habits to streaming and direct downloads of video. As a result, consumer usage on the Internet is now growing faster than business use. During peak viewing times in North America in 2012, Netflix alone accounts for 25 per cent of all traffic (upload and download), YouTube another 16 per cent, other CDN traffic 18 per cent, and all P2P traffic 12 per cent. However P2P still is the largest driver of upstream traffic on fixed networks in North America, accounting for 53 per cent of that traffic according to Sandvine. Cisco predicts that by 2016 video traffic equivalent to all the movies ever made will traverse the world's IP networks every three minutes.

Several other major trends in usage are driving growth in traffic. One is is the development of cloud services that are moving applications from desktops into data centers. Another is the growth of mobile data. Cisco predicts that by 2016 there will be three mobile devices for every man, woman, and child in the world, and that mobile data traffic will grow by a factor of eighteen between 2011 and 2016, a CAGR of 78 per cent, or three times faster than the growth in fixed network traffic.

CDN functionality may also find an expanded role in research and education. Broad-based collaborative research projects involving large data sets and distributed computing would benefit from the same methods used by CDNs to efficiently distribute consumer video. Educational television and online instruction programs could also benefit.[23]

3.3 Increased importance of quality

While the old mix of services on the Internet was somewhat sensitive to latency, the new mix is increasingly so.[24] Voice service has migrated from traditional TDM networks to the Internet, in the form of VoIP. Two-way video services have become more prevalent. Interactive games have increased in complexity, and streaming of games is displacing game consoles. And while large buffers can help one-way video steaming to tolerate some latency, consumers are becoming less willing to wait for buffers to fill. The migration of functions to the cloud means that operations that used to be handled locally on the desktop are now subject to latency between desktop and data center.

For business, two-way video conferencing is becoming more important as firms become more dispersed geographically and travel becomes more costly. Cisco predicts that video conferencing will grow eightfold between 2011 and 2016, significantly faster than other business traffic. And with global financial transactions growing in volume and speed, the tolerance for delay has become dramatically lower -- so much so that one operator is willing to spend $300 million to reduce the delay between London and New York by 5.2 milliseconds.[25]

4. Market response to changing demand

The combination of shifting demand for services by consumers and businesses, as well as dramatic changes in the structure of the Internet itself, have created both opportunities and challenges for market participants.

4.1 Improvements to quality

Many of the structural changes discussed above -- exchange of traffic locally at IXPs, increased use of peering, reduced reliance on transit, direct delivery of content and local caching through CDNs -- all combine to flatten the architecture of the Internet, producing shorter routes, fewer hops, and lower latency. CDN functionality is already used to deliver a very large proportion of Internet traffic. A new study estimates that local caching could be used for

as much as 98 percent of all Internet traffic, so there is almost no limit to the potential scope for the shift of traffic to CDNs.

4.2 Continued investment

Despite earlier fears that low prices for Internet connectivity could undermine investment, in fact the necessary investment in the fabric of the Internet has continued. If anything, the market for undersea cables appears to be experiencing a boom. And that investment has not been confined to the more developed economies, but has extended to regions which are now starting from a lower level of infrastructure, and markets that have struggled to overcome a variety of challenges.

4.3 New challenges for operators

While investment has moved forward for the core of the Internet, incumbent operators of access networks, both fixed and mobile, have faced a series of new challenges. The traditional core services on which these carriers have relied for their cash flow are being disrupted. Voice calling plans with the greatest margins are fading as customers drop land lines, exchange post-paid mobile plans for prepaid phones, and switch to VoIP. Linear television services which have been the core revenue source for cable operators are threatened as customers drop those plans and rely instead on online video. A recent Deloitte survey of US households finds that nine per cent have already dropped their linear cable TV subscriptions, and another eleven per cent are considering doing so.[26] The global economic downturn has also caused both consumers and businesses to limit their spending.

All of this comes as increased volumes of traffic driven by the new services, especially video, call for increased investment to augment capacity. Rapid growth in mobile data have strained mobile networks, and increasing capacity through adding spectrum or subdividing cells is expensive, and in some cases infeasible. Cable networks designed to broadcast linear TV are often ill equipped to handle greatly increased video traffic from the Internet. While existing last-mile facilities may be able to handle the load, middle mile facilities and regional nets between the IXP and the last mile will generally have to be augmented to deal with the shift from broadcast to online video delivery.

While these challenges are real, they may also have been overstated by operators in some markets. While, as discussed in the next section, these market challenges are driving the evolution of business arrangements, they may call for intervention by policy makers.[27]

4.4 New business models and relationships

In the face of the changes in patterns of use and market structure, participants up and down the value chain are re-evaluating their business models and seeking to adapt.

Content creators and media companies are exploring ways to gain from the new avenues of distribution the Internet offers, while maintaining defensive strategies to preserve the revenues they get today from established delivery channels, such as linear television.

Internet content aggregators, such as Google, iTunes, Netflix, and Amazon, are negotiating on the one hand with content creators for the right to distribute their content online. On the other hand, they are negotiating, either directly or through the CDNs they hire, with local access or "eyeball" networks the terms under which they will be able to deliver their content to end users. Issues for these discussions might include whether they would peer with the access network or accept some form of paid peering, and the division of labor in the provision of real resources necessary to ensure the desired quality and handle the increased traffic. Some CDNs, for example, may be willing to transport traffic deep into the terminating network, and place caches close to the end user. By doing so, the CDN improves the quality of its service, while also contributing in kind to the middle-mile investment the access network must make to in order to handle the traffic.

At the end of 2010, disputes arose on both sides of the Atlantic, arising from these kinds of negotiation, that caught the attention of national regulatory authorities (NRAs), and raised concerns about net neutrality.

In the US, the dispute was between Level 3, acting as a CDN on behalf of Netflix, and Comcast, in its role as provider of cable modem service. In France, the dispute was between the US-based transit provider Cogent, acting on behalf of a video site based in Hong Kong, China named MegaUpload, and the French access network Orange. In both cases complaints were filed with the NRAs, the Federal Communications Commission in the US and ARCEP in France; after considering the cases, neither NRA chose to intervene.[28] Cogent then filed a complaint to the competition law authority in France, which so far has not chosen to intervene either.[29]

Despite the attention garnered by these high-profile cases, it appears that the more usual outcome of such negotiations is that the CDN has been able to peer with the local access network on a settlement-free basis.[30] In this way the market appears to be addressing many of the concerns raised in the net neutrality debate, such as the terms on which a content provider could deliver traffic to an access network, whether there would be a charge on the "other side" of the market, and how the physical costs of the interconnection arrangements would be divided between the parties.

However, a report earlier this year from the Body of European Regulators for Electronic Communications (BEREC), the association of European regulators, found a number of practices that gave cause for concern, including the widespread blocking of over-the-top VoIP applications by a few fixed incumbents and a larger number of mobile operators.[31]

Another response to market changes by incumbent operators is taking the form of what might be termed a "rotation" of their retail rates structures. Until now each operator has tended to view its traditional service as the core of its rate structure -- voice service for fixed and mobile operators, linear TV for cable operators -- and the new service segments they have entered (broadband and video for fixed and mobile, broadband and voice for cable) as "add-on" services providing incremental revenue. Now, with voice and video applications riding over broadband connections, these operators are realizing that the core service they provide is connectivity. This has led to restructuring of their offerings to make broadband connectivity the core offer, around which voice and video become add-ons. For example, both Verizon and AT&T, the two largest mobile providers in the US, have recently announced new data plans under which the subscriber buys a bucket of data, rather than a bucket of minutes, which is then shared among family members. Voice calls are unlimited, but data use is not.

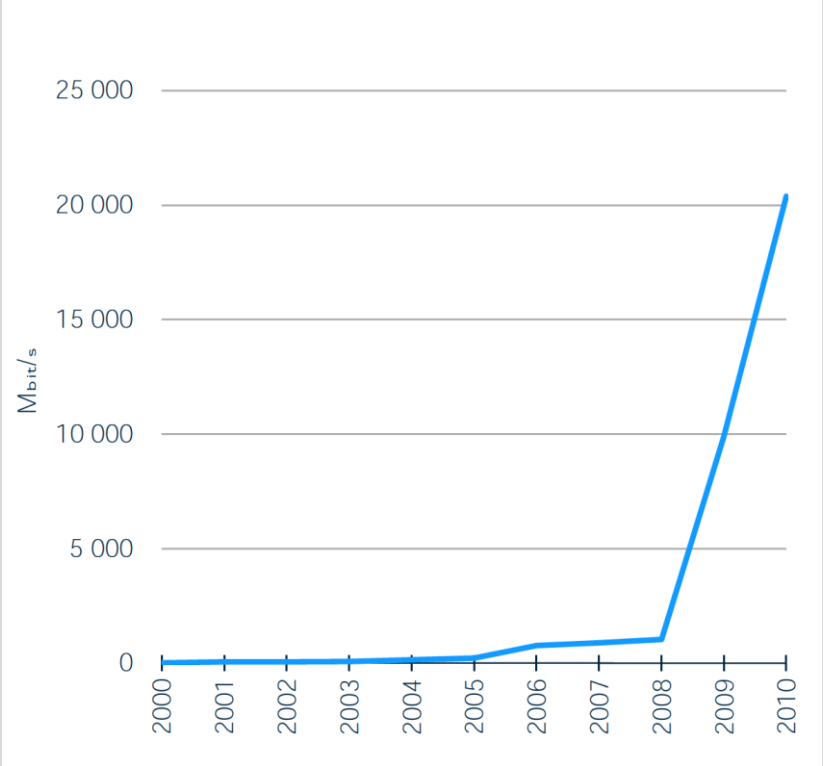
4.5 Virtuous circles in developing markets

The development of broadband services and use of the Internet have faced difficult challenges in many developing economies, given a combination of limited demand and high costs. In recent years, however, a combination of sound enabling policies and private investment have also produce many examples of significant growth and progress.

In **Kenya**, the Internet exchange KIXP was established at Nairobi in 2001, under a license from the Communications Commission of Kenya (CCK).[32] The exchange is operated by TESPOK, an association of ISPs.[33] Bandwidth capacity at KIXP grew gradually until 2009, when it began a period of dramatic growth made possible by the confluence of other factors, as shown in Figure 10.

As discussed above, several new undersea cables have recently been deployed around the African continent. Four new cables have been landed in Kenya in the last three years: The SEACOM and TEAMS cables in 2009, EASSy in 2010, and LION2 in 2012. By mid-2010 (i.e., not counting LION2) Kenya had 20 Gb/sec of international Internet bandwidth (see Figure 9). This was 20 times the amount available before the cables listed here landed, and 2000 times more than a decade earlier. An undersea capacity of 200 Gb/sec is available to be drawn upon if necessary. Recently a second IXP was opened in Mombasa, where all of the undersea cables land.[34] This has made it easier for Kenyan ISPs to shop competitively and to load-balance among the different cables, as well as saving on transport costs to Nairobi.

Figure 10: Kenya's international Internet Bandwidth Capacity (Mb/sec)



Source: CCK

This new international capacity has been complemented by the development of domestic and regional transport. Domestic backbones include the government-sponsored National Optical Fibre Backbone Infrastructure (NOFBI), a network built by the Kenya Power & Lighting Company (KPLC), and private networks owned by Orange and Kenya Data Networks. In November 2011 Safaricom announced plans to build its own 4000 km fiber-optic. These developments have reduced prices for domestic transport, reinforcing the cost advantages of exchanging traffic domestically, rather than at some foreign IXP.

Regional transport resources have also been put in place, including two links to Uganda, a point of presence in Kenya of the Tanzanian national fiber network, and planned links to Ethiopia and South Sudan. These links have allowed KIXP to become a regional hub, as KIXP members have won customers from neighboring countries, and have provided access to the undersea cables for landlocked neighbors. In the second half of 2011, 56 per cent of the Autonomous System numbers routed through KIXP were from 16 foreign countries, some as far away as the United States.[35]

The creation of KIXP, even before many of the transport investments discussed here, significantly reduced costs and improved quality. Latency was reduced from a range of 200-900 milliseconds to a range of 30 to 60 milliseconds.[36]

In 2011, Google placed a cache at KIXP. This combined with the factors discussed above, led to a dramatic increase in the amount of traffic exchanged at KIXP, with peak traffic now above one Gb/sec.[37] KENIC, the administrator of the .top level domain, has connected its root server to KIXP, which has helped it to become the most widely used TLD in Kenya, ahead of .com. KRA, the tax authority in Kenya, has benefited from the more robust exchange of local traffic to implement successful online systems to support clearing of customs for importers and filing income tax returns.[38]

Other countries in Africa have also realized substantial benefits from the establishment of domestic IXPs. In **Ghana**, for example, two IXPs were established in 2005.[39] Both were operated by non-profit organizations. GIX today has 15 members; the second IXP, AIX, is no longer active. As in Kenya, new undersea cable investment has created additional international bandwidth. Five different cables now land in Ghana; the most recent, WACs, connects fifteen landing stations along the west African coast with London. The WACs connection

to Ghana was turned up early this year. As in Kenya, this international bandwidth has been complemented by some investment in domestic fiber transport.

Some of the same benefits have also been realized in Ghana. Costs have been reduced by eliminating the tromboning of traffic. Latency has been reduced from about 500 ms to about 25 ms. Google has established a cache at GIX. The peak traffic exchanged at GIX is about 540 Mb/sec, or about half the volume at KIXP.

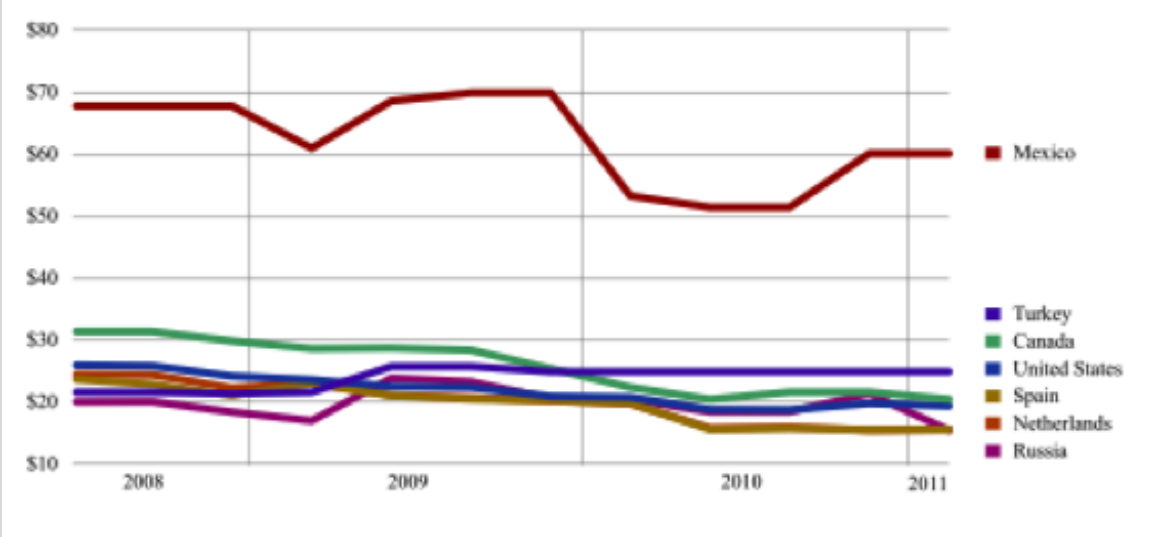
In Nigeria, IXPN was established in Lagos in 2006. It currently has 38 members, though not all of those are connected to the exchange.[40] Many of the benefits realized in other settings are already materializing in Nigeria. The peak volume of local traffic exchanged at IXPN is about 300 Mb/sec.[41] Tromboning of local traffic has been largely eliminated. Latency has been reduced from 200-400 ms to 10 ms or less. Google extended its network to Lagos in March 2010, and established a cache at IXPN. As in the other exchanges, some have noted Google's presence has led to a rapid increase in traffic, with Google now representing more than 50 per cent of all the traffic exchanged.[42]

IXPN is planning to become a distributed exchange by establishing six points of presence (POPs) in different regions of the country. This deployment could play a constructive role in reducing the cost of domestic transport. The first two points were established in Abuja and in Port Harcourt in 2012.[43] When IXPN was created, a decision was taken to limit its members to the exchange of local traffic. If that restriction were relaxed, IXPN could also become a hub for the aggregation of long-haul international traffic and for the exchange of traffic with neighboring countries.
The presence of the IXP has also created other opportunities for business development. For example, Interswitch, the leading platform for electronic transactions and payments in Nigeria, is connected to IXPN. Established by seven Nigerian banks, Interswitch links 10,000 ATMs and 11,000 point-of-sale terminals.[44] This framework has begun to attract financial platforms that were formerly hosted abroad have begun to return to Nigeria. Nigeria has opportunities to utilize IXPN to promote the distribution of domestic content both in-country and internationally, since Nigeria already has a film industry that produces more films each year than any other country except India.[45]

The African examples discussed here illustrate the potential for IXPs to generate significant benefits when combined with other elements of liberalized policy and private investment. However, the converse is also true: the lack of an IXP can limit opportunities. Figure 12 compares retail prices for transit provided to enterprise customers in different countries. The difference in transit costs shown here for Mexico and Turkey is partly explained by the lack of an IXP in Mexico.

Much remains to be done to promote the development of the Internet in Africa. Only about 1 percent of Internet traffic generated in Africa is exchanged locally, and 99 per cent of that exchange is concentrated in four countries: Egypt, Kenya, Nigeria and South Africa.[46] However, progress is being made through the deployment of undersea cables discussed above, which in turn have contributed to the growth of traffic at IXPs. Between June 2009 and July 2012, Africa's total inventory of terrestrial transmission networks increased from 465,659 kilometers to 732,662 km, bringing 40 per cent of the population within reach of an operational fiber node.[47] A number of projects are under way to increase the reach of regional transport and make regional traffic exchange more economic. For example UbuntuNet, an alliance of 13 national research and education networks (NRENs) plans to establish, over the next three years, backbones extending up both east and west coasts from South Africa, with extensions to exchanges in Europe. UbuntuNet members already peer at KINX in Nairobi, TINX in Dar es Salaam, CINX in Cape town, and JINX in Johannesburg, as well as in Amsterdam and London. At the European exchanges it is then able to buy transit cheaply.[48]

Figure 12: Retail price of enterprise Internet transit, mbps/month, in USD



Source:Telegeography

5. *Policy challenges for the future*

The available evidence shows that the global market for IP connectivity has performed very well. It has produced low prices, directed resources efficiently, and enabled the extension of the Internet to users around the world.

5.1 Variation in Outcomes

The development of Internet resources and opportunities has varied significantly by region and by country.[49] These differences are based in part on geography, distance, and scale, but are also highly sensitive to competitive conditions within country and to related choices by governments with respect to liberalization. These factors, rather than any market failure in global markets for IP connectivity, have played the major roles in determining the success of Internet development in emerging markets.

Costs of the inputs necessary to provide broadband have declined as demand has grown and markets have developed. In particular, the prices paid in many developing countries for international Internet connectivity have declined, in part as a result of the new investments in long-haul cable capacity discussed above. [50] Reductions in rates for international Internet connectivity, while both likely and welcome, will have a diminishing effect on the price at which domestic networks can offer broadband, as they will operate on a diminishing share of those networks' total cost.

5.2 Policy in developed markets

In developed countries, the legal and regulatory frameworks for telecommunications, and liberalization of those frameworks to promote competition, were in place before the development of the Internet. The Internet benefitted from the general framework of liberalization that provided freedom of market entry, access to rights of way, availability of leased lines, and so on. However, the market for the exchange of IP traffic has grown up outside the existing regulatory framework that has applied to the interconnection and the exchange of traditional circuit-switched voice, or TDM, traffic. As described above, the IP market has performed better than TDM markets have done.

Over time the TDM voice market has declined, and the IP market has grown. Legacy telco networks have adopted IP for most internal functions, and traditional services such as voice and video have been replaced by IP-enabled applications. This process has led to the possibility of a collision between the old, regulatory framework and the new, unregulated universe of IP connectivity. In some cases, policy makers might regret the loss of enforceable rules or of data reporting on the traffic exchanged outside the regulatory framework.

In others, interested parties might feel the loss of some right they enjoyed under the regulatory scheme, such as the ability to demand interconnection or to assess termination charges. This in turn has led to calls for NRAs to consider regulation of IP interconnection and traffic exchange.

In a few developed countries, regulatory authorities have considered this issue. In 2006 the Polish regulator, UKE, adopted some requirements to provide transit on the Polish incumbent, Telekomunikacja Polska (TP). This action was effectively vetoed in 2010 by the European Commission, which found that the UKE had not met the criteria for identifying new markets for regulation.[51] In the announcement of the Commission's decision, Digital Agenda Commissioner Neelie Kroes said: "The Commission fully shares the objectives of the Polish regulator in seeking competitive markets, but our assessment is that regulation of these particular markets for Internet traffic exchange services is not necessary to protect consumers or competition. If the market itself is able to provide for fair competition, don't disturb it with unnecessary regulations."[52]

Some concerns have been raised about arrangements for the exchange of voice traffic where the calls are being routed using a telephone number, since in most numbering systems the assignment of the number to the carrier serving the recipient gives that carrier some control over termination that it would not have for other IP traffic.[53] For this reason what little regulatory activity there has been among developed country regulators has dealt with voice traffic.

In the United States, the Federal Communications Commission (FCC) has generally refrained from regulation of IP traffic exchange, although a few limited provisions have been agreed as conditions for the approval of mergers. The FCC has recently taken comments from parties on whether regulation should be applied to the exchange of voice traffic over IP interfaces, but has yet to take any action.[54]

In Canada, the Canadian Radio-television and Telecommunications Commission (CRTC), has recently adopted a number of new regulatory provisions with respect to network interconnection for voice services.[55] The CRTC found that IP interconnection for voice traffic should continue to be carried out under bilateral commercial arrangements. It also found it unnecessary to mandate a default tariff for IP voice network interconnection. However, if a carrier is providing IP voice network interconnection to an affiliate, a division of its operations, or an unrelated service provider, then it must provide similar arrangements with other carriers. The carriers are to complete the negotiation process within six months of a request for interconnection. Either party may request mediation by the CRTC staff, or apply to the CRTC for intervention if an arrangement is not concluded within the six-month period.

The record in this area among developed countries is therefore quite limited. While the possibility of failure in IP markets cannot be ignored, and some intervention may be necessary in the future, as a general matter this temptation should be resisted, and a "bright line" should be drawn to avoid the application of traditional remedies to this new market. The reasons for this are many. Perhaps most obvious is the simple fact that prices in the regulated markets for TDM traffic exchange are many orders of magnitude higher than equivalent prices for IP traffic. This is the case even though many of the same firms participate in both markets. Clearly IP markets operate differently from the traditional ones.

Traditional frameworks for TDM interconnection and traffic exchange have sought to impose a particular order, such as "calling party pays," and in so doing have created a cascading flow of funds among customers and networks. While this may have been useful as a way of making the trains run on time, and funding certain social policy objectives, it wasn't based on sound economic principles.[56] The IP market has succeeded in part because it has never had to follow any such rule, or to serve as a conduit of funds. Rather, it serves only as a means for networks to exchange connectivity, nothing more or less, and is able to set a separate value for each such exchange.

Traditional frameworks for TDM markets have sought to guard against anticompetitive refusals to deal (i.e., refusal to interconnect) by imposing an obligation to interconnect. In a number of TDM markets, this has been necessary. However, in the absence of such obligations, participants in any market discipline unreasonable behavior, such as high prices or unreasonable terms, by refusing to deal with parties who behave that way.

The results of the survey of peering agreements discussed above suggest that the Internet has been able to achieve universal global connectivity with less than one per cent of a full mesh; that is to say that fewer than one per cent of all the bilateral arrangements that could exist actually do exist. One of the important functions of the market for IP connectivity is to determine which of the possible arrangements should be created and to direct resources efficiently where they are needed. It would be difficult for the IP market to perform this important role if parties had a general obligation to enter into such arrangements.

The irony of regulation in markets for interconnection is that the very tools that are available to policy makers to address perceived market failures also create and perpetuate market failures. This does not mean that such tools should never be used, but it does strongly suggest that the threshold for imposing them should be very high. The speed at which the Internet ecosystem continues to evolve is another cause for concern, as any regulation is likely to be obsolete before it can be adopted.

For similar reasons, the most sound approach for regulators to adopt where disputes arise over the termination of CDN traffic may be to observe the development of those markets, and intervene only when necessary (ex post) if possible. This appears to be the course already adopted in most countries, including the previously cited examples in France and in the United States. The negotiations up and down the value chain – between content creators and Internet aggregators of content, between those aggregators and CDNs, and between CDNs and terminating access networks – are establishing the terms of trade for new forms of content delivery. In particular the agreements being struck between CDNs and local networks are providing market-based answers to many of the questions that have been raised in the debate over net neutrality. They are determining how content will be delivered to broadband users, on what terms, and what resources will be brought to bear to ensure quality, and by whom. So far, the terms of these agreements appear to fall within a reasonable range, most often on a settlement-free basis, with a few examples of paid peering. Further, quality is being enhanced, not by subtractive means (traffic management software) but by adding resources in the form of direct transport and caches close to the end user.

In the context of these negotiations, it may be the case that the agreement between a CDN an incumbent operator may involve some payment (i.e., paid peering) although in practice most agreements so far have been settlement-free. As long as these agreements do not indicate a pattern of unreasonable exercise of market power by incumbents (and so far they have not) then NRAs do not need to intervene. On the other hand, NRAs also should not intervene to impose any mandatory termination payment on CDNs, or on any other network that delivers traffic to local access network. Providing adequate investment for local access networks is a worthwhile objective, but those networks should have to earn their revenue by providing value businesses, consumers, or interconnecting networks are willing to pay for through voluntary commercial agreements. Governments should not support this approach, and they should prevent any collusive action to impose such a system.[57]

5.4 Policy choices in emerging markets

Liberalization attracts investment, builds Internet assets and scale, and promotes growth by reducing costs. The only process that can shift the terms of trade in a country's favor in the international market for internet connectivity is increasing competition and investment, both in that country's domestic market and in the market for long-haul transport. Fortunately substantial progress has been made in these areas in recent years.

In emerging markets authorities have faced policy choices between defending the existing business models of national incumbents and liberalization to promote competition and the adoption of new services. These choices can be challenging as government is naturally concerned about the incumbent's ability to support future investment, to contribute revenues in the form of license fees, and to perform other desired social functions such as the provision of universal service.

Each country must find its own policy balance among potentially conflicting objectives. However, the conflict may not be as clear as it appears. The experience in many emerging markets has been that liberalization, by attracting investment and opening new opportunities, has been able to stimulate economic growth while also promoting increases in Internet resources, teledensity, and broadband deployment. These develop-

ments, in turn, have allowed countries to achieve better terms of trade in the international market for Internet connectivity.

The policy frameworks to promote development of Internet assets are in many ways the same ones that have been used to liberalize markets for traditional services. While the long-term case for regulation of IP interconnection is no better in emerging markets than in developed ones, there may be a case for short-term intervention where defensive actions by the incumbent have prevented the development of a domestic market. Best policy practices for promoting Internet market development will be discussed below.

5.5 The process for international treaty revision

The ITU's World Conference on International Telecommunications 2012 (WCIT-12), which meets in December 2012, will review the International Telecommunication Regulations (ITRs)[58] where the international treaty that is the basis of today's connected world will be reviewed. The ITRs were agreed in 1988 at the World Administrative Telegraph and Telephone Conference in Melbourne, Australia, and came into force in 1990. The ITRs set out principles for ensuring that networks can connect with each other smoothly, and that international services will be offered in a fair and efficient manner.[59] Within this context, proposals have been made to add provisions to the ITRs to foster cooperation in the development of international IP interconnections by promoting best effort delivery and end to end quality of service delivery.[60]

5.6 Best practices for the promotion of a virtuous circle of development

Governments in emerging economies can contribute to the development of a virtuous circle of investment and growth by adopting policies that open markets, promote competition, reduce barriers to investment, and facilitate the expansion of demand.

The most basic element of best practice is liberalization that opens the telecommunication market to competition. This would include the establishment of an independent regulator, privatization of the incumbent, opening the market to competitive entry without entry barriers or high license fees, access to rights of way, and availability of leased lines at reasonable rates.

Since mobile networks are likely to be important providers of broadband in most developing countries, policies that enable them to expand efficiently will promote rollout and take-up. These would include assignment of adequate spectrum resources, and policies that facilitate tower sharing, approval, and construction.

The development of international Internet connectivity will depend on the ability of investors in long-haul transport facilities arrange entry points at reasonable cost. Policies that simplify licensing for landing rights for undersea cables and cross-border arrangements for terrestrial routes, that minimize licensing fees, and that limit the ability of the incumbent to control such points, will facilitate such investments. Public investment may be helpful, but should be organized with care to avoid undoing the beneficial effects of privatization. The establishment of national backbones has in some countries crowded out private ISPs.

The development of domestic and regional transport networks is crucial both for IP backbones and for backhaul to deploy mobile networks. Market entry without excessive license fees and access to rights of way are important enablers.

As discussed above, establishing an Internet exchange point in-country or in-region can reduce reliance on transit, improve service quality, and provide a hub to attract investment. However, there is no guarantee that an IXP will succeed; the Packet Clearing House directory of global IXPs includes many that are now inactive.

- IXPs that are operated by independent entities without ties to any carrier are most likely to be successful. All of the examples cited above in Kenya, Ghana, and Nigeria are run by independent, non-profit entities. Development of IXPs in Brazil has been led by the Brazilian Internet Steering Committee (CGI), a public-private partnership funded in part by domain name registrations within the .BR country-code top-level domain.[61] Between 2006 and 2011, the number of IXPs in Brazil has grown

from four to nineteen.[62] The CGI has made a policy of studying the factors contributing to the success or failure of other IXPs around the world. A cooperative membership model in which member ISPs participate in decision making helps to establish trust.

- Government can minimize barriers to the establishment of IXPs, such as high licensing fees. NRAs can have a role of neutral arbiter; the Uganda Communications Commission and the Malaysia Communications and Multimedia Commission have both played this role.[63] The regulator may also intervene in resolving objections raised by the incumbent, as in the case of Kenya.[64] However, direct management of IXPs can have unanticipated negative effects. For example, requirements that all members of an IXP must join a multilateral peering agreement may discourage some parties from joining the IXP.

- Attracting complementary assets, such as CDN caches and DNS root-servers, can add to the attractiveness of joining an IXP.

- A multilateral peering agreement at the IXP can reduce transaction costs and minimize communication or trust issues that might inhibit bilateral agreements.

- An ideal location for an IXP would have access to an international facility (undersea cable or terrestrial), be convenient to several potential member networks, and have a reliable source of electric power.

- Aggregation of traffic at an IXP can help its members of the exchange obtain better terms of trade from transit providers. Good practices to obtain better terms also include multi-homing to avoid being tied to one provider; regular monitoring and re-negotiation of contracts to take advantage of improvements both in the volume of traffic at the IXP and in competition; and arrangements with content providers to improve quality and reduce costs.[65]

Effective measures to limit anticompetitive behavior by the incumbent, such as monopolization of international gateways, denial of access to rights of way or leased lines, or control of IXPs. Regulation, or, in some cases, "jawboning" may be necessary to encourage agreements for IP traffic exchange with competing carriers.

Promotion of demand for broadband services. This could include e-government initiatives to deliver government services online, investment in networks for research and education, and promotion of development of local content. This objective can also be promoted through public-private partnerships. For example, Google has participated in a Google Apps Supporting Program (GASP) which has already established connections between the Lagos IXP and four participating universities. The program included the donation of a Juniper router to IXPN and training by Google on management of the network.[66]

Limits on foreign direct investment make it difficult to attract the investment necessary to expand broadband and Internet infrastructures, and limit participation by international carriers, content providers, and CDNs.

High domestic prices for network equipment can be a significant barrier to investment in Internet resources. High domestic prices for customer equipment, such as laptops and smartphones, as well as, high import duty taxes, luxury goods and service taxes, or certification policies that raise domestic prices for these items can inhibit broadband demand and Internet usage.

Defensive policies limiting the availability of attractive applications such as VoIP will limit the usefulness of broadband, discouraging take-up, while artificially raising costs to domestic consumers and businesses. Promotion of arrangements to allow the exchange of VoIP on an IP basis ("VoIP peering"[67]) would also facilitate development of this market.

6. Conclusion

The global market for Internet connectivity continues to grow rapidly and to perform well, producing low prices, directing resources efficiently, and calling forth the investment needed to sustain its growth. However, the results have varied significantly by region and country, driven by differences in distance and scale, as well as by government policies. Developing countries face challenges in promoting growth of Internet assets that will support the widespread availability and adoption of broadband.

In the last few years, significant new investments have been made in both international and domestic Internet connectivity in many developing economies. These have allowed growth in those countries to proceed at annual rates much higher than those observed in developed regions, albeit from a lower starting point. Countries with effective, liberalized policy frameworks have been best positioned to promote a virtuous circle of investment and growth. This paper has explored policy best practices to encourage a process in which investment, demand growth, and improving terms of trade can reinforce one another in support of rapid Internet and broadband development.

[1] This subject of this paper is the universe of IP traffic exchanged globally. This includes exchanges which are not part of the public Internet. For example, in its estimate of 30.7 exabytes per month of global IP traffic in 2011, Cisco includes 6.8 exabytes of what it defines as "managed IP" traffic, such as corporate IP WAN traffic and IP transport of TV and video. For the purposes of this paper, IP traffic and Internet traffic will be used interchangeably, unless there is a specific reason to draw a distinction. See Cisco Visual Networking Index: forecast and Methodology, 2011-2016, (Cisco VNI2012) at Table 1. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf

[2] Weller, Dennis and Bill Woodcock. IP Traffic Exchange - Market Developments and Policy Challenges, OECD DSTI/ICCP/CISP(2011)2/Final forthcoming October 2012 at page 5. See also the Annex to this paper DSTI/ICCP/CISP (2011)2/ANN/FINAL.

[3] See Cisco VNI 2012 at Table 3. A zettabyte is one thousand exabytes.

[4] Some of the reasons for the difference in performance are discussed in the Annex to Weller and Woodcock (2012).

[5] The term ISP is used generically here to denote a network that participates on the Internet, including both backbone and local access networks.

[6] See Weller and Woodcock (2012), Annex 1. The same results can be found in Woodcock, Bill, and Vijay Adhikari, from Packet Clearing House (http://pch.net/resources/papers/peering-survey.)

[7] For instance, latency experiments conducted on Bing and Google search sites showed that a 2 second slowdown changed the number of queries per user by -1.8% and the revenue per user by -4.3% for Bing, while a 400 millisecond delay resulted in a -0.59% change in the number of queries per user for Google.
See http://perspectives.mvdirona.com/2009/10/31/TheCostOfLatency.aspx

[8] For a directory of IXPs, see http://pch.net/ixpdir.

[9] For a list of countries without an IXP, see Weller and Woodcock (2012), Appendix 4

[10] Labovitz, et al, Atlas Internet Observatory, 2009 Annual Report (Atlas 2009), at Page 15. http://www.nanog.org/meetings/nanog47/presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf. The study was a joint project of Arbor Networks, The University of Michigan, and Merit Network

[11] http://blog.netflix.com/2012/06/announcing-netflix-open-connect-network.html

[12] For a discussion of this process, see Weller, Dennis, "The Internet Market for Quality," Communications & Strategies, 4Q 2011. (Weller 2011)

[13] Labovitz, Craig. "CDN and Over-the-Top Traffic Data," Content Delivery Summit, May 2012. http://www.contentdeliverysummit.com/2012/Agenda.aspx

[14] Appendix 1 lists the undersea cables in operation globally in 2000, 2006, and 2012.

[15] http://www.telegeography.com/press/press-releases/2012/04/18/submarine-cable-construction-continues-despite-untapped-potential-capacity/index.html

[16] For a layered version of Figure 6 that shows the stages in which capacity around Africa has been and will be added over time, see http://www.slideshare.net/ssong/african-undersea-cables-a-history

[17] http://blogs.broughturner.com/2010/04/africa-moves-from-satellite-to-fiber-links.html

[18] Andrew Blum, "A Dive into the Digital Deep", Wall Street Journal, May 25, 2012. http://online.wsj.com/article/SB10001424052702304840904577422370903409342.html?mod=business_newsreel

[19] http://www.telegeography.com/press/press-releases/2012/04/18/submarine-cable-construction-continues-despite-untapped-potential-capacity/index.html

[20] See Akue-Kpakpo, Abosse, Study on International Internet Connectivity in Sub-Saharan Africa, March 2012 at page 20. For a list of cables and their ownership, see http://www.cablemap.info and http://manypossibilities.net/african-undersea-cables/

[21] http://blog.nielsen.com/nielsenwire/online_mobile/u-s-teen-mobile-report-calling-yesterday-texting-today-using-apps-tomorrow/.

[22] LTE smartphones configured for CDMA networks generally will not allow the user to download data and use the carrier's voice service at the same time. This creates an incentive for users to switch to over-the top VoIP applications that use the phone's data capability, and for the carriers to adopt VoIP for their own voice services.

[23] See http://billstarnaud.blogspot.ca/2012/06/why-cdns-are-critical-to-future-of-r.html

[24] Many services are also sensitive to jitter, which is caused when different packets take very different routes. This is another issue addressed by more direct routing provided by CDNs.

[25] See fn 18.

[26] http://gigaom.com/video/deloitte-cord-cutters/

[27] See, for example, Marcus, J. Scott, and Allessandro Monti, "Network operators and content providers: Who bears the cost?" WIK Consult 2011. http://ssrn.com/abstract=1926768

[28] In February 2011, in response to a question at a congressional hearing, the chairman of the FCC, Mr. Genachowski, expressed the view that the FCC's recent order on network neutrality was focused on protecting broadband consumers, not on peering disputes. The network neutrality rules "don't change anything with existing peering agreements," he said. See WSJ, "FCC Chairman: Net Neutrality Rules Don't Cover Comcast-Level 3 dispute." February 16, 2011. http://online.wsj.com/article/BT-CO-20110216-718576.html

[29] For a discussion of these cases and their implications, see Weller (2011). For a more recent report, see http://www.olswang.com/articles/2012/07/the-net-neutrality-debate-recent-developments-in-europe/

[30] Labovitz (2012) for example reports that CDNs are "now (nearly) completely peered."

[31] http://berec.europa.eu/eng/document_register/subject_matter/berec/press_releases/24-berec-publishes-net-neutrality-findings-and-new-guidance-for-consultation

[32] KIXP was initially launched in 2000, but was forced to close after a complaint from the incumbent Telkom Kenya that the IXP violated its exclusive right to carry international traffic. KIXP reopened in 2001, with a license from the CCL, the first IXP in the world to be required to have a license. See Kende, Michael, "Overview of recent changes in the International IP interconnection ecosystem," ITU Workshop on Apportionment of Revenues and International Internet Connectivity, Geneva, January 2012.
[33]
[34] See Akue-Kpakpo (2012) at 18.
[35] Mwangi, Michuki, "The African Peering & Interconnection Scene: Developing the Critical Mass," European Peering Forum, September 2012. http://www.peering-forum.eu/assets/presentations2012/AfricanPeering.pdf
[36] Russell Southwood, "Via Africa: Creating Local and Regional IXPs to Save Money and Bandwidth," International Telecommunication Union and International Development Research Center, 2005, http://goo.gl/D1rkK, at page 12.
[37] Kende 2012 at Slide 16.
[38] Mawangi (2012)
[39] See Bulley, Ayitey, "The Peering Scene in Ghana," Africa Peering and Interconnect Forum, Accra, August 2011
[40] http://www.nixp.net/index.php?option=com_content&view=article&id=13&Itemid=13
[41] Mwangi (2012)
[42] Choi, Yen, "Building Critical Mass at an IXP: The IXPN case study," Africa Peering and Interconnect Forum, Accra, August 2011
[43] Nigeria: NITDA Establishes IXPss to Crash Internet Cost, http://allafrica.com/stories/201205220342.html
[44] http://www.interswitchng.com/#PAYMENT%20INFRASTRUCTURE. See also Mwangi (2012)
[45] "Nollywood: Lights, camera, Africa," The Economist, September 27 2012, http://www.economist.com/node/17723124?story_id=17723124&CFID=153287426&CFTOKEN=59754693
[46] Mwangi (2012)
[47] Hamilton Research, Africa Bandwidth maps http://www.africabandwidthmaps.com
[48] Martin, Duncan, "UbunduNet's connectivity, peering, transit, and all that," AfPIF, August 2012. http://www.internetsociety.org/sites/default/files/images/Duncan%20Martin_UbuntuNet%20Update%20for%20AfPIF_2012.pdf
[49] A review of market developments by region and country is provided in Weller and Woodcock (2012)
50 Southwood (2005) at page 8.
[51] For a more complete discussion, see Weller and Woodcock. See http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/240&format=HTML&aged=0&language=EN&guiLanguage=en. Commission letter at http://circa.europa.eu/Public/irc/infso/ecctf/library?l=/commissionsdecisions&vm=detailed&sb=Title.
[52]
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/240&format=HTML&aged=0&language=EN&guiLanguage=en.
[53] For discussion of this point see Weller and Woodcock, and Marcus, et al, The Future of IP interconnection: Technical, Economic, and Public Policy Aspects. WIK-Consult, 2008, prepared for the European Commission (WIK 2008), at Pages 114–120.
[54] See Report and Order and Further Notice of Proposed Rulemaking, FCC 11-161, Adopted October 27, 2011. Released November 18, 2011. (FCC Universal Service and Access Reform Order) See also Comments filed February 24, 2012, and Reply Comments filed March 30, 2012.
[55] See "Network interconnection for voice services," File number 8643-C12-201105297, 19 January 2012. (CRTC 2012)
[56] In a general model of traffic exchange, Katz and Hermalin found that the commonly used frameworks, such as calling party pays, are optimal only in extreme cases, or corner solutions, where extreme values of the relevant parameters, such as demand elasticities and incremental costs, are assumed. Hermalin, Benjamin E., and Michael L. Katz, Sender or receiver: who should pay to exchange an electronic message? Rand Journal of Economics, Volume 35, No. 3, Autumn 2004 http://faculty.haas.berkeley.edu/hermalin/Hermalin_Katz_RAND.pdf
[57] For further discussion, see Weller and Woodcock (2012).
[58] http://www.itu.int/en/wcit-12/Documents/WCIT-background-brief4.pdf
[59] Article 1.3 of the ITRs says: "These Regulations are established with a view to facilitating global interconnection and interoperability of telecommunication facilities and to promoting the harmonious development and efficient operation of technical facilities, as well as the efficiency, usefulness and availability to the public of international telecommunication services."
[60] http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf"
[61] Weller and Woodcock (2012)
[62] https://prefix.pch.net/applications/ixpdir/ See also Oliveira, Salerme, "International Internet Connectivity - The Brazilian Experience," ITU Workshop on Apportionment of Revenues and International Internet Connectivity, Geneva, January 2012
[63] Southwood (2005) at page 23.
[64] Akue-Kpakpo (2012) at 21.
[65] Galliano, Roque, "Transit Service Practices," ITU Workshop on Apportionment of Revenues and International Internet Connectivity, Geneva, January 2012
[66] http://www.google.com/africa/universityprograms/inst/gasp.htm
[67] For more detailed analysis on the topic, see the GSR09 Discussion paper on the Future of VoIP interconnection, at: http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_VoIP-interconnect_VanderBerg.pdf

INTERNATIONAL TELECOMMUNICATION UNION

GSR 2012 Discussion Paper

Demystifying Regulation in the Cloud:

Opportunities and Challenges for Cloud Computing

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 19 October 2012.

TABLE OF CONTENTS

1 DEMYSTIFYING REGULATION IN THE CLOUD: OPPORTUNITIES AND CHALLENGES FOR CLOUD COMPUTING

Professor Ian Walden, Queen Mary, University of London and Baker & McKenzie

1. Introduction

> "The rise of the cloud is more than just another platform shift that gets geeks excited. It will undoubtedly transform the information technology (IT) industry, but it will also profoundly change the way people work and companies operate. It will allow digital technology to penetrate every nook and cranny of the economy and of society, creating some tricky political problems along the way."
>
> Source: Economist, 'Let it rise', 23 October 2008.

With the emergence of ubiquitous broadband connectivity, cloud computing offers an alternative platform from which Information and Communications Technologies (ICT) providers can offer powerful and innovative new services, while providing users with the opportunity to gain access to computational resources and applications beyond those traditionally feasible. It challenges our perception of how to utilize and exploit ICT to engage economically and socially more efficiently and effectively. Uncertainties over the legal and regulatory treatment of cloud computing may, however, act as an obstacle to its adoption.

This paper considers the cloud computing phenomenon, from a technical, market and social perspective, and examines its legal implications, the role of regulation and regulators and how policy makers can create an environment conducive to its take-up.

2. Cloud technologies

Cloud computing has emerged over recent years as the latest manifestation of networked computing. It represents a shift in computing power from so-called 'thick client' solutions, whereby the applications used are present on personal computers while the data may be hosted and shared on a remote server, to a 'thin client' environment, where both the applications and the data reside on the remote server. This trend is being made possible by the widespread availability of fast resilient communication networks over which data can be transmitted. To an extent, the shift represents a return to the early years of computing, when mainframes dominated the environment and where access took place through 'dumb' terminals.

Cloud computing is not a single technological solution, but is rather an umbrella term used to describe a range of different technologies and market offerings. Numerous definitions of cloud computing exist[1], often reflecting the different perspectives of providers and users. The ITU, for example, defines cloud computing in the following terms:

> "A model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and ser-

vices), that can be rapidly provisioned and released with minimal management effort or service-provider interaction. Cloud computing enables cloud services."[2]

For the purposes of this paper, the following definition is used:

"Cloud computing provides flexible, location-independent access to computing resources that are quickly and transparently allocated or released in response to demand.

Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers.

Charging is commonly on an access basis, often in proportion to the resources used."[3]

Examining the different elements of this definition in further detail helps to better understand how cloud computing differs from other forms of IT services, such as outsourcing. First, 'flexibility' means that the computing resources are available to the user as and when needed, on-demand, with the associated efficiencies for both the user and provider, rather than fixed and dedicated for the customer[4]. Second, 'location-independence' is possible as a result of the 'death of distance'[5] made possible by modern communication networks, such as the internet. Third, 'virtualised' services means that the resources created for users, such as storage, operating systems and applications, are distinct from the underlying actual physical resources on which they operate, such as a server farm. Virtual machines emulating physical machines. Fourth, the actual physical resources provided by the service providers are 'shared' by the customers, again resulting in more efficient use of the infrastructure. In certain situations, the customer may be unwilling to share with other customers, due to security concerns. As such, 'private' cloud services may be utilized, whereby the resource is dedicated for a single user or shared by a restricted community rather than available to the public', or a 'hybrid' cloud service, where certain resources are restricted, while others are public[6]. Finally, the reference to 'charging' reflects the fact that 'public' cloud services are generally purchased on a commodity-basis, on the provider's standard terms and conditions, rather than individualized and negotiated agreements, as is usually the case in IT outsourcing.

2.1 Cloud opportunities

What is driving the take-up of cloud computing? As with any area of business, the ability to reduce costs and increase productivity often lies at the heart of the decision to adopt cloud solutions. Cloud computing offers general business and organizational benefits, as well as benefits in the exploitation of ICTs[7].

Similar to IT outsourcing, cloud computing can offer users substantial cost savings over traditional models of ICT ownership. From a cloud user's perspective, such savings can arise in four key areas:

- Labour costs, as fewer ICT-dedicated personnel are required by enterprises;
- Energy efficiencies, from not having to operate the hardware resources to service the needs of the enterprise;
- Real estate, from requiring less space for the ICT equipment, and
- Usage licences, through the shift from End-user licences to service-based delivery[8].

It is these cost savings and others that have led policy makers to enthusiastically embrace cloud computing: "The medicine needed for our credit squeezed economy"[9].

The scalability of cloud services enables increased productivity and improved responsiveness to changing customer demands and market conditions. It reduces risk for organizations, enabling them to trial new ideas and processes without the need to invest heavily in new technologies. In particular, cloud can facilitate new means of collaborative working practices, reflecting in part models from the open source community, both within and between organizations.

2.2 Cloud challenges

What barriers exist to the uptake of cloud computing? One leading concern is data security, the trust, reliability and dependency in moving data and applications to a remote third party. While such concerns are real and need to be adequately addressed, as discussed further below and in the paper on cloud privacy[10], they are in part also cultural, requiring a change in attitude about how to use ICT systems. In 1999, Scott McNealy, then head of Sun Microsystems, made the infamous statement about online privacy: "You have zero privacy anyway. Get over it!". This could be rephrased for a cloud environment as: "Everything is shared. Get over it!". Altering cultural attitudes to embrace innovative ICT solutions can sometimes be as difficult as addressing the technical challenges.

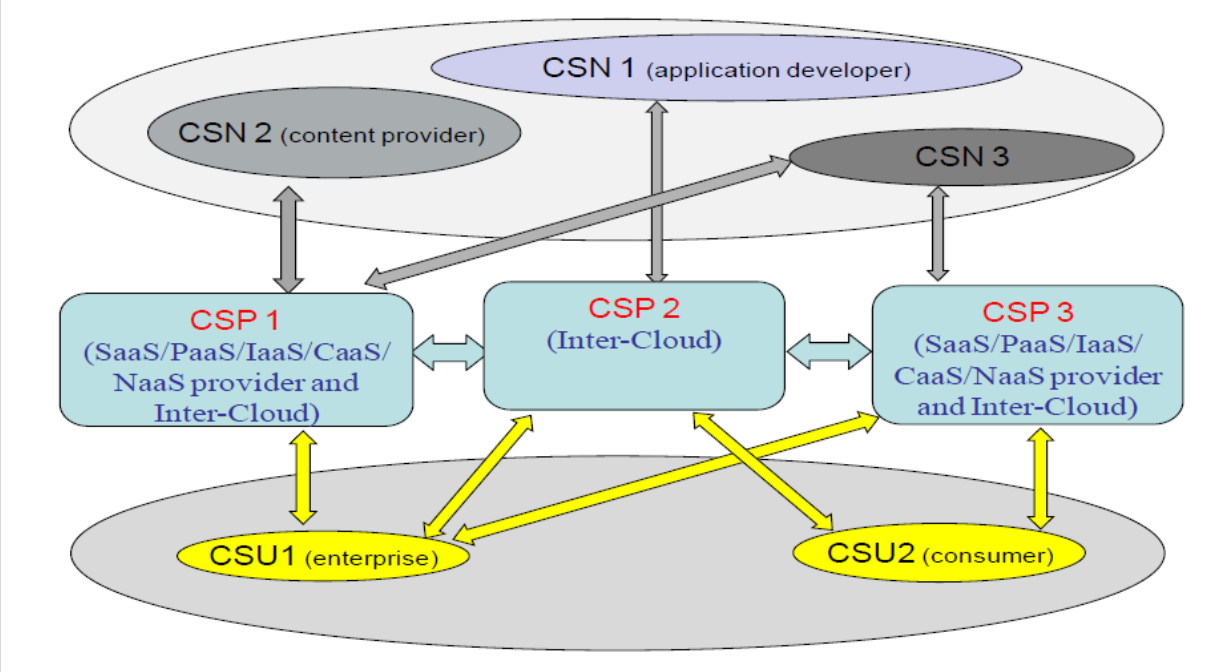
Another barrier for cloud computing is the availability of connectivity and sufficient bandwidth. Accessing a cloud service 'anytime, anyplace, anywhere' requires a robust telecommunications infrastructure and network access. The past 30 years of market liberalization and technical development have enabled this in many parts of the world, especially with the current deployment of broadband next generation networks ('NGNs'), satellite and 4G (IMT Advanced) wireless network infrastructures. However, adequate connectivity remains a problem in all countries, although it remains significantly challenging in the developing world.

For large users, enterprises and public authorities, the adoption of cloud computing is likely to be piecemeal. Users will trial services for particular applications, such as email, before committing wholesale to a cloud solution for most, if not all, their ICT needs. As such, interoperability and compatibility with legacy technology can also be a barrier for cloud users. In IT outsourcing, the provider will generally take on responsibility for the legacy technology and will migrate users on to any alternative solution. In cloud, the user often remains responsible for integrating the legacy systems and the cloud services.

Legal and regulatory uncertainty can also present a barrier to cloud adoption. In large part, these uncertainties arise in a 'public cloud' environment, where users are less able to influence the technical architecture that underpins the cloud service. Uncertainties about information ownership and control may inhibit users from placing their data with third parties. The transborder nature of cloud creates uncertainties about applicable law, similar to that for other internet services. A different jurisdictional approach to key legal issues, such as the protection of personal data between Europe and the US, can generate uncertainties about whether the use of cloud services can be carried out in a compliant manner.

The regulatory characterization and treatment of cloud computing may itself deter its take-up until regulators clarify the situation. Closely related to such uncertainty is the determination of competence in respect of the regulation of the cloud market. If viewed as a telecommunications service, then the telecom regulator can exercise jurisdiction. Conversely, if cloud is seen as an information service, then competence may lie with the ICT regulator, if there is one, or potentially the media regulator. Such sectoral regulation may then have to operate in conjunction and co-operation with horizontal national regulators, such as a data protection authority, in respect of certain issues.

Box 1: Actors with some of their possible roles in a cloud ecosystem



Source: ITU-T FG Cloud Technical Report Part 1, Introduction to the cloud ecosystem *(02/2012).*

3. Cloud markets

Since cloud services are varied, and becoming increasingly differentiated, so the markets that they supply are diverse, from wholesale to retail, business, public sector, as well as consumer. Increasing numbers of IT companies are either establishing new 'cloud' services or are recasting existing services as 'cloud'. The most common categorization of cloud services is into three: Software as a Service ('SaaS'), Platform as a Service ('PaaS') and Infrastructure as a Service ('IaaS'); although the label, 'X as a Service', is now being used for a range of different services[11].

SaaS primarily involves the use of remote applications by end-users, including productivity-related applications, such as Google Docs and Microsoft's Office 365; social networking, such as Facebook and MySpace, and the delivery 'over the top' ('OTT') content, such as video-on-demand services. PaaS are typically targeted at developers, enabling collaborative application development, such as open source software communities. IaaS generally involves the provision of virtual machines, offering processing and storage capacity.

The cloud computing market also comprises layers of different technologies, often supplied by diverse companies within the supply chain (e.g. Apple's iCloud SaaS is hosted on Amazon IaaS). Cloud users' depend on various 'service providers' for their use of the cloud, of which three broad categories are distinguished for the purposes of this paper[12]:

- A cloud service provider ('CSP'), who has a direct contractual relationship with the subscriber to the service, whether offering a SaaS, PaaS, IaaS or other variant;
- A cloud infrastructure provider ('CIP'), who provides the cloud service provider with some form of infrastructure[13], such as server farms and processing capacity, including persistent storage;
- A communication service provider, who provides the transmission service enabling the cloud user to communicate with the cloud service provider.

Usually, the cloud user will only contract directly with the cloud service provider and the communication service provider, the 'stack' of suppliers comprising the cloud service often being opaque to the user. This, in itself, may represent a risk for the user, since they may not be aware of the chain of contracts that underpin the provision of the service and, significantly, whether commitments entered into by the contracting service provider are adequately reflected down the supply chain. Alternatively, a user may contract with a systems integrator, which provides all aspects of the service, which is more akin to a traditional outsourcing arrangement.

4. Cloud as a regulated activity

How should cloud be characterized from a regulatory perspective? The answer to this question, as in many areas of regulation, is: it depends! The following examines some key areas of regulation, other than privacy and data protection, which are addressed in another GSR Discussion Paper[14].

4.1 Telecommunications law

Of the three categories of provider adopted earlier, clearly the communication service provider will be governed by telecommunication law, national, regional and international. Whether the cloud service provider or cloud infrastructure provider can be so characterized will depend on the nature of the service being provided. Under European law, for example, the primary regulated activities in the communications sector are the provision of 'electronic communication networks' and 'electronic communication services'[15]. The former comprise transmission systems, including 'switching and routing equipment' that enable the conveyance of signals; the latter consists 'mainly in the conveyance of signals'[16]. In many, if not most, cases, while cloud services are dependent on telecommunications networks and services for communicating with their customers, such services are not *per se* characterized as being networks and services. However, a cloud service provider may offer a SaaS application that provides call-handling functionality for an enterprise, which is analogous to a PBX[17], and this could be regarded an either a regulated network or service. In addition, the utility and shared nature of much cloud provision would also render it a 'public' network or service, thereby subject to a broader range of compliance obligations than applicable to equivalent 'private' services.

Uncertainty about the regulatory treatment of cloud services echoes previous experience with other emerging communication technologies, such as Voice over IP ('VoIP'). When VoIP applications first emerged in the mid-1990s for PC to PC communication, they were generally treated as a form of software, rather than a communication service[18]. As VoIP emerged as a major platform for voice communications across public networks and usage became widespread, there was recognition that uncertainty over its regulatory treatment created vulnerabilities for consumers, in areas such as network integrity and emergency call access, and market distortions, undermining the value of network investments carried out by traditional network operators[19]. In response to this uncertainty, regulators, such as those in the EU, kept a watching brief on market developments; developed a harmonized approach to the handling of certain emerging issues of concern, such as numbering, competition rules and applied existing regulations on a technology-neutral basis[20].

Drawing analogies between VoIP and cloud computing is limited to the extent that cloud computing services currently primarily provide remote alternatives to the desktop computer, i.e. terminal equipment at the edges of the network, rather than communication services. However, as noted above, some SaaS applications are specifically designed to replicate network functionalities, which places them within the regulated sphere of telecommunications. In addition, similar to VoIP, the 'born digital' generation may increasingly view cloud services, especially social networking, as the primary communication platform, utilizing 'always-on' connectivity services, which can give rise to regulatory concerns, such as interoperability and data portability, that are similar to issues addressed under telecommunications regulation, i.e. interconnection and number portability[21].

From a public policy perspective, it is arguable whether future telecommunications law may need to recast its traditional regulatory definitions and boundaries; shifting the focus from purely technical concepts, such as the transmission of signals, to a more market-based approach, encompassing the intention of service providers and expectations of the consumer.

4.2 Consumer protection law

In response to most market developments, comprehensive national consumer protection laws, governing issues from advertising to mandatory rights and obligations, will usually be sufficient to control unfair and abusive practices. However, such laws may need to be reformed and updated to reflect the general shift from traditional products and services to embrace the unique challenges of digital information and services, such as cloud.

In addition, sectoral consumer protection laws may also sometimes be necessary to address the particular needs of the sector. In telecommunications, for example, regulatory best practice has meant that most liberalized markets have adopted some level of sectoral rules governing the relationship between service providers and subscribers. Such consumer protection rules are generally designed to meet one of two objectives. First, certain rules facilitate market liberalization and help maintain competition from a demand-side, such as number portability and transparency obligations. Second, the nature of telecommunication as a 'utility-like' service[22], similar in kind to energy and water, has meant the governments have recognized the need to intervene not only to ensure access, through universal service policies, but also to regulate the terms of such access, through imposing minimum standards in the contractual relationship.

While the cloud computing market is not directly analogous to the telecommunications sector, policy makers have recognized a potential need to intervene[23]. On the one hand, as noted earlier, communications-like cloud services, such as social networks, are viewed by many as critical platforms from which to engage in social and economic activity, offering services upon which they are increasingly dependent. On the other, as noted below, market developments may result in the emergence of data-handling practices designed to inhibit consumers from exercising choice and moving between service providers.

As cloud services become widespread, consumer protection authorities are increasingly being called upon to intervene to protect the interests of consumers from abusive and deceptive practices. In the UK, for example, the Advertising Standards Authority has found against a cloud hosting provider who misleadingly advertised 'unlimited packages', when limitations in server capacity meant that certain customers had been unable to utilize the service[24]. Similarly, a web-hosting company was held to have mislead by claiming a '99.99 Uptime Guarantee', which it could not substantiate in the face of a customer complaint that they had suffered 3 significant network failures in a 3 month period[25]. While in France, a court has held that a Facebook user is not bound by the dispute resolution provision in Facebook's standard terms that requires all disputes be brought exclusively before "a state or federal court located in Santa Clara County"[26]. The court ruled that the provision was not brought sufficiently to the attention of the user to be binding, in breach of the French Code of Civil Procedure[27].

Another concern that cloud users may have when placing data in the cloud is the possibility of 'lock-in', where it becomes difficult to retrieve the data in a suitable format to enable it to be moved to a competing provider. Data portability is an emerging issue in the cloud computing sector that has relevance for competitive nature of the cloud market as a demand-side measure; similar in nature to number portability obligations in telecommunications[28]. Migration from one cloud service to another may be restricted pursuant to the terms of an agreement with a cloud service provider or difficult due to technical incompatibility[29]. Moreover, were a service provider to include in its standard terms conditions that constrain a customer from porting, replicating or backing-up data, this would raise concerns from a competition law as well as a consumer protection perspective. Such terms may be deemed to be in breach of competition law if they either are not necessary for providing the service, result in barriers to entry, distort competition and harm consumers. Rights of data portability would reduce lock-in effects and require competitors to compete for their existing customers as well as increasing their customer base.

The European Commission is aware of the potential harm that may arise from a customer's inability to port their data, but grounded in concerns about individual privacy, rather than from a competition law or consumer protection perspective. In January 2012, the Commission published a proposal to reform the current regime in the European Union[30]. Among other things, it contains a proposal that a right of data portability be recognized as an individual right within a privacy context. According to the Commission, an individual should have the right to withdraw his own personal data and "any other information provided by the data subject", from an application or

service and transfer such data into another application or service, as far as this is technically feasible.[31] To facilitate such portability, the Commission has reserved the right to specify the 'electronic format' in which the data should be provided, as well as the "technical standards, modalities and procedures for the transmission" of the data[32].

Recognition of data portability as an individual right *per se* would mean it is not necessary to evidence a resulting harm to competition. The Commission proposal suggests that the simple fact that customers are being prevented from transferring their personal data from one application or service to another would be enough to justify action aimed at forcing providers to guarantee data portability, if it would be technically feasible. Thus, regulating data portability in the cloud computing sector could prove to be more effective and straightforward via the enforcement of data portability rights under the umbrella of data protection policy than via the enforcement of competition law.

4.3 Competition law

Consumer issues concerning data portability may reflect broader concerns about the competitive nature of the cloud market, which may trigger intervention by competition regulators. Provider 'lock-in' may occur within any segment of the cloud market, SaaS, PaaS or IaaS, inhibiting the movement of data, applications and/or services. Anti-competitive effects may arise from a range of behaviours[33].

It can result from a lack of industry standards or, conversely, the development of de facto standard attributable to a marker leader, such as Amazon APIs[34]. Restrictive licence conditions may also as a result undermine competition. In April 2010, for example, Apple imposed restrictions pursuant to the terms and conditions of its licence agreements with independent developers of iPhone Apps. Apple required the exclusive use of Apple's native programming tools and approved languages for the development of iPhone Apps. Imposing such restrictions was considered by the European Commission as a conduct which could result in harm to competition for platforms that competed with Apple's Apps platform. As a result of preliminary investigations by the Commission, in September 2010, Apple voluntarily announced the removal of the restrictions, therefore allowing third-party application development environments to be used to submit Apps, resulting in greater flexibility to developers.[35]

Market participants in related sectors may constrain customers from move to a cloud platform. In July 2010, for example, the European Commission launched an investigation regarding IBM's computer mainframes.[36] IBM is being investigated for two practices in this sector: tying its mainframe hardware to its mainframe operating system and discriminatory behaviour towards competing suppliers of mainframe maintenance services.[37] IBM is being suspected of using its dominance in the mainframe operating system to leverage its position in the hardware market.[38] If proven, IBM's conduct is likely to make it more difficult for existing customers to migrate their data and applications to public cloud services, which do not require the purchase of vast amounts of hardware and software as IBM's private clouds.

Public procurement practices may be another source of anti-competitive behaviour. An example of this situation can be found in the US case of *Google v United States Interior Department*.[39] In October 2010, Google filed a claim against the U.S. Interior Department alleging that its public procurement practices illegally distorted competition by requiring, in relation to a US$59 million contract for ICT services, messaging technologies to be based on Microsoft Business Productivity Online Suite, therefore excluding Google from public procurements and restricting competition. The court granted an interim injunction in favour of Google and stated that the U.S. Interior Department's public procurement practices violated competition rules, therefore requiring the defendant to modify the procurement criteria.[40] Although the judgment did not find bad faith or wrong doing by Microsoft, it in effect brought to a halt the deployment of Microsoft's Business Productivity Online Services cloud computing solution and e-mail system at the U.S. Interior Department. The decision was intended to avoid lock-in effects and harm to competition given that without a preliminary injunction, the award would put into motion the final migration of Interior's email system, achieve 'organizational lock-in' for Microsoft, and cost Google the opportunity to compete.[41] The court therefore considered the possible harm to a competitor and to competition resulting from the network effects that would have been created by giving preference to Microsoft in public procurement.

Finally, it should be noted that there may be competition issues not only in the service cloud, but also in the infrastructure layers upon which cloud services are built and depend. In particular, there may be competition issues at the network level, which impinge on end-user access to cloud services, from unbundling issues to 'network neutrality'. Access to cloud services is provided by telecommunication companies that have historically been part of concentrated markets, which have developed from previous State-owned incumbent monopolies[42]. Connectivity, in terms of availability and affordability, is a concern not only in developing economies, but also in countries where the policy of market liberalization has not sufficiently eroded the market power of the incumbent operators. These issues are being addressed by telecommunications policy makers and regulators, through policies such as 'open access' that ensure fair and equivalent access for service providers, including cloud, to bottleneck facilities at an infrastructure level[43].

Telecoms regulators in many jurisdictions are highly experienced at working with industry to manage the process of number portability, especially in determining the technical, operational and cost implications[44]. As such, were data and application portability to be pursued as part of a policy initiative to promote cloud computing, whether under the auspices of competition law or consumer protection, it would obviously make sense to build on such experience.

4.4 Environmental concerns

As well as being directly subject to a regulatory regime, such as for telecommunications, the provision of cloud services may trigger other regulatory concerns. As noted earlier, one key advantage of cloud services is the efficiencies achievable by the cloud user in terms of equipment and real estate. On the other hand, however, the large data centers operated by CSPs and CIPs consume vast amounts of energy, which raises its own concerns in terms of energy and environmental policy. A recent report by MusicTank, for example, argues that 'close-to-consumer' cloud storage solutions may be needed to reduce the environment impact of online music streaming services. The report suggests that YouTube alone accounted for 0.1% of global energy consumption[45].

To address environmental concerns, steps have been taken to encourage the operators of such data centres to minimize energy usage whilst providing innovate services offerings. In 2009, for example, the European Commission issued a Code of Conduct on Data Centres Energy Efficiency[46] , which is a set of voluntary measures that may be adopted or reflected in the service contract, whereby the provider commits to achieving certain efficiencies in the design and operation of data centers. Such standards may eventually become mandated through legislation.

Mechanisms for reducing energy costs include building data centers where natural and passive cooling is available. In 2009, for example, Google was granted a patent in the US for the following invention:

> "a floating platform-mounted computer data center comprising a plurality of computing units, a sea-based electrical generator in electrical connection with the plurality of computing units, and one or more sea-water cooling units for providing cooling to the plurality of computing units."[47].

Distributed storage techniques widely used in cloud computing, such as 'sharding' or 'partitioning', mean that data processing loads can also be shifted to geographical zones where power is cheap. Similarly, the flexible architecture of cloud enables redundancy to be reduced to a minimum.

4.5 Jurisdictional concerns

An additional layer of concern for regulators is the transnational nature of cloud computing, which results in a multiplicity of jurisdictions potentially 'competing' to govern the regulated activity. The movement of data into and out of a cloud service will often, as with other network-based applications, result in the data becoming subject to the rules of both the cloud user's jurisdiction and the cloud service provider, as well as any cloud infrastructure providers. The transfer of data out of the user's jurisdiction can be opaque to the user, raising issues of control and, for the national regulator, effective oversight. For some regulated sectors, such as financial services, cloud-related transfers and storage outside the jurisdiction of the regulated entity may itself breach national rules[48].

Issues of national sovereignty mean that national regulators are unlikely to be willing to surrender jurisdiction to a foreign authority, unless adequate mutual recognition arrangements are in place[49]. As such, it will require greater transparency and co-operation between national regulators to resolve conflicts of law and regulation in a cloud environment.

5. Regulatory environment

Given the benefits of cloud, governments have an inevitable interest in both facilitating its adoption in the economy, as well as utilizing it for the provision of its own e-government activities, i.e. the 'G-Cloud'[50]. Government and regulatory intervention in markets can be designed both to constrain harmful behaviours as well as facilitate beneficial behaviours. As such, policy, law and regulation can play an important role in the facilitation of cloud services. This section examines different regulatory aspects in a cloud environment that is inherently transnational, from public policy responses to private law governance through contract; a form of self-regulation.

National telecommunication regulators can, in particular, play a key role in facilitating a regulatory environment conducive to cloud computing. In addition to their experience with respect to number portability, noted above, they will also generally have experience of developing and promoting industry standards and best practice, as well as consumer protection issues, specifically in relation to the provider-consumer contractual relationship. As such, governments should look to take advantage of this experience. While much of the cloud computing market may fall outside the competence of telecoms regulators, the critical need for extensive and robust network connectivity lies directly within their remit.

5.1 Regulation as facilitation

Governments and regulators can facilitate the development of cloud computing; while removing perceived obstacles to its adoption. By improving the environment for the supply of cloud services, the cloud market as a whole will grow. Policy makers are obviously cognizant of cloud computing and its potential economic and social impact and are considering the right strategy to embrace and harness the cloud[51]. The general principle appears to be, as with developments in relation to the internet, to ensure that what occurs in the cloud does not fall outside existing legal rules and controls: "The cloud must be a place where everyone's rights are duly respected and enforced."[52]

But what measures should governments take to facilitate the provision and adoption of cloud computing? The Business Software Alliance (BSA) recently published a survey of 24 countries to identify the level of 'cloud readiness' in countries, based on the domestic policies and initiatives towards cloud computing[53]. Each country was given a score based on an index of seven policy areas that the BSA considers beneficial to cloud adoption: privacy protection, information security, cybercrime measures, protecting intellectual property, ensuring data portability, liberalized trade rules and the necessary IT infrastructure.

The survey identified a sharp divide in cloud readiness between advanced economies, with Japan considered the leader, and developing countries, including India, China and Brazil. For India, poor progress towards a national broadband network is a key factor undermining the adoption of cloud. In China, its restrictive policy on Internet content and discriminatory approach to foreign technology companies is seen as presenting obstacles to cloud, despite dramatic growth in the ITC sector over recent years. Brazil is seen as lacking an appropriate framework for the development of ICT standards, as well as giving domestic service providers preferential treatment in public procurement.

Table: European Cloud Policies

In May 2012, the European Parliament published a study on cloud computing that identified five areas where policy makers should take action to facilitate cloud computing:

- *Address legislation-related gaps* – e.g. providing for the possibility of collective redress against security and privacy breaches in the cloud;
- *Improve terms and conditions for all users* – e.g. develop model contracts to ensure that user interests are better represented;
- *Address stakeholder security concerns* – e.g. the feasibility of independent auditing and certification systems;
- *Encourage the public sector cloud* – e.g. through integrating cloud computing in e-government plans;
- *Promote further research and development in cloud computing* – e.g. on the economic and environmental impact of cloud computing

Source: European Commission, Directorate General for internal Policies, IP/A/IMCO/ST/2011-18, May 2012

To what extent is cloud likely to offer developing countries opportunities for economic growth? In terms of the building of processing capacity, the large server farms that characterize current public cloud provision, developing countries obviously may offer relatively cheap real estate. However, in terms of access to reliable power generation and broadband communications, developing countries often lack the necessary infrastructure. While mobile penetration in Africa is substantial, fixed broadband penetration is insufficient, despite the recent landing of optical fibre submarine cables[54]. A recent study of cloud in Africa, produced a 'Cloud Readiness Index' based on a different range of primary and secondary factors than that used in the BSA survey, including Internet penetration, literacy rates and value lost due to electrical outages, rather than policies[55]. Unsurprisingly, South Africa ranked top, but with Zimbabwe, Sudan, Senegal and Kenya in the top 5.

A similar 'Cloud Readiness Index' for Asia evaluated 10 key attributes across 14 countries, including international connectivity, power grid quality, business efficacy and global risk, which incorporated the presence of earthquake fault lines[56]. It found that Japan led the region, with Hong Kong, South Korea and Singapore following closely behind, although for different reasons. Hong Kong was seen a becoming a data hub for north Asia, due to its international connectivity, with many data centres locating there. By contrast, South Korea's position was being driven by an ambitious cloud strategy involving government funding of up to US$2 billion by 2014.

In April 2012, the ITU published a study on cloud computing in Africa, which contained ten recommendations of measures to be taken to facilitate cloud computing:

1. *Effective regulatory progress* – including the need to adequately address data protection and security concerns;
2. *Maintain a regulatory watch* – to ensure that states are aware of regulatory best practice;
3. *Careful preparation of cloud computing outsourcing contracts* – including robust clauses on data security and availability;
4. *Conformity with existing provisions* – cloud contracts should also reflect other minimum regulatory requirements;
5. *Establishment of data centres in Africa* – to reduce the cost of bandwidth and increase speed of access;
6. *Quality of data centres* – to ensure data centres are service orientated, agile, automated, well protected and ecologically sound;
7. *Introduction and/or upgrading of regulation* – such as data protection laws
8. *The launch of training programmes*
9. *Cross-border standardization and regulation* – the need to participate in cloud standardization initiatives[57]

The successful implementation of these recommendations will depend on action by, and co-operation between, a range of government departments and regulatory entities, including telecommunication authorities. An effective data protection regime, for example, relies on a statutory framework supported by an independent supervisory authority. While it can facilitate trade in services with developed nations, particularly in Europe, a data protection regime also imposes additional costs on domestic businesses, which can be unpopular in the short term. Creating a favourable regulatory environment without recourse to overly bureaucratic interference is a challenge for all jurisdictions and regulators.

5.2 Contractual arrangements

Private law regulation through contract offers service providers and users a self-regulatory mechanism for generating a framework of legal certainty and security in cloud computing. Cloud contractual arrangements come in varying shapes and sizes, but will generally comprise four distinct components, whether in a single agreement or a set of linked documents (generically referred to as the 'cloud contract')[58]:

- Terms of service, detailing the key features of the relationship, both cloud-specific and general boiler-plate provisions (e.g. choice of law);
- Service level agreement, detailing the service features being provided, the standards that they should meet (e.g. service uptime) and any compensation mechanism where the standards are not met;
- Acceptable use policies, detailing permitted or impermissible conduct by users (e.g. copyright infringement);
- Privacy policy, detailing the approach taken to the processing of user data, particularly consumers.

The terms of a cloud contract can be distinguished into cloud specific-provisions and standard terms; although of equal importance in terms of defining the provider-user relationship. The former provisions generally focus on two key aspects, (a) the treatment of the data submitted by the cloud user into the cloud service, including issues of data ownership, integrity, preservation, disclosure and location; and (b) the specifications of the 'service' being offered to the cloud user, such as service availability. The standard terms will include such matters as provider liabilities, dispute resolution and applicable law.

From a public policy perspective, however, self-regulation through contractual agreements can raise concerns when market practice facilitates a situation where contracts do not present a fair balance of liabilities and responsibilities between cloud providers and users, especially SMEs and consumers. In this circumstance, regulatory intervention in the freedom to contract may be necessary to rebalance the relationship. In the telecommunication sector, regulation may determine, for example, the minimum contract terms offered to a consumer[59]; obligations to meet certain standards for quality of service[60]; and compensation arrangements for a failure to meet a performance standard[61].

In the consumer market, CSPs will generally dictate the terms on which the service is offered. Such standard terms and conditions are inevitably biased in favour of the provider, even though they may vary considerably according to the markets from which the cloud provider originates; e.g. providing hardware (e.g. IBM), software (e.g. Microsoft), outsourcing, communications services (e.g. Rackspace) or retail products (e.g. Amazon)[62]. At the enterprise level, a recent study suggest that service providers are increasingly being forced to negotiate agreements in order to win the business and, therefore, are conceding on issues in favour of the user[63]. The issues, on which most negotiation took place with respect to the terms of service, were provider liability, service level agreements, data protection and security and intellectual property rights. In terms of the mechanism of agreement itself, the right of service providers to unilaterally amend service features and termination rights were also key areas of dispute. The study suggests that while enterprise cloud contracts will remain distinct from the consumer segment, some of the concessions achieved in enterprise negotiations are likely to trickle down into the provider's standard terms of business[64].

Another obvious influence on the contractual environment for cloud services is the public procurement practices of public administrations, as they are often the single largest purchaser in the emerging cloud market. As public authorities embrace cloud services, such as for the provision of eGovernment services, they, similar to enterprise users, are in a good position to negotiate more favourable terms and conditions with cloud service providers. In the US, for example, the Chief Information Officer, within the Office of Management and Budget has issued best practice guidance for the acquisition of cloud services[65]. The guidance addresses the selection of a service, the service level agreement, end-user agreements, e-discovery and record-keeping issues. Inevitably, a key concern for the public sector is that of security in the cloud.

6. Ensuring a secure cloud

A secure cloud environment can be seen as having two main dimensions. First, the user will be concerned that the data, applications and resources are available as and when they are required. Second, users will want assurance that their data cannot be accessed and obtained by an unauthorised person. Availability may concern the data centres on which the data and service resides or the communication networks over which the data and services are accessed. While the former lies within the control of the CSP and will generally be addressed in the contractual agreement with the user, such as service level guarantees, the latter may lie beyond the control of either the CSP or the user, particularly when accessing over the public internet. The less robust the public internet, the greater the vulnerability of cloud users. As such, the communications infrastructure in developing countries is therefore a key factor in the take-up of cloud computing and sectoral regulators have a key role to play.

Responsibility for security obviously depends as much on the cloud user as the service providers[66]. Encryption, for example, may be applied by the communication service provider to create a secure transmission tunnel to and from the cloud service, while the cloud provider will generally encrypt the data being stored. The user, however, is also capable of applying their own layer of encryption to prevent any of the 'stack' of service providers having access to the data in an intelligible form, if there is a lack of trust[67]. Currently, however, while users can encrypt data while stored in a cloud service, it is not technically possible to maintain such encryption while actually processing the data in an application, which represents a potential vulnerability. In addition, for service providers to be able to provide support services to the customer, they may require access to user data in the clear. The proliferation and deployment of cryptographic techniques is a regulatory matter in many countries, e.g. under export control regimes, which may impact on cloud service provision as much as other uses of ICT. However, such issues are beyond the scope of this paper[68].

6.1 Information ownership

Cloud security is not only about data confidentiality, integrity and authenticity; it is also raises concerns about information ownership. In most legal systems, while information per se is not recognized as a kind of personal property, there are a range of legal entitlements granted over information, from personal data, such as data protection laws, to intellectual property rights, such as copyright and patents. In a cloud environment, users entrust their data to a cloud service provider, often located in a foreign jurisdiction. As such, users will want reassurance that such entrustment does not alter their rights in the submitted data, thereby undermining its value, or the rights of third parties, which could expose them to liability.

While a user will be seeking reassurance; from a CSP's perspective, they will require adequate contractual rights or licensed permissions to be able process and manipulate the submitted data in the normal course of the provision of the service, including generating multiple copies for security purposes. The scope of rights or permissions demanded by the CSP may be an area for negotiation in enterprise agreements, while creating concerns for consumers subject to a CSP's standard terms[69]. In addition, the CSP will generally demand warranties and indemnities from the user that they do not place any data into the cloud service without the relevant permissions, which could expose the CSP to secondary infringement liability.

An ownership issue may also arise with respect to the meta-data generated by the use of the cloud service and the information derived from this data[70]. For the CSP, the ability to derive value from this meta-data may comprise

part of the economic rationale for the service, hence the prevalence of 'free' services within the consumer cloud market, while cloud users may be concerned that such data can reveal their commercial secrets or personal data. Under the telecommunications law of many countries, controls are imposed over the ability of service providers to use the meta-data (e.g. 'traffic data') generated by customers through the use of their communication services[71]. Such controls recognize both the potential value of such data, as well as the potential for undue interference. As cloud computing becomes more widespread, consideration may be given to the need for similar such regulatory controls over the meta-data generated through the use of cloud services.

As noted above, one aspect of the uncertainty over information ownership in the cloud arises from the fact that the data will often be transferred out of user's jurisdiction to be held on servers residing in foreign jurisdictions, about which the user may have little, if any, knowledge about the legal rules. For governments, this risk to data sovereignty is often one they are not prepared take[72]. One innovative approach to addressing this concern has been to utilize traditional national and international rules governing diplomatic immunity[73] to extend the domestic law of the cloud user to encompass the physical data centers in the foreign territory where the cloud service is located[74]. While such an approach requires a willingness on behalf of the government of the country hosting the data centres to surrender sovereignty in this manner, it is an example of how legal techniques can be used to directly facilitate economic development.

6.2 Data retention and deletion

Mention has already been made in this paper of the potential concern that a user may have about their ability to port their data into and out of a cloud service, due to formatting constraints; as well as the data access rights necessarily granted service providers in course of the provision of support services. A third access-related issue is the treatment of user data once they have terminated a cloud service. From the user's perspective, they will have two concerns:

- Will they be given adequate opportunity to retrieve their data and applications from the cloud service?
- What steps will the service provider take to delete copies of the user data?

On the first issue, research has found that some providers offer customers a certain grace period following termination during which the customer can manage the transition of the data and applications out of the service; while others assert that data will be deleted immediately[75]. On deletion, some 'free' providers reserve the right to delete data in dormant accounts; while others retain data from terminated accounts for limited periods to enable customers to change their minds. What appears absent in most agreements is detail about the actual technical measures taken by providers to delete data, which could vary from allowing it to be overwritten over time, with the associated security vulnerabilities, to warranties of compliance with public standards[76].

Data protection regimes generally impose obligations that address both the retention and deletion of personal data. Such rules can be used to improve commercial practices in the area. Consumer protection law may also be used to ensure that consumers are not unfairly deprived of an adequate opportunity to retrieve their data upon service termination.

6.3 Security standards

Ensuring that cloud computing occurs in a secure environment is obviously not just a concern for users, but is also a concern for governments trying to facilitate the take-up of cloud. Security is obviously one element of the service being provided to the user; therefore it will be addressed in the contractual agreement. However, obtaining security assurances on a generalized basis, however, will require the development of standards against which cloud service providers can be judged. There are existing security standards that cloud service providers may adopt and utilize in a cloud context, such as ISO/IEC 27001 for information security systems[77] or SAS70[78], both of which provide for external auditing and certification. Secondly, cloud-specific standardization initiatives are being pursued, such as the Cloud Security Alliance[79], which is developing mechanisms, such as the CloudTrust protocol[80] designed to promulgate best practice in the industry and transparency for cloud users. Within the ITU-T, Study Group 17 has

been working on cloud security since April 2010, developing guidelines and requirements in a number of areas, including identity management[81]. The need for audit rights and accountability practices to be embedded in the cloud environment may be driven in part by the demands of regulators to which the cloud user may be subject, whether sectoral, such as in the financial services sector, or horizontal, such as data protection authorities.

A third source of cloud security standards is the public sector. In some countries, public authorities are beginning to adopt cloud computing solutions offered by the private sector, but only where those services have been externally accredited as offering sufficient levels of assurance[82]. Given the scale of public procurement on the market for IT products and services, such government-led security standards can be expected to have a significant influence on market developments. However, they may also generate an obstacle to the market for cloud computing if they are over-specified, undermining the cost benefits of cloud computing by imposing requirements for unnecessarily stringent standards; as recently noted:

> "Recognize that technology and process standardization that are an inherent part of the public IT cloud experience are among the fastest ways to reduce complexity and drive improved IT and business efficiencies; conversely, understand that opting for anything customized beyond the standard technology or process offered by a cloud service provider will quickly change IT deal economics back closer to what they have been in the past, before cloud."[83]

In addition, advisory bodies have published guidelines on security and privacy, designed to promulgate good practice without mandating compliance[84]. In Europe, ENISA, for example, identifies eight security-relevant parameters that should be addressed, measured and subject to specific procedures when negotiating with a cloud service provider, including service availability, incident response, data life-cycle management and log management[85].

6.4 Law enforcement access

When placing data in the cloud, users inevitably have concerns about unauthorised access to such data; exposing state or commercial secrets and breaching individual privacy. While such threats are viewed as primarily emanating from organized crime, access by law enforcement agencies in the course of an investigation (or indeed litigants in the course of a civil claim) has itself become a heightened privacy and security concern, particularly in relation to the threat of action by US authorities under the 'Patriot Act'[86] in a global market where US-based cloud providers dominate[87].

Cloud users, particularly from the commercial and public sector, will have three key concerns about law enforcement access to data held in the cloud. First, the data itself may represent significant commercial value, which needs to be protected from unauthorised disclosure. Second, the data will often be held outside the user's jurisdiction, subject to legal rules and procedures with which the user is unfamiliar, creating uncertainty about the governing framework. Third, the placing of data in the cloud may itself represent a breach of legal obligations owed by the user towards a third party, such as the data protection rights of customers[88].

As noted earlier, location independence and the use of shared resources is a feature of cloud-based services. For sensitive data, therefore, cloud computing may not offer a solution or at least the public cloud. Even where service providers offer users the ability to determine the location of their data, such as Amazon, which offers users the choice of placing their data in a Europe or US cloud, the reality of 'follow-the-sun' support for such services will generally mean that the data remains accessible by persons outside of the stated location. In April 2011, for example, Dropbox was forced to change the wording used in a 'help' article to reflect an amendment made to its terms of service. It had stated that "Dropbox employees aren't able to access user files"; part of the security assurances made to its customers relating to its use of encryption. However, its terms incorporate a provision enabling it to hand over user data in compliance with a valid court order, which required it to clarify that its employees are 'prohibited' from accessing user files, rather than being unable to access them[89].

While good security is key to the development of cloud computing, it also represents a new challenge for law enforcement agencies (LEAs) in terms of investigation criminality. On the one hand, accessing and obtaining forensic

material in a cloud environment raises issues about the legality and enforceability of LEA actions in as transnational environment. On the other hand, the tools that LEAs have traditionally used to obtain data may need to be updated to reflect the cloud environment. In Europe, for example, the European Telecommunications Standardization Institute (ETSI) is currently developing a draft standard for lawful interception of cloud services, building on previous standards developed for telecommunication providers[90].

The ability of LEAs to access cloud data will generally depend both on the legal framework in the requesting and requested jurisdiction, as well as the contractual terms under which the cloud service provider offers its service. Traditionally, the obtaining of evidence from a foreign country is carried out under treaty-based mutual legal assistance ('MLA') procedures, which ensure full judicial oversight. However, such procedures are notoriously slow and cumbersome, not suited to digital investigations. As a consequence, more flexible procedures were adopted in the Council of Europe Convention on Cybercrime[91] in 2001, which are applicable in a cloud environment. The Convention is an instrument of public international law and embraces over forty member state signatories, including non-European countries such as the United States.

As well as providing for MLA procedures, the Convention also permits a domestic LEA to obtain data from a foreign source without the need to go through MLA in certain circumstances. Under Article 32, a domestic LEA can obtain foreign data where the data is "publicly available (open source) stored computer data" or where the domestic LEA "obtains the lawful and voluntary consent of the person who has a lawful authority to disclose the data..". The latter is most relevant to a cloud environment and is concerned with the persons who have authority over the data. The cloud user could obviously grant authority, but is unlikely in the course of a criminal investigation. However, the cloud service provider will also generally reserve the right, in the user service contract, to disclose user data in certain circumstances. Such circumstances can range from a high threshold, such as the receipt of a valid court order, to a low threshold based on the service provider's discretion or perception of its best interests.[92] Whether a cloud service provider will disclose customer data will obviously depend on a range of factors, including the country making the request, the nature of the offence being investigated, and the type of the data being requested. However, as noted above, the current market dominance of US cloud providers has focused attention on the ability of US LEAs to access cloud-based data. From a user's perspective, preventing such disclosure in all circumstances is only possible where the user implements its own security measures, such as encryption, thereby rendering any disclosed data unintelligible. Otherwise, contractual procedures can be agreed with the service provider ensuring that, where permissible, the user is given prior notification of any request for disclosure, to enable them to pursue legal recourse preventing such action[93].

7. Proposed Recommendations

This discussion paper has examined the emerging trend of cloud computing and its regulatory treatment and implications. As with other areas of ICT development, regulation can facilitate the adoption of cloud computing by establishing an environment in which both providers and users have certainty and trust. Based on the preceding analysis, the following recommendations are addressed to regulators as representing some common practices, which may become 'best practices' for the regulation of cloud computing:

- **Broadband infrastructure and open access:** Cloud computing is dependent on an ample and robust communications infrastructure to which service providers have access on a non-discriminatory basis. Regulators need to consider taking measures to ensure that communication providers do not engage in conduct designed to, or having the effect of, constraining the provision of cloud services for reasons that are not transparent, objective, non-discriminatory and proportionate.

- **Cloud standards:** The development and widespread adoption of appropriate national, regional and international technical and organizational standards are required to address a range of concerns among cloud providers and users, including the integration of legacy systems with cloud interfaces; data and application portability and security.

- **Security:** The adequacy of the organizational and technical security measures implemented by cloud service providers has an impact beyond the interests of cloud users themselves. Two recommendations are made:

    - **Breach notification** – Providers should be obliged to notify relevant national regulators (whether sectoral or horizontal) and, in certain circumstances, cloud users when significant breaches of security occur that may impact, directly or indirectly, on the security of cloud user data.

    - **Standards, Certification and Audit** - Compliance with security standards requires external review and oversight not generally feasible on a per user basis. National, regional and international audit criteria and certification systems should be encouraged and endorsed.

- **Cloud transparency:** Cloud service providers should be obliged to notify users of the chain of providers that underpin the provision of the service to the cloud user.

- **Cloud contracts and service level agreements:** In a rapidly developing and diversifying marketplace, the terms under which cloud services are provided should generally be left to the parties involved. In the consumer space, however, consideration could be given to the drafting of model provisions addressing key issues of concern to users, such as quality of service, data portability and information ownership.

- **Consultative decision-making process:** National regulators need to consult with cloud service providers and other market stakeholders about the appropriate regulatory treatment and characterization of certain cloud services, with a view to issuing guidance providing legal certainty for market entrants and cloud users.

- **Regulatory co-operation:** Cloud services impact on a range of regulatory areas, both within jurisdictions and across multiple jurisdictions. Regulators should establish formal and information procedures to co-operate and co-ordinate regulatory decision-making that is targeted at cloud service providers, as well as be cognizant of the potential collateral impact that non-targeted regulations may have on the cloud market.

[1] E.g. NIST, 'The NIST Definition of Cloud Computing', No. 800-145, September 2011.

[2] ITU-T FG Cloud Technical Report Part 1, *Introduction to the cloud ecosystem* (02/2012).

[3] See further Bradshaw, S., C. Millard and I. Walden, "Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services" *International Journal of Law and Information Technology*, vol. 19, no. 3, 2011: pp. 187-223

[4] In telecommunications, the shift from circuit-switched to packet-switched network architectures represented a similar step-change in the efficient use of transmission resources.

[5] Francis Cairncross, *The Death of Distance*, Texere Publishing, 1997.

[6] Sun Microsystems White Paper, 'Introduction to Cloud Computing Architecture', June 2009, at 9. See also NIST, *Cloud Computing Synopsis and Recommendations*, No. 800-146, May 2012.

[7] See generally ITU-T FG Cloud Technical Report Part 7, *Cloud computing benefits from telecommunications and ICT perspectives* (02/2012).

[8] 'The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010', http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

[9] Vivian Reding, European Commissioner, July 2009.

[10] GSR 2012 Discussion Paper, *The Cloud: Data Protection and Privacy – Whose cloud is it anyway?*.

[11] E.g. HP refer to the cloud offering 'Everything as a Service', see http://www.hp.com/hpinfo/initiatives/eaas/index.html

[12] The ITU-T FG Cloud Technical Report Part 1 (02/2012) distinguishes three types of actor in the cloud ecosystem: the cloud service user, the cloud service provider and the cloud service partner (at 2.1.3).

[13] For the purpose of this paper, 'infrastructure' refers to any component of the cloud service, not an IaaS.

[14] GSR 2012 Discussion Paper, *The Cloud: Data Protection and Privacy – Whose cloud is it anyway?* See also ITU-T Technology Watch, *Privacy in Cloud Computing*, March 2012.

[15] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (OJ L 108/33, 24.4.2002).

[16] Ibid., at arts. 2(a) and (c) respectively.

[17] Public Branch eXchange. E.g. Interactive Intelligence, White Paper: 'A new approach to Communications as a Service (CaaS).

[18] See, for example, Walden, I., "The regulatory implications of Internet telephony", pp.226-231, *Computer and Telecommunications Law Review*, vol. 2, no. 6, 1996.

[19] ITU WTPF 2001, *Report of the Secretary-General on IP Telephony*, 31 January 2001.

[20] E.g. European Regulators Group, 'Common position on VoIP', ERG (07) 56rev2, December 2007. Available at http://erg.eu.int/doc/publications/erg_07_56rev2_cp_voip_final.pdf

[21] See generally the *Telecommunications Regulation Handbook* (10th ed.), IBRD, World Bank, *info*Dev and ITU, 2011.

[22] See, for example, Carr, *The Big Switch: Rewiring the World, from Edison to Google* (Norton: New York 2008).

[23] E.g. ITU-D, Regulatory and Market Environment, *Cloud Computing in Africa: Situation and Perspectives*, April 2012; European Parliament study, *Cloud Computing,* European Commission, DG for Internal Policies, IP/A/IMCO/ST/2011-18, May 2012.

[24] ASA Adjudication on UK2 Group, 29 February 2012. Available from www.asa.org.uk

[25] ASA Adjudication on WEBHOSTUK Ltd., 11 July 2012.

[26] See Facebook 'Statement of Rights and Responsibilities' (version dated June 8, 2012), at 16.1.

[27] Cour d'Appel de Pau, 1ère Chambre, Dossier 11/03921, *Sébastian R v Société Facebook Inc*, 23 March 2012.

[28] I.e. Directive 2002/22/EC (OJ L 108/7, 24.4.2002), art. 30.

[29] Facebook is an example of a cloud computing provider that does not allow its users are to move their data to competing providers. On the other hand, Google's Data Liberation Front is an initiative which intends to facilitate data portability to and from Google's products, http://www.dataliberation.org/.

[30] Commission proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11/4 draft, 25 January 2012.

[31] Ibid., at article 18.

[32] Ibid., at article 18(3).

[33] See generally Bornico, L., and Walden, I. "Ensuring competition in the Clouds: The role of Competition law?", *ERA Forum* (2011) 12, pp. 265-285 (8,453 words).

[34] Brockmeier, J., "Amazon APIs: Cloud Standard or Zombie Apocalypse?", 12 April 2012, available at http://www.readwriteweb.com/cloud/2012/04/amazon-apis-industry-standard.php

[35] See "EUROPA - Press Releases - Antitrust: Statement on Apple's iPhone policy changes," September 25, 2010.

[36] "EUROPA - Press Releases - Antitrust: Commission initiates formal investigations against IBM in two cases of suspected abuse of dominant market position," 26 July 2010.

[37] See Ibid.

[38] Ibid.

[39] See *Google Inc. and Onix Networking Corporation v. The United States and Softchoice Corporation* (United States Court of Federal Claims 2011).

[40] See Ibid.

[41] Ibid., para 25.

[42] See generally Walden, I. (ed.), *Telecommunications Law and Regulation*, 4th ed., OUP, 2012.

[43] See GSR 2011 Discussion Paper, *Open Access Regulation in the Digital Economy*, 2011.

[44] E.g. Body of European Regulators for Electronic Communications, 'Report on best practices to facilitate consumer switching', BoR (10) 34 Rev1, October 2010.

[45] MusicTank, 'The Dark Side of the Tune: The Hidden Energy Cost of Digital Music Consumption', 2012, available at http://www.musictank.co.uk/resources/reports/energy-report

[46] Available at http://ec.europa.eu/information_society/activities/sustainable_growth/docs/datacenter_code-conduct.pdf

[47] See http://www.google.com/patents/US7525207

[48] E.g. In Germany.

[49] As provided under European Union law.

[50] See, for example, http://gcloud.civilservice.gov.uk/

[51] E.g. Australia Government, *Cloud Computing Strategic Direction Paper*, April 2011.

[52] N Kroes, (2011) "The Role of Public Authorities in Cloud Computing", Aspen Institute IDEA Project Plenary, *Brussels, 24 March,* <www.aspeninstitute.org.> accessed 27 April 2012.

[53] BSA/Galexia, 'Global Cloud Computing Scorecard: A Blueprint for Economic Opportunity', 2012, available at http://portal.bsa.org/cloudscorecard2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf

[54] E.g. SAT-3 in Southern Africa, EASSy in East Africa and WACS in West Africa.

[55] Laverty, A., 'The Cloud and Africa – Indicators for Growth of Cloud Computing', available at http://theafricanfile.com/ict/the-cloud-and-africa-indicators-for-growth-of-cloud-computing/

[56] Asia Cloud Computing Association, *Asia's first 'Cloud Readiness Index'*, 7 September 2011, available at http://www.asiacloud.org/index.php/products/cloud-readiness-index/162

[57] ITU-D, Regulatory and Market Environment, *Cloud Computing in Africa: Situation and Perspectives*, April 2012

[58] Bradshaw, at 6.

[59] E.g. EU, Directive 02/22/EC on universal service and users' rights, art. 20.

[60] E.g. Nigerian Communications Act 2003, s. 104.

[61] E.g. Australia, Telecommunications (Consumer Protection and Service Standards) Act 1999, Part 5.

[62] Bradshaw.

[63] See Hon, W., C. Millard and I. Walden, "Negotiating Cloud Contracts – Looking at Clouds from both sides now", forthcoming in the *Stanford Technology Law Review*, currently available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055199

[64] Ibid., at p.42.

[65] CIO, 'Creating effective cloud computing contracts for the federal government', 24 February, 2012; available at https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

[66] See generally ITU-T FG Cloud Technical Report Part 5, *Cloud security* (02/2012).

[67] Kamara, S., and K. Lauter, "Cryptographic Cloud Storage", in Sion, R. and others (eds), *FC'10 Proceedings of the 14th International Conference on Financial Cryptography and Data Security* (Springer-Verlag Berlin, Heidelberg 2010), 136.

[68] See ITU-D report *Understanding Cybercrime: A Guide for Developing Countries*, March 2012, at section 6.3.11.

[69] However, public campaigning may sometimes result in changes to company terms. For example, as a result of previous controversies, Facebook recently put its proposed revisions to its 'Data Use Policy' and 'Statement of Rights and Responsibilities' to a vote of its users. See http://www.insidefacebook.com/2012/06/01/facebook-puts-proposed-policy-changes-up-to-a-vote-following-activist-campaign/

[70] See generally Reed, C., 'Information "Ownership" in the Cloud' (2010) Queen Mary School of Law Legal Studies Research Paper No 45/2010: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461

[71] E.g. Rwanda, Law N° 44/2001 of 30 November 2001 governing telecommunications, art. 24.

[72] See Irion, K., "Government cloud computing and the policies of data sovereignty (September 30, 2011). Available at SSRN: http://ssrn.com/abstract=1935859 .

[73] E.g. Vienna Convention on Diplomatic Relations (1961), *UN Treaty Series*, vol. 500, p.95.

[74] See http://www.wisekey.com/en/solutions/DataSovereignty/Pages/default.aspx

[75] Bradshaw, at 203.

[76] Ibid. E.g. BS EN 15713:2009 'Secure destruction of confidential material'.

[77] http://www.iso.org/iso/catalogue_detail?csnumber=42103

[78] American Institute of Certified Public Accountants, *Statement on Auditing Standards (SAS) No 70, Service Organizations*. It was replaced in June 2011 by *Statement on Standards for Attestation*

Engagements (SSAE) No 16.

[79] https://cloudsecurityalliance.org/

[80] https://cloudsecurityalliance.org/research/ctp/

[81] See http://www.itu.int/ITU-T/studygroups/com17/index.asp

[82] E.g. the UK HM Government has issued 'G-Cloud Information Assurance Requirements and Guidance', 10 May 2012.

[83] IDC, 'IT Cloud Decision Economics: 10 Best Practices for Public IT Cloud Service Selection and Management', July 2011.

[84] E.g. NIST, 'Guidelines on Security and Privacy in Public Cloud Computing', December 2011.

[85] ENISA, 'Procure Secure: A guide to monitoring of security service levels in cloud contracts', 2012.

[86] The full title is: 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001', Pub.L. 107-56.

[87] See the 'Top 100 Cloud Service Providers, 2012 Edition, available at http://www.talkincloud.com/tc100/.

[88] E.g. International Chamber of Commerce, Policy Statement 'Cross-border law enforcement access to company data – current issues under data protection and privacy law', Document No. 373/507 (7 February 2012).

[89] Sherman, M., "At Dropbox, even we can't see your dat- er, nevermind" (19 April 2011), available at http://www.bnet.com/blog/technology-business/-8220at-dropbox-even-we-cant-see-your-dat-8211-er-nevermind-8221-update/10077

[90] ETSI Draft Technical Report 101 567, April 2012.

[91] CETS No. 185, entered in force 1 July 2004 ('the Convention').

[92] E.g. Apple's the privacy policy for its iCloud service, states that it will disclose personal information if necessary "by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence", as well as where Apple "determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate." (www.apple.com/privacy).

[93] See further the discussion paper on the privacy aspects of cloud computing.

GSR 2012 Discussion Paper

The Cloud: Data Protection and Privacy

Whose Cloud is it Anyway?

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper to: gsr@itu.int by 19 October 2012.

The views expressed in this paper are those of the author and do not necessarily reflect the opinions of Charles Russell LLP, ITU or its Membership.

TABLE OF CONTENTS

1 THE CLOUD: DATA PROTECTION AND PRIVACY WHOSE CLOUD IS IT ANYWAY?

Author: Stephanie Liston, Senior Counsel (Charles Russell LLP)[1]

INTRODUCTION

"To secure the public good and private rights, against the danger of … faction, and at the same time to preserve the spirit and form of popular government, is then the great object to which our enquiries are directed"[2]

Like James Madison and the Federalists, new technologies engendered by the advent, growth and development of the Internet pose challenges for policymakers and regulators. Technical innovation itself is breaking down traditional barriers and creating significant commercial opportunities for economic growth and wealth creation.

The object of this paper is to consider, in the cloud: how to protect an individual's privacy and personal data? To what extent regulation is required to protect privacy? And, how to apply effective, efficient, clear, balanced and proportionate regulation in relation to cloud services provided over the Internet – a global communications network with no stop lights or zebra crossings.

Cloud computing has been recognised as a technology "game changer".[3] European Commission (EC) Vice President Neelie Kroes included cloud services with e-Health and ConnectedTV as offering huge benefits for citizens and businesses, and an overall boost to the European economy.[4]

Cisco has produced a global cloud index. It has predicted:

- "Annual global Cloud IP traffic will reach 1.6 zettabytes by the end of 2015. In 2015 global Cloud IP traffic will reach 133 exabytes per month.
- Global Cloud IP traffic will increase twelvefold over the next 5 years. Overall, Cloud IP traffic will grow at a CAGR of 66 percent from 2010 to 2015.
- Global Cloud IP traffic will account for more than one-third (34 percent) of total data center traffic by 2015."[5]

In terms of revenue, the global cloud computing market is forecast to grow 22 percent annually to US$241 billion by 2020.[6]

This paper will briefly consider the definition of cloud services together with their economic and social benefits[7]; current privacy and data protection regulation as applied to cloud services; the effectiveness of current regulation and enforcement to preserve privacy; and consider a fit for purpose regulatory model that effectively balances commercial needs and opportunities, technological reality and a citizen's reasonable expectation of privacy in an international digital eco-system.

1 *THE CLOUD: WHAT IS IT?*

1.1 Consideration of the Definition of Cloud Computing

The definitions of the cloud are many and various. They range from a simplistic statement that it is the use of virtual servers available on the Internet to anything consumed outside a firewall, including conventional outsourcing. Cloud computing has been compared to the supply of utilities such as gas and electricity. "The shift from local software to Cloud computing has been compared to the switch from local electricity generation to electricity grids in the 20th Century."[8]

This definition captures the essence of cloud computing:

- Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand.
- Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers.
- Charging, where present, is commonly on an access basis, often in proportion to the resources used.[9]

Clouds, by any definition, do not respect international boundaries unless they have to. However, with the type of personal data they hold, uploaded by individuals, businesses and governments it is fundamental that clouds are trusted and accepted – perhaps as much or more than a tax haven.

There are three primary types of cloud computing service models:

- Infrastructure as a Service (***IaaS***):
  A cloud based virtual server providing networking and storage services and other infrastructure services. The customer does not manage or control the data centre but may have control over the data or operating systems placed into the infrastructure. For example, Amazon web service or AWS.

  The market was worth US$1 billion in 2011 and is estimated to be worth about US$7 billion by 2013.

- Platform as a Service (***PaaS***)
  Where a customer can use its own applications on the Cloud Service Provider (***CSP***)'s infrastructure. The customer can control the data, the applications and part of the hosting environment.

  The market was worth US$2 billion in 2011 and is estimated to be worth about US$8 billion by 2013.

- Software as a Service (***SaaS***)
  This is the most commonly used form of Cloud services. Customer access the CSP's applications through the Internet. Facebook, webmail and other social networking sites fall into this category.

  The market was worth US$15 billion in 2011 and is estimated to be worth about US$17.5 billion by 2013[10].

These services do not necessarily respect clear boundaries. They may be layered, stacked or intertwined to create a particular or bespoke service model. Existing models have been described as private cloud, community cloud, public cloud or hybrid cloud:

- Private cloud refers to infrastructure owned by or operated for the benefit of one (typically large) customer. It can be located on or off the customer's premises.
- Community cloud refers to infrastructure owned by or operated for, a number of organizations on a shared basis. It supports a specific limited group of users with specific common interests, such as governments.
- Public cloud refers to infrastructure shared among a variety of users with no particular set of interests. It is sometimes described as "multi-tenanted". The infrastructure is owned by the organization selling cloud services.
- Hybrid cloud refers to infrastructure and services that incorporate two or more of the above. An example would be a bank operating a private cloud for sensitive data and putting other data into the public cloud to lower costs and extend capacity.

1.2 **Economic Benefits**

The demand for data storage is expanding dramatically with the exponential growth in data production, digital stores, digital libraries, digital archives, usage and retention requirements. The use of cloud services by individuals (webmail, social networking sites, e-commerce) is now part of everyday life in developed countries. Cloud services are used for wholesale or trade purposes (which is the primary focus of this paper) as well as for personal or individual use.

E-commerce brings people and businesses together internationally and has the potential to drive dramatic economic growth.

Governments looking at ways to economise and provide optimal services to its citizens in e-learning and e-health, for example, have the opportunity to use this technology to bring enormous social benefits.

Though there are infrastructure challenges in the developing world, such as lack of broadband access as well as power shortages and outages, the potential to use cloud services to increase educational opportunities and spread health benefits is enormous.

Basic commercial advantages of cloud services include:

- Lower costs of IT services provision because companies can share resources in one place; users can avoid expenditure on hardware and software; consumption is billed as a utility with minimal upfront costs; typically low, fixed periodic service charges; applications are updated without expensive upgrades; and the cost per user of cloud computing decreases as the number of users increases.
- Customers have access to a wide and growing range of applications without having to download or install anything.
- Access to the cloud is available anytime and anywhere.
- The cloud provides flexibility to accommodate increasing and decreasing demand. The customer only pays for the services it takes.
- Green objectives: pooled resources enable use of centralized and more energy efficient data centres and efficient energy supply strategies[11].

1.3 **Cloud Economics, Freedom and Flexibility v Personal Privacy and Data Protection**

There is a significant tension between the financial benefits cloud services offer to governments, businesses, citizens and consumers and the risks such services may pose to an individual's privacy or personal data.

Different stakeholders in the Internet domain value privacy differently. A Policy Department of the European Parliament commissioned a study which articulated the diverse views this way:

"… policy makers have an appreciation of its (privacy's) value because of the role that privacy plays in delineating and characterising society and supporting the exercise of certain other interlinked fundamental rights. Businesses and economic agents value (or, more commonly do not) privacy for the way in which it may enable or deny access to personal data. Finally, individuals can hold competing and at the same time contradictory estimations of what 'privacy' is 'worth' to them: for example – in an abstract sense recognising its importance in contributing to liberal democracy on the one hand, but trading it economically for benefits on the other."[12]

Generational differences may influence individuals' attitudes to privacy and their use of the Internet. The active use of Facebook and other social media sites have made the Internet a place to gather. Freely putting personal information in the cloud, has perhaps desensitised or undervalued an individual's personal information from the individual's perspective. But is this correct? Do consumers have enough information and knowledge about how this data might be used and the possible risk to its security. Personal data is being referred to as "the new oil" from a commercial perspective. Should consumers have an economic right to benefit from trading this data? And if so, what is the intrinsic value of the data?

To what extent should policy makers, regulators (whether ICT or data protection) and business co-ordinate to promote "Cloud Literacy"? If a citizen gives away or trades data in the cloud – an effective regulator should facilitate education of citizens and consumers as to the risks to privacy and their personal data when using cloud services, as

part of its regulatory agenda. The choice, of course, belongs to the individual, but it ideally should be an informed choice.

To what extent should policy makers around the world play a role in protecting personal data if the individual has willingly and knowingly provided it and no longer has a reasonable expectation that the information will remain private? Just as fundamental as an individuals right to privacy of personal information is the individual freedom and privilege to waive that right.

It is clear that the Internet and cloud services are becoming an increasingly significant business tool. However, without clear cloud standards and consistent regulation, trust in electronic transactions will be reduced and the potential benefits will not be achieved. The challenges are to balance the interests of stakeholders, policy makers, governments, businesses, citizens and consumers to arrive at a pragmatic approach to regulation. To be effective, the approach must be consistent, clear and proportionate. It must also acknowledge the global - not geographically confined – nature of the Internet, as well as the pace of technological change.

The next section will consider examples of the patchwork of differing existing regulatory models.

2 *DATA PROTECTION AND PRIVACY REGULATION*

2.1 Background

89 countries have adopted privacy or data protection laws.[13] A critical element of many of these laws is how they regulate international data flows as a mechanism for protecting individual privacy and enforcing national policies.

The Organisation for Economic Co-operation and Development (***OECD***) adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. Data protection laws were passed in a number of European countries in the 1970s. At a regional level, Convention 108 of the Council of Europe was passed in 1981 and the original EU Data Protection Directive was enacted in 1995 (***European Directive***)[14]. The European Directive places significant emphasis on the location of data; restricting its transfer to countries that do not have similar privacy protections. In contrast, the Asia-Pacific Economic Co-operation (***APEC***) enacted its voluntary Privacy Framework, which provides protection for personal data on an accountability basis in 2004.

When the OECD Guidelines were adopted, the Internet had not emerged. Protecting privacy by restricting the geographic movement of personal information was possible. The data was typically in a physical form – whether it be written, tapes or other physical medium. This continued to be the case in 1995 when the European Directive was implemented.

Business, the economy and technology have fundamentally changed. The economy is increasingly international. Data processing is growing dramatically in importance due to increased data usage and the value of different forms of data. The global economy is currently undergoing an "information explosion" which can "unlock new sources of economic value, provide fresh insights into science and hold governments to account."[15] The advent of the Internet and now the proliferation and potential value of cloud services require a careful re-evaluation of whether the provisions of these guidelines and regulations for the protection of privacy need to be fundamentally re-evaluated, re-constructed and harmonised to be "fit for purpose" at a global level.

The following is a brief review of the existing privacy and data protection frameworks in the European Union, generally, and as implemented in the UK, France and Germany; the United States; Canada; Brazil; South Africa; Japan and India. Countries have been chosen to reflect a diverse group, including both developed and developing countries. Europe is the initial focus and the most extensive because many countries who have adopted or are considering the adoption of data protection regulation have followed the European model. The model is also useful to illustrate the problems presented to business and the economy by the lack of clear and consistent laws implemented seamlessly across international borders.

The focus is on the aspects of the frameworks that are relevant and particularly problematic in the cloud environment. The aspects of privacy and data protection legislation that fundamentally affect cloud computing are (i) the duties of the party controlling the relevant data; (ii) transborder data transfer restrictions; (iii) data security; and (iv) applicable law.

The recent Global Cloud Computing scorecard published by the Business Software Alliance (***BSA Scorecard***) surveyed 24 Countries to map their relative "cloud readiness".[16] The scorecard rated seven policy areas the BSA determined

to be beneficial to cloud services. The study found a sharp divide between developed and developing countries. The Republic of Korea and Japan were high on the list, where as Brazil and South Africa were at the bottom.

This is a recent map providing an indication of where data protection laws are in place or in the legislative process.

PLC : General Counsel briefing: privacy & data protection as at 23 February 2011

2.2 European Union

2.2.1 Privacy

The fundamental principle of privacy in the European Union (EU) is set out in Article 8 of the European Convention on Human Rights which states that "everyone has the right to respect for his private and family life, his home and his correspondence." This right to privacy is not absolute, however, and can be restricted under certain circumstances.

EU privacy law itself has a particular focus on the protection of this personal data and seeks to balance the privacy debate in an era where online content, especially personal data and access to it have developed exponentially. The International Data Corporation (IDC) predicts that the amount of information and content created and stored digitally will grow from 1.8 zettabytes (ZB) in 2011 to over 7 ZB by 2015.[17]

Cloud computing is just the latest technological development driven by this expansion and in turn it brings fresh challenges to the protection of personal data. Data in the cloud may be easy to access and to manipulate, but it is also harder to locate and maintain control over - which makes compliance with EU legislation and, indeed enforcement, particularly difficult.

The EU's e-Privacy Directive[18] is targeted at public communication network providers and states that personal data should only be accessed by authorised personnel for legally authorised purposes, that stored or transmitted personal data should be protected against accidental or unlawful destruction, accidental loss or alteration and unauthorised or unlawful storage processing, access or disclosure. Communication providers are required to implement a security policy for the processing of personal data and national authorities are granted rights to audit such policies. Notification requirements for personal data breaches are also imposed upon the providers.

This has particular and high profile significance in the context of cookies which can be used by operators to gather personal data without the knowledge of the individual user. The amended e-Privacy Directive,[19] which came into effect in 2009, states that Member States may only permit the use of cookies if the data subject has given their consent and has been provided with clear and comprehensive information, particularly in relation to the purposes of the processing. It is unclear to what extent the legislation will be enforceable from a practical perspective.

2.2.2 **Data Protection**

The current European Directive applies to the collection and processing of personal data within the EU. Personal data is defined broadly as "any information relating to an identified or identifiable natural person," whilst processing involves "any operation or set of operations which is performed upon personal data".

The implementing law of an EU Member State is applied to the processing of personal data by an entity established within that state or by equipment situated within that Member State. Entities that determine the purpose and means of the processing of personal data are termed "data controllers", whilst entities that process the personal data on behalf of the data controller are called "data processors".

The European Directive specifies minimum measures to be implemented, leaving Member States the option of putting stricter requirements in place. This has resulted in significant variations in data protection laws across the EU, which cause complex and divergent compliance issues for businesses controlling or processing personal data in Europe, and in fact internationally (see section 2.3 below).

2.2.3 **Duties and Responsibilities of the Cloud Client and the Cloud Service Provider (*CSP*)**

Under the European Directive, data protection obligations are generally imposed upon data controllers, whilst data processors are only subject to specified security requirements. Differing Member State definitions and translations, along with the blurred categorisation of a CSP as a controller or processor make this ambiguity particularly significant.

The cloud client decides the purpose and organisation of any processing and thus, as a data controller, must accept responsibility for abiding by data protection obligations. The CSP will claim that simply hosting the service gives little control over the nature of any processing by the client and thus it cannot also be a controller. The lack of control means that the CSP will attempt to avoid liability for data quality, compliance with individual rights or the obtaining of any consents in relation to personal data and will often include provisions to reflect this within its terms and condition of service – which must be in writing.

The client is often responsible for the full burden of data protection obligations and compliance, despite having little control over the actions of the provider or movement of the data.

2.2.4 **Transborder Data Transfer Restrictions**

Under the European Directive, personal data must not be transferred to non EEA countries that are adjudged to have inadequate personal data protection measures in place. The European Commission (***Commission***) has deemed Andorra, Argentina, Canada[20], the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey and Switzerland to have adequate protection. The US Safe Harbor Scheme is also accepted as adequate for the purposes of transferring certain personal data, subject to some notable exceptions and now to specific due diligence.

Though there are some exceptions to the rule available, cloud computing is typically conducted without a stable location and providers are unlikely to be based only in the specified countries. The customer may not be able to ascertain the real time location of data that is being processed or stored. Of course, neither will regulators be obliged to enforce the restriction be able to ascertain this information.

The Independent Data Protection Working Party established under Article 29 of the European Directive (***Working Party***) has recently stated that the US Safe Harbor Certification alone may not be deemed adequate. Cloud providers should therefore obtain and retain evidence that certification is both up to date and their cloud provider is compliant with safe harbor requirements.[21]

If transfers need to be made to countries outside those that have "adequate" laws, Standard Contractual Clauses (***SCCs***) may be utilised. The SCCs contain non-negotiable provisions that set out transfer and security measures that have been deemed adequate by the Commission under Article 26(4) of the Directive. The benefit of using the provisions is reduced by registration and approval requirements that apply in some EU Member States. Registering or obtaining approval can be a very time consuming and bureaucratic process.

International businesses can adopt binding corporate rules (***BCR***) which require approval, for the regular transfer of data throughout their corporate networks.

2.2.5 **Data Security**

As data controllers, cloud clients have an obligation to take "appropriate technical and organisational measures to protect personal data"[22], thus data security forms an important aspect of the cloud computing contract.

The Working Party has put forward standardised data protection safeguards to be included in such contracts.[23] These safeguards include technical and organisational measures that aim to preserve the availability, confidentiality, integrity, ability to isolate, accountability, portability and individual rights to the personal data.

Accountability is particularly key to ensuring compliance and thus audit rights are becoming increasingly important to clients. However, the granting of these rights presents a practical problem for providers who use shared infrastructure for their clients. Granting access may itself compromise the confidentiality and security of data belonging to other clients.

Accountability can also be an issue in circumstances where sub-processors are used by the primary cloud provider. Most Member States leave the determination of appropriate technical and organisational measures to data controllers and processors. However, some Member States have prescribed onerous obligations - such as requiring data controllers to independently authorise each subcontractor and enter into direct contracts with all processors in the chain.

2.2.6 **Applicable Law**

The nature of cloud computing with shared resources, constantly moving data and multiple processors and subcontractors means that locating data and the processing of it is inherently difficult. The divergent implementation of the European Directive across the EU causes further problems when considering data protection compliance and which law or laws apply to its movement or processing.

2.2.7 **Compliance with Data Protection Requirements**

In a cloud service relationship, as outlined above, clients will typically bear the risk of data protection compliance despite the providers being responsible for the security and transferring of data. A controller must take appropriate technical and organisational measures to be confident of its compliance. Smaller businesses or individuals may have limited contractual power to negotiate the provider's terms.

Cloud clients are required to exercise due diligence with respect to choosing a provider who offers sufficient guarantees of reliability, competence and security safeguards for the client to be confident it is complying with relevant laws.

CSPs have an opportunity to differentiate their services and enhance business prospects by adopting terms of business and providing assurances to customers as to these processes and compliance. For example, Amazon has created a European Cloud to provide customers with confidence that data will not cross borders in breach of the European Directive. A number of self regulatory codes of practice are being established to address this issue (see section 3.3 below).

2.3 **Example of the Patchwork of Different Practises across the EU**

2.3.1 **United Kingdom**

In the UK, the Data Protection Act 1998 (the ***DPA***) forms the primary legislation that implements the Data Protection Directive. The DPA is regulated in the UK by the Information Commissioner's Office (***ICO***). The ICO's role is to provide guidance on data protection compliance, maintain a register of data controllers and investigate and sanction breaches of the DPA.

The UK Courts have narrowed the meaning of personal data in comparison to mainland Europe[24] so that for the data to be subject to the provisions of the DPA, the data must (i) be biographical in a significant sense; and (ii) "focus" on the individual, rather than some other person or transaction or event.

The ICO has wide ranging enforcement powers which include requiring the production of information; requiring a change of operating practices (a breach of which would be contempt of court); audit powers over central government departments, entry and inspection powers (with a court warrant) and monetary penalty notices of up to £500,000. Criminal sanctions are rare but remain available in certain circumstances, such as a failure to notify the ICO of a DPA breach.

Undertakings from a data controller's CEO are now also seen as a low cost method of enforcement. These undertakings state the failings of the company along with remedial steps that will be taken and are published on the ICO's website.

In the UK the Financial Services Authority is also able to enforce data protection breaches under its own regulatory regime under the Financial Services and Markets Act 2000 (***FSMA***). FSMA places wide obligations on financial services organisations including specific operational rules around data security and handling in its Systems and Controls Rules.

2.3.2 **France**

The implementing data protection legislation in France is the Data Processing, Data Files and Individual Liberties Act[25], as amended (the "DP Act"). This is regulated by the proactive National Commission on Computers and Liberties (***CNIL***).[26]

CNIL has published guidance on the legal processing of personal data which imposes notification and co-operation requirements on data controllers, as well as requirements to keep personal data secure and, in certain circumstances, to obtain CNIL approval prior to processing. Data subjects must also be kept informed of their rights.

There is no obligation to appoint an in-house or external data protection officer, although it is encouraged by the CNIL. Since 2005 more than 7,000 companies and a quarter of those listed on the Paris stock exchange have appointed a data protection officer.

The CNIL are active in regulating data processing and have powers to carry out audits and issue warnings or formal notifications to data controllers who do not comply with their obligations. Should the data controller fail to comply with the CNIL or breach the DP Act, the CNIL may impose an injunction preventing further processing or levy a fine proportional to the seriousness of the transgression. Fines for first breaches may not exceed €150'000, whilst a further breach within 5 years may be fined up to €300,000. Fraudulent or otherwise illegal data collection is governed by the Criminal Code and punishable by up to five years imprisonment and a €300'000 fine.

2.3.3 **Germany**

The use of personal data in Germany is primarily regulated by the Federal Data Protection Act of 1977 (*Bundesdatenschutzgesetz*) (***FDPA***) which has been amended so as to implement the Directive in 2001. Data protection regulations can also be found in the Social Act (*Sozialgesetzbuch*), the Telemedia Act (*Telemediengesetz*) and the Telecommunications Act (*Telekkommunikationsgesetz*).

The German national data protection authority is the Bundesbeauftragte Für den Datenschutz und die Informationsfreiheit (***BFDI***). Each of the federal states (*Lander*) also have their own regional data protection authorities. These regional authorities have recently been subject to scrutiny and restructuring to improve their independence following a European Court judgment in March 2010 which found that Germany had failed to implement the Directive correctly by placing the regional authorities under the state authority.

Personal data should be obtained directly from the data subject unless required by law for a genuine business purpose or if disproportionate effort would be required and there are no indications that the data subject's interests would be affected. Further, the FDPA puts particular emphasis on designing data protection systems to process as little personal data as possible such as through the anonymising or pseudonymising of the data subject. The data controller remains responsible for regulatory compliance and must have a written agreement with any data processor containing specific contractual requirements.

International data transfers are subject to the standard EU principles, save that since April 2010, German data exporters must check whether US data importers that have self-certified under the Safe Harbor scheme are actually compliant. The Working Party has recently endorsed this approach.

The BSA Scorecard points to Germany as an example of a country that threatens to undermine any advantage it may have had in being "cloud ready" by being overly restrictive in its interpretation of the EU Directive, requiring some data to be kept within national borders.

At least one German lawyer has noted that though the regulations are very strict in Germany, their enforcement is relatively lax[27].

Each regional authority can impose fines of up to €300,000 whilst non-compliance can be deemed a criminal offence with imprisonment of up to two years or fines possible. Fines should exceed the economic gain by the offender and may themselves exceed €300,000.

2.3.4 2012 EU Data Protection Proposals

On 25 January 2012, the Commission published its proposed reforms for data protection legislation within the EU.[28] The proposals contain a Regulation (for general and commercial data protection) and a Directive (for processing in the areas of police and criminal justice). The draft Regulation will replace the European Directive which is seen as out of date following numerous technological developments.

The proposals aim to increase an individual's online privacy rights and introduce new obligations on organisations. Contained within a Regulation, the changes will be directly applicable within the Member States in an attempt to harmonise the current "fragmented and outdated" data protection legislative framework. Co-operation between Member States is encouraged with the view that a single data protection regime should reduce red tape whilst ensuring that individuals and organisations are clear on their respective rights and obligations. It is also intended to make compliance more straight forward and consistent.

The key changes that have been proposed include:

- National regulatory authorities will have the power to take action against organizations in other Member States in certain circumstances and may issue fines of up to €1million or 2% of a company's annual turnover in some cases.
- An expanded definition of personal data that captures any information relating to a data subject and a requirement that an individual's consent must be explicit.
- The draft Regulation will have a wider application and include non-EU entities that process personal data that relates to EU citizens.
- Organizations will be required to report data breaches without undue delay and, if feasible, within 24 hours of the breach.
- There will also be requirements on data controllers to carry out data protection impact assessments, appoint data protection officers and inform third parties of any breaches.
- Individuals will be given a new "right to be forgotten" under certain circumstances and will no longer be subject to a fee for subject access requests.
- Finally, international data transfers will be subject to a more detailed regulatory framework requiring safeguards to be in place and authorities to undertake prior checks, whilst the derogations available to data controllers will be more restrictive.

The proposals were announced at the start of 2012. Their controversial nature has and will attract significant lobbying and debate which could mean long delays before implementation. Indeed, the UK Government is already reported to have stated that Member States should have more flexibility over the implementation of the reforms and has questioned the £3billion value of benefits projected by the Commission.

2.4 United States Privacy and Data Protection

US Legislation changed dramatically following the terrorist attacks of 11 September 2001 with the introduction of the US Patriot Act.[29] The US Patriot Act permitted the sharing of personal data of anybody suspected of involvement with terrorism or money laundering activities and introduced a requirement for financial institutions to implement anti-money laundering systems. This combination, in conjunction with multi-chain processes, has resulted in the

possibility of broad access and sharing of personal information. The US Patriot Act has been viewed by Europe as a significant risk to data privacy and has put the Safe Harbor scheme in jeopardy.

The right to privacy has been recognised by the US Supreme Court based on the US Constitution, despite there being no explicit constitutional right contained within it.[30] Many states have privacy protections within their own constitutions. Only California has extended the protection of data from government interference into an obligation on the private sector.[31]

The United States has spawned a wide range of narrowly applicable federal and state laws relating to the use of personal data. This patchwork, similar to the lack of harmony in Member State implementation of the European Directive, is incompatible with the nature of cloud computing. However, businesses and government are working to establish and implement credible self-regulation and guidelines.

Nationally, the Federal Trade Commission Act[32] (***FTC***) prohibits unfair practices. This has been applied to online and offline privacy as well as data security policies. The FTC also monitors and enforces any breach of the Safe Harbor Rules. However, doubts have been raised about the FTC's enforcement effort with respect to the Safe Harbor Rules. The FTC's first action for breach of the Safe Harbor principles was only in 2011 – against Google regarding its Buzz service, for not giving notice or choice to users when it used information collected through Gmail for different purposes.

The Financial Services Modernisation Act (***FCMA***) and Health Insurance Portability and Accountability Act (***HIPAA***) regulate the collection and use of financial and medical information, respectively. Among the range of federal legislation, there are specific acts that regulate, for example, the collection and use of email addresses[33] and telephone numbers[34].

At state level, there are many laws relating to data protection and most states have enacted some form of privacy legislation. Forty-six states have enacted laws requiring notification of security breaches involving personal data. California leads the way with a developed framework that includes an established Office of Privacy Protection and laws comparable to those in Europe. These include requirements for companies to maintain reasonable security measures to protect personal data[35] and to disclose details of third parties with whom they have shared the personal information[36].

There has also been a move toward a more European approach at federal level with the issuing of a Consumer Privacy Bill of Rights in February 2012. This is the first comprehensive privacy bill introduced to the Senate in over a decade. The bill sets out fundamental principles that companies should observe, namely that individuals should control the use of their data whilst maintaining access and correction rights; data use should be secure, transparent and consistent with the context of collection; there should be reasonable limits on what data is collected and retained and companies must remain compliant and accountable. There are also proposals for a national security breach notification law[37] and a requirement for reasonable security policies and procedures to protect computerised personal data.[38] These proposals signal dramatic change to American privacy laws. However, they are yet to gain the requisite support in Congress.

2.5 Data Protection in Canada

The Canadian Charter of Rights and Freedoms contains a right "to be secure from unreasonable search or seizure"[39] which the courts have extended to protect an individual's "reasonable expectation of privacy".[40] Recent case law from the Court of Appeal in Ontario has also introduced a common law tort of invasion of privacy or, specifically, "intrusion upon seclusion".[41.]

At federal level, privacy is regulated by the Privacy Act 1985 and the Personal Information Protection and Electronic Documents Act 2000 (***PIPEDA***). The PIPEDA applies to all regulated activities except where the federal government has determined that provincial law is substantially similar to it. Although the applicable legislation may differ, the relevant provisions will be similar. Provincial legislation that has been found adequate includes the Act Respecting the Protection of Personal Information in the Private Sector 1993 in Québec and the Personal Information Protection Acts 2003 of both Alberta and British Columbia.

Responsibility for personal information falls to the Office of the Privacy Commissioner of Canada at federal level, whilst certain provinces also have their own authorities. Standard exceptions to the application of the legislation apply, but in Alberta and British Columbia, personal information may also be transferred in certain business transactions (such as share sales) without consent, provided the parties comply with certain specified requirements. Consent in Canada may be express, implied or even deemed, depending on a narrowing set of circumstances. The

same sliding scale applies to the level of security requirements which will depend on the sensitivity and amount of information along with the method of its storage.

Canadian laws do not restrict international transfers of personal data. Any transfer remains the responsibility of the disclosing party who must ensure that appropriate protections are in place and the third party will abide by these protections. One aspect that may be considered is the location where the data may be held. Consent to the transfer must be obtained from the data subject, although this may be implied via consent to general terms and conditions. Provinces tend to impose additional requirements upon disclosing parties such as developing specific policies and taking reasonable steps to ensure security measures are maintained. There is also no approval procedure for data transfer agreements in Canada and, indeed, no standard form agreements have been approved by the national authorities.

2.6 Brazil's Data Protection Regime

Brazil is yet to implement specific data protection legislation although its Constitution does set out fundamental rights to both privacy and secrecy of correspondence.[42] The Civil Code also provides (i) that an individual may request relief from any threat to personality rights,[43] and (ii) that the private life of an individual is inviolable and judges may be asked to take steps to prevent actions contrary to it.[44]

There are also broad protections within the Consumer Protection Code.[45] These include consumer rights of access and correction to any recorded personal data, requirements for such records to be clear and objective with the recording of negative information limited to five years and a requirement for inaccurate data to be promptly corrected with the correction conveyed to any possible addressee within five business days. The Pubic Prosecutor's Office can enforce privacy rights whilst government authorities, such as the Bureau of Consumer Protection, can impose administrative fines of up to $1.7million if consumer rights are involved.

The current lack of legislation gives no reference or certainty to companies that process personal data and this, along with varying case law, potentially makes operating cloud services in or to Brazil unattractive. As a result, the BSA Scorecard has put Brazil at the bottom of the list of "cloud ready" countries.

A specific Brazilian Data Protection bill is now in the pipeline and Congress is soon to vote on the first reading of a bill that sets out a general legal framework for the Internet, the "Marco Civil da Internet" (***MCdI)***.

The MCdI is heavily based upon European legislation and covers Internet access, network neutrality, the liability of Internet services providers, data retention and the necessity of a judicial order for law enforcement authorities to obtain users' personal data. It places limits on collection and usage of personal data, with an individual's consent required for any processing, whilst companies would also have to notify a newly established "National Data Protection Council" (***NDPC***) in the event of a data security breach. This central authority would publish compulsory compliance recommendations and have powers including suspensions, prohibitions and media announcements. The MCdI also obligates personal data processing companies of more than 200 employees to appoint a data protection officer who would have to report directly to the NDPC and be responsible for all of the company's personal data processing.

2.7 South Africa's Data Protection Regime

South Africa currently has no specific data protection legislation but a right to privacy is set out within its Constitution. There are also relevant personal information provisions contained within the Consumer Protection Act 2008 (***CPA***) and the Electronic Communications and Transactions Act 2002 (***ECT***). Compliance with the latter is voluntary and any adherence must be recorded in an agreement with the data subject.

There is, however, a new Protection of Personal Information Bill (***POPI***) which is making its way through the South African Parliament. The POPI's aim is to regulate the processing of personal data and in doing so establish an Information Protection Regulator to oversee its administration. The final provisions of the POPI are subject to change, but personal information carries a broad definition, covering information relating to an identifiable juristic person, which includes corporate entities and trusts. Correspondence that is implicitly or explicitly confidential is also covered by the definition.

The POPI imposes eight mandatory information protection conditions upon data controllers: accountability; processing limitation; purpose specification; further processing limitation; information quality; openness; security safeguards and data subject participation.

Similar to the European Directive, the current draft bill prevents the international transfer of personal information unless specific provisions are met.[46] Such transfers are only permitted by a "responsible party" and subject to specific requirements. These include consent from the data subject; the international recipient being subject to laws or contracts containing comparable levels of protection to the POPI; the transfer being necessary for the performance of a contract to which the data subject is a party or that benefits him, or the transfer benefiting the data subject and it being not reasonably practicable to obtain consent (but if it were the data subject would be likely to give such consent).

A South African data protection regulator will not be established until the implementation of the POPI. Future failures to comply with notices under the POPI or obstructing the regulator will be punishable by a fine of up to ZAR10million or imprisonment of up to ten years.

2.8 Data Protection in the Kingdom of Saudi Arabia

The Kingdom of Saudi Arabia currently has no specific data protection legislation, although a right to privacy is established in a number of different Saudi Arabia laws. Saudi Arabia's Basic Law of Governance sets out the overriding principle that all correspondence and communications between parties should be kept strictly confidential and should not be disclosed. This overriding principle is supported by provisions contained in other legislation, including the Saudi Arabia Telecommunications Act issued under the Council of Ministers Resolution no. 74 (2001) (**Telecommunications Act**) and the Saudi Arabia Anti-Cyber Crime Law 2007 issued by Royal Decree no. M/17 (**Anti-Cyber Crime Law**). There are also particular laws and regulations in Saudi Arabia which provide for the protection of data and confidential information held by various entities, including financial and insurance institutions, hospitals and the majority of Government entities.

The Telecommunications Act regulates internet service providers and telecommunication companies in Saudi Arabia. It prohibits internet service providers and telecommunication companies from, amongst other things, disclosing any information relating to their subscribers and customers and from intercepting telephone calls or data carried on the public telecommunications network (Article 38.7). It also prohibits internet service providers and telecommunication companies from intentionally disclosing the information or contents of any message intercepted in the course of its transmission, other than in the course of duty (Article 38.13).

If no relevant legislation containing specific data protection and privacy provisions can be applied to the facts in question, the Saudi Arabia courts will apply Shari'ah or Islamic law. The Shari'ah principles establish a tort claim for damages for the wrongful disclosure of a person's personal information where that disclosure results in loss or harm to the individual. The degree of liability and penalties for breaching Shari'ah law relating to the protection of personal information will be determined on a case by case basis, although severe penalties may be imposed.

As indicated above, Saudi Arabia has no data protection authority or national regulator. However, the Telecommunications Act imposes a fine up to Saudi Riyals (SAR) 5,000,000 for failure to comply with the provisions thereof.

The Anti-Cyber Crime Law also imposes a number of civil and criminal sanctions relating to the breach of the privacy and data protection restrictions/ obligations contained therein, including:

- A fine of SAR 500,000 and/ or up to one year's imprisonment for the interception of data transmitted through an information network without legitimate authorisation;
- A fine of SAR 2,000,000 and/ or up to three years' imprisonment for the illegal access of bank data, credit information or information relating to the ownership of securities; and
- A fine of SAR 3,000,000 and/ or up to four years' imprisonment for unlawfully accessing computers to modify, delete, damage or redistribute personal information.
- A fine of SAR 3,000,000 and/ or up to four years' imprisonment for unlawfully accessing computers to modify, delete, damage or redistribute personal information.

2.9 **Data Protection in the United Arab of Emirates**

The United Arab of Emirates (**UAE**), a federation of seven entities each of which is subject to federal and local laws, currently does not have any specific data protection legislation, although a right to privacy is set out within its Constitution and in various UAE laws.

The UAE Constitution states that an individual enjoys "freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law." (Article 31).

In addition, the Penal Code (Federal Law 3 of 1987 as amended) establishes certain rights of privacy and the protection of personal data. These include the prohibition of the publication of news, pictures or comments pertaining to the secrets of people's private or family life, even if it is true (Article 378); the prohibition of the interception and/ or disclosure of correspondence or a telephone conversation without the consent of the relevant individuals (Article 380); and the prohibition of any person who because of his profession, craft, situation or art is entrusted with a secret from disclosing or using that secret for his/ her own or someone else's benefit without the consent of the person to whom the secret relates unless otherwise permitted by law (Article 379).

The protection of an individuals personal data and rights to privacy are also established in other legislation and regulations in the UAE, including:

- The UAE Labour Law (Federal Law 8 of 1980) which imposes record-keeping obligations on employers in relation to information pertaining to its employees;
- The UAE Cyber Crimes Law (Federal Law 2 of 2006) which prohibits "hacking";
- The UAE Commercial Transactions Law (Federal Law 18 of 1993) and The Electronic Transactions and Commerce Law (Federal Law 1 of 2006) which imposes record-keeping obligations on banks and commercial traders;
- The UAE Telecommunications Regulatory Authority Privacy of Consumer Information Policy which enshrines the right to the protection of personal information relating to subscribers/ customers by telecommunication service providers; and
- The UAE Medical Liability Law (Federal Law 10 of 2008) which provides for the protection of confidential patient information.

These UAE federal laws are often supported by emirate-level laws, particularly in relation to banks/ financial institutions and telecommunication companies and internet service providers.

It should be noted that there are a number of Free Zones established in the UAE, each of which is subject to its own specific regulations and procedures (including, in certain cases, in relation to data protection and privacy). By way of example, the Dubai International Financial Centre (**DIFC**) enacted the Data Protection Law No.1 of 2007 (**DPL 2007**) which governs the collection and use of personal data in the DIFC. It requires the data to be processed accurately, securely and lawfully and particular care should be taken when processing 'sensitive' personal data.

The UAE has no national data protection regulator or authority responsible for monitoring compliance with the data protection laws. It should however be noted that failure to comply with the data protection laws can lead to both criminal penalties (including imprisonment and/ or fines) and civil remedies.

In the DIFC, the laws and regulations contained within the DPL 2007 are administered and overseen by the Commissioner of Data Protection (**CDP**) (Article 7(1) and 21(2)). The DPL 2007 states that the CDP will need to conduct reasonable and necessary inspections and investigations before notifying a data controller that it has breached or is breaching the DPL 2007 (Article 32). If the laws and regulations have been breached, the CDP may issue a direction to the data controller to do or refrain from doing any act or thing (Article 32(1)); or to refrain from processing any specified personal data or to refrain from processing personal data for a specified purpose or in a specified manner (Article 32(2)).

In addition, the DIFC Court may issue orders which include remedies for damages, penalties or compensation if it thinks it is just and appropriate in the circumstances.

2.10 **Data Protection in India**

There is no specific constitutional right to privacy in India, although the Supreme Court has established that privacy should be included within the Right to Life and Personal Liberty.[47]

The collection and processing of personal data in India is regulated under the Information Technology Act 2000 (***IT Act***). The IT Act states that companies must maintain reasonable security practices whilst processing personal data[48] and if obtained under a contract, such data must not be disclosed in breach of that contract without the data subject's consent.[49] Consequently, international transfers are only subject to consent when data is obtained under contract. The IT Act does not provide a definition of a data controller nor does it include a specific requirement for the form or content of consent.

The Indian Government sought to clarify the IT Act by issuing guidance in April 2011[50] (***2011 Rules***) which stated, among other obligations, that written consent is required for the collection of sensitive personal data and that the processor of any such data must publish a privacy policy on its website. Parties must also comply with internationally recognised reasonable security practices.[51]

A Personal Data Protection Bill was proposed at the end of 2006 with the intention of harmonising data protection regulations within the country, establishing a data protection authority and creating a formal right to privacy. Commentators have said that clauses such as the protection of an individual's "honour and good name" make the protections too broad.[52] It is no surprise that the bill is yet to make it through Parliament.

In the absence of a dedicated Indian data protection authority, breaches of the IT Act are adjudicated by each state's Secretary of the Ministry of Information Technology who is granted sanctioning powers that include imprisonment of up to three years and a fine of up to INR500,000.[53]

2.11 **Japanese Data Protection**

Japan is a member of APEC and as such subscribes to its approach to privacy. The Act on Protection of Personal Information (***PPI Act***)[54] regulates the collection and use of personal data in Japan. Any form of data handling is covered, but the PPI Act only applies to situations involving the personal information of 5,000 or more individuals.

The PPI Act imposes common obligations of consent, security and providing information, alongside additional requirements to supervise employees and third parties who handle the personal data.[55] Consent is not defined, although it can be implied. Specific exceptions from the application of the PPI Act are also outlined. These include the handling of personal information for reporting the news, literary works, academic studies, religion or political related activities.

There is no specific provision within the PPI Act restricting the international transfer of personal information. Similar to the Canadian accountability approach, Japan puts the burden of compliance on the party having prime responsibility for the data. All transfers to third parties carry an obligation to supervise and, should the third party be using the data, consent from the data subject is also required.

The BSA Scorecard indicated that Japan would be an excellent model for those interested in advancing cloud computing. Japan's set of laws "support and facilitate the digital economy and cloud computing – from comprehensive privacy legislation that avoids burdens on data transfers and data controllers …".[56] Japan also leads in the development of international cloud computing standards.

Japan has no data protection authority, but the Consumer Affairs Agency has overall responsibility for deciding basic policy along with limited sanctioning powers such as making recommendations and, if necessary, ordering corrective measures to be taken. Enforcement falls to government departments which regulate data protection within their own sector. Failure to comply with the data protection laws can lead to sanctions from the relevant minister who can impose fines of up to JPY300,000 and six months imprisonment. Guidelines are also frequently issued, with the system relies heavily on self regulation and adherence to these recommendations.

2.12 **The Tension between Freedom and Regulation: Is the Current Patchwork of Regulation Fit for Purpose in the Cloud?**

The short answer is no. National regulation with respect to privacy and data protection was built 20 to 30 years ago. The advent in many countries of a global digital eco-system built on dramatic changes to technology was not foreseen by policy makers or regulators. It is now fundamentally outdated.

The development and deployment of services over the Internet and in the cloud typically cross national boundaries – it is not the exception! To restrict international data flows in the interest of protecting privacy rights is no longer an effective or efficient tool. The diverse set of rules across EU countries, for example, illustrates the complexity created for CSPs and their business customers (i.e. the data controller) to comply with the laws of each jurisdiction in which it operates. The effect is to slow down the growth of cloud services in Europe.[57] If there is not a shift in policy and regulation in Europe, and other countries followings its model, they will not be competitive in areas which should be a major source of economic growth.

The inherent difficulty of enforcing European and other similar transborder data flow restrictions gives rise to a lack of effectiveness in protecting personal data.[58] Policy makers need to address this problem by establishing frameworks which are cloud ready and provide efficient, clear and proportionate protections.

There is increasing confusion as to who has the duty to protect personal data. Clear lines of responsibility need to be established to allow stakeholders to understand and comply with requirements. One party in the chain of cloud activity must take responsibility and be accountable. Regulation should clarify rather than confuse the accountability issue. Individuals must have the absolute privilege to waive their right to privacy.

It is also unclear, in a global eco-system, which jurisdiction has authority to deal with a complaint. Consumers are left wondering who to complain to about services received in the UK, for example, but delivered from abroad. Businesses and CSPs face an equally daunting task of trying to discover exactly with which laws they are required to comply.

Significant security issues surround the development of cloud services. The person accountable for preserving personal data must have and take responsibility for ensuring they take steps to identify exactly how data processing will be managed and effectively protected. A risk assessment will need to be made taking into account practical physical storage concerns, location, technology that may be used to protect data and the ability to move data from one provider to another, as well as the right and ability to have data removed in accordance with applicable data protection regulations.

For cloud services to develop, CSPs need both freedom to innovate and clear direction. The advances being made in self-regulation[59] and the development of privacy enhancing technologies[60] present practical and effective solutions to protect privacy and enhance the security of cloud based services.

Section 5 below describes some best practice policies and recommendations for future data protection and privacy laws that reflect the reality of the international digital economy and promote economic growth while consistently and effectively protecting the privacy of personal information.

2.13 **The Opportunity Cost of Regulation**

Fundamental changes are needed to privacy and data protection legislation and governance to ensure they are fit for purpose over the next 10 to 20 years. Regulation is required to incentivise stakeholders to craft and provide their cloud services without unduly compromising the privacy rights of individuals whose personal data they hold and process.

Regulation in the national and regional patchwork form as found today, presents a muddy environment in which individuals, businesses and CSPs are trying to find their way. This confusion has at least delayed the take up of cloud services. Governments are carefully evaluating the use of cloud services – which could bring huge benefits in both cost savings and exciting developments in services such as e-health, e-learning etc. The Commission's initiative on government procurement - bringing regulators and stakeholders together - is a welcome step in advancing the contracting process and potential use of cloud services by Governments. The initiative may provide sufficient clarity and best practice to be adopted by the private sector.

The costs of compliance with diverse laws in multiple jurisdictions, however, seem unacceptably high. One report suggested that businesses comply with the most stringent EU Member State requirements and then could be relatively sure of complying with most other data protection laws.[61]

A balance also needs to be crafted between regulation for privacy and regulation for security. Moving personal information across borders will expose that data to possible interception by foreign law enforcement.

In many cases law enforcement requests may conflict with data protection laws, including in those of countries where the data originated or where it is stored. Such requests may also violate commitments made by companies to customers or employees, leading to potential legal liability and a loss of reputation. Political tensions may also arise between countries when authorities in one country request companies to disclose personal data stored in another one. The attendant legal and political issues, not to mention uncertainty, may discourage companies from investing in certain countries and may limit the free movement of data.[62]

These conflicts are particularly acute in the cloud – with increased cross border data flows and the expansion of illegal activity on the Internet.

Harmonisation of international data protection rules and co-operation between governments where rules are inconsistent would be the best solution.[63] The International Chamber of Commerce (***ICC***) has made a number of recommendations to governments and law enforcement authorities, including (i) taking into account the possibility that law enforcement requests may violate foreign data protection laws; (ii) making formal and specific written requests including the legal basis for the request; (iii) making cross-border requests for data stored abroad through mutual legal assistance treaties; (iv) giving companies the opportunity to evaluate the legitimacy of the request; (v) avoiding the requirement for companies to enter into supposedly "voluntary" agreements to deliver information and under threat of penalties and (vi) allowing companies to limit potential liability, by anonymysing or shielding personal data of parties that are not being investigated.[64]

The current conflicts and confusion in privacy and data protection regulation are having a significant negative effect on global trade and the take up of cloud services. Though many of the regulations are severe and cumbersome, the enforcement of regulations has generally been *ad hoc*. There are obvious difficulties in identifying the occurrence of a breach and proving same.

2.14 **The Role and Importance of International Co-operation**

Cloud services, whether provided to individuals through social networking or webmail or to businesses of any size or governments, are by their nature global. Governance models must take account of the international nature of the cloud. Technology is moving quickly towards further international expansion. For example, Google had patented floating data centres. Might they sport an EU Member State flag?

There are a number of initiatives underway that are fostering international co-operation. In 2009, data protection authorities from 50 countries approved the "Madrid Resolution" on international privacy standards.[65]

The standards proposed were international minimums. The principles were put forward in an attempt to achieve the greatest international consensus, with a view to influencing the development of legal and institutional structures for those countries yet to adopt a framework for data protection.

In particular, the resolution defined a number of principles and rights to guarantee the effective protection of privacy at an international level as well as ease the international flow of personal data essential in a cloud environment. The basic principles of lawfulness and fairness, purpose specification, proportionality, data quality, transparency and accountability were widely accepted. It is interesting to note that transborder data flow is not included in "basic principles", but set out in a different section. The proposal also expressed the need for supervisory authorities and co-operation and co-ordination of activities by different states, better compliance with applicable laws, limited international transfers of data – subject to consistent legal protections based upon relevant laws or contractual protections and offering awareness, education and training programmes.

A number of large companies welcomed the initiative and signed a declaration in support.[66]

The upcoming ITU World Conference on International Telecommunications in December 2012 will be a major treaty writing conference. The 1988 International Telecommunications Regulations (***ITRs***) will be reviewed and renegotiated. Some Member States would like to see a substantial increase in the scope of the Treaty. This could potentially include Internet and privacy issues.

In January 2012, Vice President Neelie Kroes proposed that public authorities and industry, cloud buyers and suppliers come together in a "European Cloud Partnership". The Cloud Partnership will propose common requirements for cloud procurement by looking at standards, security and ensuring competition rather than lock-in. At the second phase, the Partnership is to deliver "proof of concept resolutions" for the common requirements. In the third phase, reference implementations will be built. The Commission is investing €10million in the project. The project is directed at government Cloud procurement, but is expected to influence procurements by the private sector.[67]

As yet there is no universally binding privacy legislation covering all countries of the world. In Europe, as described in section 2.2 above, Member States have implemented the European Directive differently causing difficulty in compliance and significant administrative costs for operators. Though current proposals are intended to harmonise the approach, they do not go far enough to take account of the global nature of cloud services. The current US approach is also fragmented, with a variety of state and federal laws, mixed with self-regulation.

The ITU-T Technology Watch Report on Privacy in cloud computing[68] provides additional examples of privacy principles in other organisations and countries.[69] These include a description of the Odense Municipality case, a review of the EU Data Protection Directive; a definition of privacy by design and the use of PETs to implement privacy by design. Privacy by design generally refers to technical design of the processing system to integrate and implement effective privacy protection.

The Report identifies the three main privacy challenges in cloud computing as (i) complexity of risk assessment in a cloud environment, (ii) the emergence of new business models and their implications for consumer privacy and (iii) achieving regulatory compliance.

The Report also outlines the current work of the ITU-T SG 17 on cloud computing security. The ITU also set up a focus group on cloud computing security in 2010.

These steps are welcome as the lack of consistent and coherent domestic and international policies and regulation is having an unjustified chilling effect on the uptake of global cloud services. Policy makers, regulators and commercial stakeholders need to work together to develop standards, working practices, new technologies and educational tools which are "fit for purpose" in the changing global environment.

Section 5 outlines the options for future co-ordination and co-operation in the development of frameworks for the protection of privacy and data protection in a cloud world.

3 *ENFORCEMENT OF DATA PROTECTION AND PRIVACY LAWS IN THE CLOUD*

3.1 The Regulator's Role and Ability to Enforce Data Protection and Privacy laws in the Cloud

With the international nature of cloud services and the inconsistent international regulatory environment, the national regulators (both the ICT regulator and the specialized privacy/data protection agency), have a significant challenge. First – how are breaches of relevant laws to be discovered in the cloud? If discovered, will the national regulator have jurisdiction to effectively address the breach if it occurs outside its borders?

There are numerous laws following the European Directive restriction on transborder data flows. It is difficult, if not impossible, to know how well such a regulation can be enforced. There are still relatively few enforcement actions. "The fact that some of the largest economies in the world (such as China and Japan) have not been the subject of a formal EU adequacy decision means that there must be substantial non—compliance at least with regards to data flows from the EU to those countries."[70]

There is also a balance to be achieved between protection of personal data and national security risk that may give government a legitimate interest in having access to personal data. Particular concern has been expressed across Europe about the breadth of the US Patriot Act. To monitor the extent and potential threat of foreign governments having access to personal data, Google maintains a register of the requests it receives from governments. The most requests are received from the US, followed by India and Brazil.[71]

It is critical that individuals as well as businesses and other private and public bodies know which data protection rules regulate the protection and processing of data.

The Working Party adopted an opinion on applicable law (WP179) "to improve legal certainty, clarify Member States' responsibility … and ultimately provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller."[72]

Data controllers, regardless of location, may be subject to data protection laws of one or more Member States depending on the activities undertaken.

It may be challenging for businesses to assess which laws it should comply with. If a business operates globally, a clear understanding of the European Directive will be important and the adoption of BCRs may be appropriate. The European Directive continues to be influential in the development of data protection laws globally, including in Hong Kong (China), Dubai and developing countries – such as South Africa.

The draft European Regulation includes ambitious territorial scope, both within the EU (with regulators permitted to levy cross-border fines) as well as provisions requiring compliance by non-EU based organisations. It also includes mandatory notification of data breaches within 24 hours. It is unclear how these provisions will be enforced in practice.

These practical challenges raise once again the need for international co-operation and harmonization if cloud computing is to have the opportunity to grow as promised and to provide a significant catalyst to global growth.

3.2 Recent Examples of Enforcement Directives

3.2.1 UK[73]

- **ACS:Law**

  In May 2011, the ICO concluded its investigation into the law firm ACS:Law which had been involved in one of the UK's most high profile data breaches, involving some 6,000 data subjects.

  ACS:Law had acted on behalf of copyright holders within the music and adult film industries in pursuing illegal filesharers. In the process of doing so, the firm became the target of Internet activists and, due to inadequate I.T. systems, the details of the 6000 individuals and the names of the works they were accused of sharing were published on the Internet.

  The leaked information was a gross invasion of the individual's privacy and the ICO's investigation found that no one at the data controller had any IT qualifications, the IT system in use was not intended for business use and cost £5.99 a month, and there were no proper firewalls or access controls in place.

The ICO concluded that in the ordinary course of sanctioning, a monetary penalty of £200,000 would have been imposed. However, because ACS:Law was the trading name for a sole practitioner of limited means, the fine was reduced to £1,000. This reduction attracted strong criticism and even the theoretical level of fine was seen as particularly low in light of such a serious breach.

- **Torquay Care Trust**

  On the 6 August 2012 a health trust in Torquay was issued an ICO penalty of £175,000 after sensitive details of 1,373 employees were accidentally published on the Trust's website and remained there for 19 weeks. The ICO found that the Trust had no guidance for staff on what information should or should not be published online and had inadequate checks in place to identify potential problems.

- **Google Inc.**

  In November 2010, Google Inc. was required by the ICO to sign and publish an undertaking following the collection of payload data via its Street View mapping service.

  In collecting data for the service via publically available wi-fi signals, Google had also captured data from private individuals such as emails, URLs and passwords without their consent.

  The ICO chose not to impose a sanction and Google undertook to implement improved training measures on security awareness and data protection issues for its employees. Furthermore, any future project that involves significant personal data processing must have a compliance document from the outset and any data collected in breach would also have to be deleted.

  This name and shame approach was relatively soft in comparison to the sanctions imposed on Google for the same transgression in France, Spain and Italy.

3.2.2 **France**

- **Google Inc.**

  On 17 March 2011, CNIL issued a fine of €100,000 to Google following the same data collection issues encountered in the United Kingdom. In this instance the fine was for Google's failure to respond in a timely manner to CNIL's formal request in May 2010 that the company rectify its procedures. Google had undertaken to stop collecting the data and delete any data that it had collected by mistake. However, CNIL found that Google had failed to stop making use of the data and, although it had stopped collecting through its "Google cars", it had in fact continued to collect data through users' mobile phones.

  CNIL was invited by the Working Party to take the lead in the analysis of the new privacy policy that Google had undertaken to implement. In May 2012 CNIL announced that Google's answers to its questions were incomplete or approximate, that it was impossible to know Google's processing of personal data and that the obligation to inform data subjects was being ignored.[74]

3.2.3 **Germany**

Significant fines have been imposed by the German authorities in recent years. In 2009, **Deutche Bahn** was fined €1.1million for several breaches including illegal screening of employees' personal data.[75]

- **Google Inc.**

  Germany took a similarly soft approach to the UK in its treatment of Google and German residents were granted the opportunity to "opt-out" of the Street View system.[76]

3.2.4 **USA**

The FTC is the primary enforcer of national privacy laws alongside other national agencies that enforce privacy laws within their respective sector. The FTC Act provides for penalties of up to $16,000 for each offence along with imprisonment of up to ten years. The state laws of California are enforced by the California Attorney General and district attorneys.

Settlements are common in the United States and offenders may be issued onerous reporting, audit and monitoring requirements alongside monetary fines. Google may have escaped sanction from the FTC for Streetview but has recently received a record fine of $22.5 million by way of settlement for the placing of cookies on Internet browsers and misleading users who were led to believe they had opted out[77].

3.2.5 Canada

There are a wide range of enforcement methods contained within the various Canadian privacy statutes. At federal level, the Federal Privacy Commissioner has fairly limited investigatory powers and can make recommendations following violations of the PIPEDA. Provincial privacy commissioners tend to have increased powers including the ability issue fines and make binding orders.

The sanctioning of Google in May 2011 provides a good example of the limited powers of the Federal Privacy Commissioner. In comparison to sanctions for the same offences elsewhere in the world, Google was issued with recommendations including improved training of staff, adoption of a privacy governance model and deletion of the illegally collected data.[78]

3.3 The Value and Effectiveness of Self Regulation, Regulation of Commercial Relationships and Technology Solutions

It is critical to keep in mind the core value of personal privacy and data that relevant laws are trying to address and protect. In the current international data culture, the solution must be both practical and effective. The combination of cloud providers (i) establishing self-regulatory measures that address the data customer's concerns, (ii) crafting best practice contractual provisions; and (iii) creating and using security technologies to address security concerns; may well provide the best practical way forward to achieve the fundamental goal.

3.3.1 Progress in Self Regulation

There are three key reasons to increasingly rely on self-regulation with respect to on-line privacy and data protection:

- Self-regulation by CSPs who are most familiar with the technical aspects of cloud computing and the practicality of the delivery of cloud services facilitates global best practices. By integrating national and international privacy frameworks into a unified programme or code, CSPs and their customers will be in a better position to satisfy regulatory requirements and implement practical best business practices globally.
- Self-regulation evolves with technology. On-line privacy frameworks must be dynamic, like the technology they regulate. Conventional regulation is typically years behind, as discussed above.
- Self-regulation can provide strong incentives for compliance. They provide safe harbors to foster growth and promotion of best practices, which is in turn critical to the success of self-regulation.

A variety of voluntary and private sector mechanisms have been put in place in an attempt to comply with relevant regulations and provide the party accountable for the data with necessary assurances.

The US-EU Safe Harbor framework is a hybrid example of self-regulation. Companies can choose whether to adopt the framework. By self-certifying their compliance with the seven Safe Harbor principles,[79] US companies can assure EU organisations that the company provides "adequate" privacy protection for purposes of compliance. A company who self-certifies is then legally bound to comply. It is a hybrid regime because the FTC has the power of enforcement in the event of a breach of the certification. Perhaps this hybrid model of voluntary adoption of self regulatory codes coupled with enforceability by the appropriate national or indeed international regulator could be explored and considered for adoption as best practice.

Other codes of practice and standards have been implemented in Canada and Singapore. The International Organization for Standardization (***ISO***) is also working on privacy standards.

Cloud service providers have also taken measures to establish codes of practice to address the concerns of the data controller or accountable party. The Cloud Industry Forum (***CIF***) launched its Code of Practice in November of 2010. Following an extensive period of public consultation the CIF Code of Practice is intended to create a credible and certifiable code of practice that provides transparency of cloud services to allow customers to have clarity and confidence in the services, security and process used by the cloud provider.[80] It does not, however, have any legally binding effect.

The Cloud Security Alliance (CSA) is also promoting a code of best practice for providing security assurance in cloud computing and Cloud Audit is developing an application to automate the audit of cloud services[81].

In 2011, the American Institute of Certified Public Accountants (***AICPA***) established a Service Organization Controls (***SOC***) reporting framework to be applied to CSPs. One of the areas covered is privacy. The audit will examine whether personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments of the company's privacy notice and relevant accounting standards (ex Generally Accepted Accounting Principals (GAAP)).[82]

CSPs should be encouraged by policy makers and regulators to adopt clear accepted industry standards and best practice on technical, security and other critical issues relating to the services provided. Trustworthy and consistently applied certifications will go some way to address confusion.

The positive effect of the implementation of these codes and standard can be seen in the take-up by cloud providers. Autonomy (now an HP company) indicates on the first page of its Cloud Solutions marketing page that it "adheres to global certification standards, including PCI DSS, US DOD5015.02, UK TNA2002 and Australia's VERS." It also indicates that "its people, processes and technologies operate in compliance with Statement of Accounting Standard number 70 Type II (SAS70) and undergo annual SAS70 audits."[83]

The challenge for CSPs is to be able to demonstrate to business customers that their services will fulfil compliance standards the customer requires to be confident in trusting the service provider and being confident that the customer is complying with its responsibility as a data controller or accountable party.

In implementing such measures, the CSP will have to analyse the cost versus the benefits. The additional requirements could increase the cost of the cloud solution to the point that it is no longer a good business decision for either party.

In addition to self regulation and certification, the customer should, to the extent possible, look to establish clear contractual terms with the CSP. Of course, the customers' ability to negotiate the terms will depend on the customers' position and bargaining power.

3.3.2 Contractual Solutions

The contract entered into between CSPs and their customers should, to the extent possible, present a clear set of rights and relative responsibilities of the parties.

The European Directive has used private contracts as a critical tool in allowing transborder data flows. International business can adopt Binding Corporate Rules and standard approved clauses may be included in contacts between the CSP and data controller to assure compliance with relevant data protection laws. This is an interesting and effective regulatory tool.

The most challenging area for CSPs and customers is when SaaS is chosen as the cloud service. Typically SaaS vendors will have many contracts globally. They are typically for off the shelf solutions and used by individuals or small and medium sized business. The terms are typically published on the CSP's website, are very supplier centric and may be accepted electronically. They exclude all but the most limited warranties and any liability for data loss, corruption or service failure. Cloud customers who are data controllers must try to choose CSPs that will guarantee or assure their compliance with applicable law through due diligence. The introduction of self regulation and certification processes will assist in this process.

The best customer solution is to seek negotiated terms which would include service levels, service credits, data back up to preserve data from loss and agreement by the CSP to take data out of its system. Of course, this increases the cost of the service and may not be practical for smaller businesses.

The Working Party has recently provided recommendations for businesses and government administration wishing to use cloud computing services.[84] The Working Party recommends the data controller conduct comprehensive due diligence and risk analysis of the proposed service. Due diligence

with respect to cross-border transfers must be particularly robust. The process will require knowledge and action by the purchaser as well as co-operation from the CSP.

The opinion also provides guidance on the contractual arrangements that govern the commercial relationship between the customer and CSP with respect to privacy and security.

The contract shall provide for:

- appropriate transparency regarding data handling processes;
- isolation of personal data so that the personal data may be amended or deleted by the data subject;
- appropriate security measures to ensure availability, integrity and confidentiality.

Specific contractual safe guards have also been proposed, including sufficient guarantees of technical security and organisational measures, detail the customers instructions including time frame, subject and SLAs, limitation of people who have access to the data, when disclosure to third parties is permitted and on what terms, obligations for the CSP to co-operate with its client regarding monitoring and facilitating the rights of data subjects, guarantee of lawfulness of cross border transfers, definition of the logging and auditing of the data processing and identifying and delineating appropriate technical and organisational measures to manage the risk of lack of control.

In addition to these specific requirements, the contract must include the controller's instructions to the processor, obligations with respect to security measures, specifications of the conditions for destroying or returning data and obligation to provide a list of locations where data may be processed, as well as measures facilitating accountability, such as third-party audit and certification.

Helpfully, the Working Party endorses third-party certification as an acceptable means of proving compliance. This will obviously help to streamline and cut the cost of the customer's due diligence.

In addition to self-regulation and certification and carefully considered contractual terms, a third and critical form of effective protection of personal data can be found in the growth and development of privacy enhancing technologies (***PETs***).

3.3.3 Technology Solutions

The number of PETs have been increasing. The use of these technologies will potentially provide the data controller or accountable person with practical and effective means of being confident of its compliance. Examples of PETs include a variety of encryption models, technologies hiding the correlation between input and output data, private authentication protocols and anonymisation techniques to name a few[85].

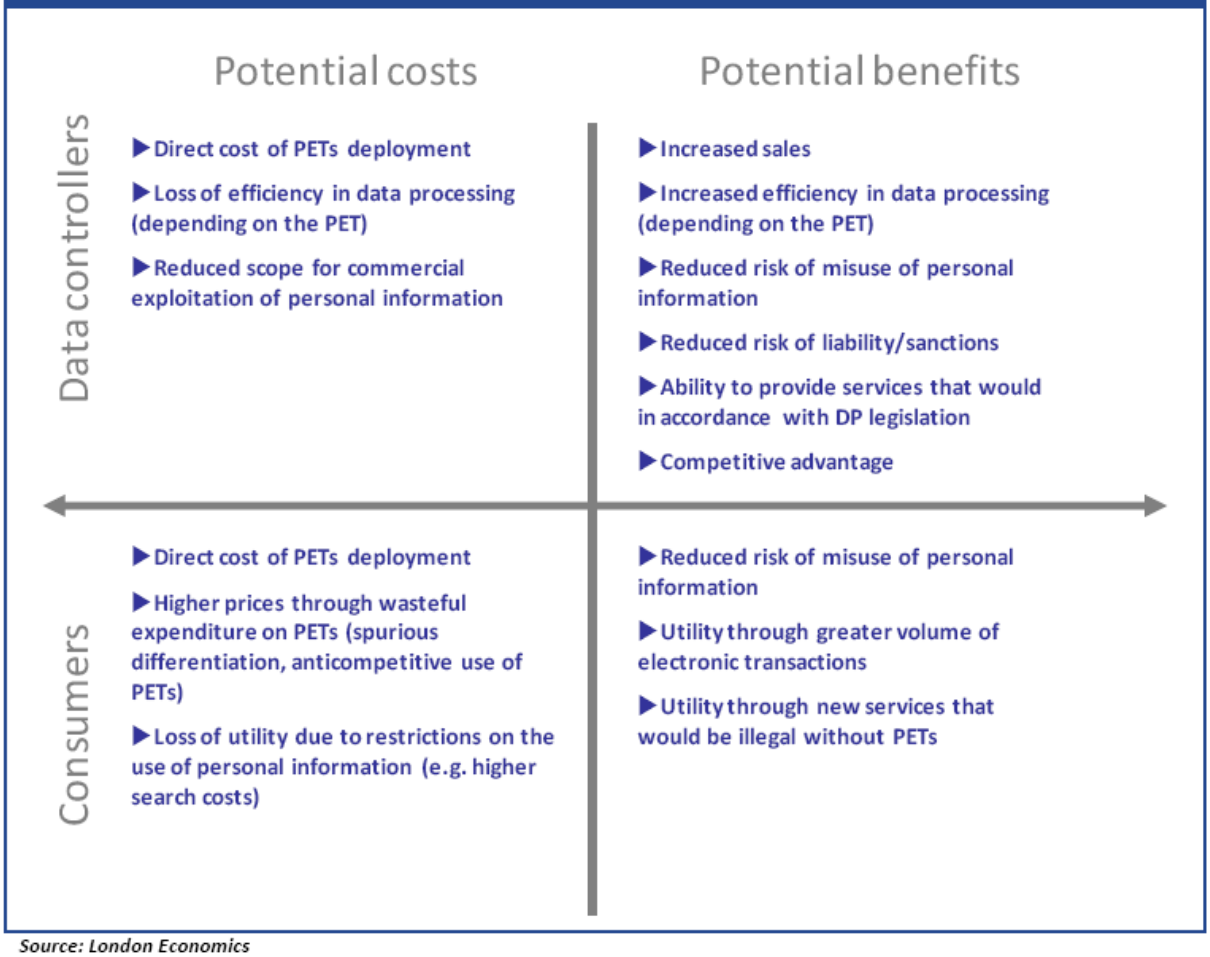
Companies like TRUSTe are rolling out new technologies and platforms that offer privacy solutions. For example, it has developed an EU Cookie Audit, which detects and reports on all first and third party tracking mechanisms present on a website.

New businesses are springing up as "cloud access security brokers". Perspec Sys, for example, provides a gateway allowing the customer to select its data protection policies, such as encryption or tokenization in a single platform. The platform is vendor-agnostic and supports multiple clouds. Consequently, concerns about vendor lock-in are addressed technically.[86]

The challenge, of course, is to increase awareness and take up of PETs. London Economics has indicated that "Market imperfections, which can include asymmetric information, externalities, lack of information sharing about privacy risks and co-ordination failures, mean that the individually rational decisions of data controllers do not necessarily lead to the optimal level of PETs deployment."[87] This essentially indicates current market failure. There is clearly a role for policy makers and regulators to overcome these barriers.

London Economics has analysed the costs and benefits of PETs deployment as follows:

Figure 1: Potential costs and benefits of PETs deployment



Source: London Economics

88

4 ARE THE ISSUES DIFFERENT IN THE DEVELOPED V. DEVELOPING WORLD?

4.1 The Infrastructure Challenge

While developed countries debate the best practice privacy and data protection regulations to meet in the cloud, most developing countries are struggling – to differing degrees – with more basic obstacles to the development of cloud services. The three key market segments of mobile, Internet and broadband are critical to delivering cloud computing. Obstacles in many developing countries (and particularly in Africa) centre on lack of infrastructure and government policy. In addition, the combination of power shortages and inefficiencies generally stall development. Mobile penetration is significant, but broadband penetration tends to be low.

4.2 The Opportunity

The ITU, the World Bank, the EBRD and other development agencies are keenly interested in ICT for Development. Cloud computing is potentially at the centre of this opportunity. Critical assistance can be provided in e-education, e-health, e-commerce, e-governance and e-environment and telecommunicating. The cloud may also provide an opportunity for business to by-pass traditional trade bottlenecks, corruption and inefficient bureaucracy. To deliver these benefits in the developing world, pieces of equipment and software must come down in price and governments must have access to financial resources and education to run their IT systems.[89]

Laverty uses the development of mobile applications as a current example of the enormous opportunity to create links between the developed and developing world that were "unimaginable before cloud computing". "A developer in Rwanda can use web based applications to create and test an app for the iPhone and then publish their completed work to Apples' App Store where any iPhone user in the world can purchase the app and download it".

4.3 Lack of Privacy Protection

Privacy International has expressed concern about the lack of adequate legal and institutional frameworks and safeguards. Without them, both corporations and governments can collect and share personal data in the name of development.

"In many developing countries the framework for the protection of personal information are either at a nascent stage, are not implemented or enforced, or simply do not exist at all".[90] Concern was expressed about the collection and storage of biometric information and the use of ID cards. The use of such information could range from identity theft, social sorting and criminal investigations.

It is critical at this stage in the development and rollout of cloud services that as part of the international ICT development agenda, practical and effective privacy regulation be an integral part of the process of investment and enhancement of services that are delivered in developing countries.

A balance must be struck between advancing development through the use of ICT, particularly cloud services, and the need for education regarding the risks and benefits of the services as well as regulation to preserve this fundamental human right of privacy.

As the cloud is evolving in developed nations – developing nations must not be left behind. The implementation of appropriate policies that both encourage investment, while protecting personal rights will be critical.

If a coherent and consistent international approach can be established to privacy in the cloud, the appropriate international organisation would be in a position to propose model laws which would move the process of take up a major step forward.

Government, policy makers and regulators need to look to the future and particularly the fundamental role and importance of international co-operation. They need to focus on the development of best practice privacy and data protection policy that preserves an individuals' rights while avoiding confusion, lack of clarity and a "heavy hand". A balance must be struck between all stakeholders that does not have a chilling effect on innovation or freedom of the Internet and cloud computing.

5 *THE FUTURE: HOW CAN DATA PROTECTION AND PRIVACY REGULATION KEEP PACE WITH TECHNOLOGY AND BE BOTH EFFICIENT AND EFFECTIVE IN THE INTERNATIONAL CLOUD CULTURE*

5.1 Best Practice Policy in the Development of Data Protection and Privacy Laws in the Cloud Eco-system

The challenge for policy makers is to balance the commercial need and individual desire for free flow of information with informed knowledge and effective control by individuals of their personal information. Clear and consistent policies need to be developed based upon current and prospective technologies. The opportunities for growth and development should not be hindered by unnecessary regulatory barriers, administrative burdens or choice of law or applicable jurisdiction issues.

The first and most important hurdle is to raise the opportunities and challenges presented by international transfers of data to the top of the agenda of national, regional and international policy makers. As the "new oil", "ministers and government officials should grant international data flows the same attention as they do international flows of capital and international trade. . . These topics are in many ways inseparable, since the ability to transfer personal data internationally is a vital component of the globalized economy."[91]

CSPs and businesses should be actively consulted and involved in the development of policies relevant to the provision of cloud services. Businesses should consider implementing research and effective cloud protection plans. Investors should consider where best to locate their cloud business. If we compare the cloud to a shared office building – what terms and conditions should be implemented? With CSPs delivering the digital economy, governments and regulators should consider offering cloud friendly investment policies while ensuring an effective framework for privacy and protection of personal, business and government data is in place.

In an effort to demystify privacy and data protection issues in the cloud, studies have been commissioned and information is being gathered on various subjects including, for example, best practice government procurement[92] and PETs[93] and the European Parliament's 2011 study "Does it help or hinder? Promotion of Innovation on the Internet and Citizens Right to Privacy."

In addition, individual attitudes must be explored and taken into account. After all, whose personal data are we trying to protect? What responsibility should individuals take for disclosure of their personal information. Individual attitudes are typically measured and identified by way of opinion polls. The 2011 Special Eurobarometer report contained interesting perspectives on individual attitudes to privacy. 74% of survey respondents considered on-line disclosure of information an increasing part of daily life; a majority expressed concerns over recording of their behaviour by way of mobile phones, payment cards and mobile Internet; and 58% did not believe there was any alternative to disclosure of personal information to obtain the benefit of desired products and services.[94]

Consumer groups tend to take a more active role in trying to protect the consumer's personal information than individual consumers do.[95] The key to analysing the real value of personal information to the consumer is obviously education and the advancement of "Cloud Literacy". A fundamental role for national ICT and data protection regulators is the facilitation of Cloud Literacy.

5.2 Recommendations for Future Data Protection and Privacy Laws

The four key areas of data protection laws that apply to cloud services are:

- Who is responsible for the protection of personal data in its possession?
- What restrictions, if any, should be placed upon the transborder flow of data?
- What security obligations should be imposed upon the party responsible for the relevant personal data?
- What law should apply in the cloud?

5.2.1 Who is responsible?

As discussed above, the current European Directive imposes primary responsibility for the protection of personal data on the "data controller".[96]

The definition applies to and imposes primary responsibility on the cloud business customer. In the case of cloud services provided to individuals, Facebook, or another provider, of social networking services or webmail would be the data controller. It does, however, also envisage the possibility of more than one "controller". When the cloud customer chooses a CSP, it is appointing that entity to process personal data on its behalf. The controller or customer has significant responsibilities to ensure that the CSP provides "sufficient guarantees" with respect to technical and organisational security measures and takes steps to ensure the CSP complies with those measures. In addition, the arrangements must be evidenced by a written contract requiring the CSP to act only on the customers' instructions and comply with obligations "equivalent" to certain security measures imposed on the customer. Processors are not typically directly subject to the European Directive.

The position regarding sub-processors is complex. If sub-processors are used they must also be obliged to act in accordance with the direction of the controller. Realistically, the efficient provision of cloud services could involve a number of sub-processors. Some member states have added the burden of requiring the customer to enter into direct contracts with each sub-processor.

With the ever increasing complexity of data processing and the involvement of multiple parties in the delivery of cloud services, the Working Party has issued guidance on the definition.[97]

Rather than clarifying the position, the Working Party further confuses stakeholders by indicating that factual functional control matters most in determining controller status. Though contractual provisions will be relevant, they will not be determinative.

These distinctions are unclear and out dated. They are unlikely to be enforceable in accordance with their terms in a cloud environment. CSPs and their customers are in the unhappy position of guessing what law might be applied and how it will be applied in a particular situation.

A different approach is taken by APEC, Canada and a number of other jurisdictions. The principle of "accountability" is increasingly being adopted internationally and advocated in Europe.[98] The accountability approach puts end-to-end responsibility on the controller of the relevant personal data. The accountability model appears to be the most effective means of clearly allocating responsibility in a cloud environment. For example, PIPEDA places no prohibition on transborder data transfers. The accountable party remains responsible for the personal data wherever it is held. This reflects a pragmatic, technically savvy and best practice approach to effectively protecting personal data.

5.2.2 Transborder Data Flows[99]

There are two schools of thought and attendant regulation relating to the international transfer of data. Harmonising and clarifying these approaches will be essential to promoting the growth and proliferation of cloud services – with their attendant economic benefits.

The European approach is based on geography. It is intended to protect against risks by the country or location to which data is transferred. The critical question is whether the importing country has "adequate" legal protections of personal data. In addition to the EU, Argentina, Morocco and Russia have adopted this approach. South Africa and other countries currently preparing data protection legislation may also adopt the geographically-based approach.

The geographic-based approach may also be questionable going forward under the General Agreement on Trade in Services (***GATS***)[100]. Data protection legislation is exempt from scrutiny under the GATS, but only so long as it is not a disguised restriction on trade.[101]

The Canadian PIPEDA and the APEC Privacy Framework imposes the obligation on the data exporting organisation to ensure the continued protection of personal data for which it is accountable. The geographic location is irrelevant. Though there is some overlap in the two legal approaches,[102] the best approach to provide clarity would be to try to internationally harmonise the two diverse principles.

It is now questionable whether, in light of the growing international digital environment and the prospective economic benefit cloud services present, whether the geographic restrictions imposed by current laws present not very well disguised restriction on international trade. Consider the fact that CSPs are now creating separate geographic clouds to accommodate EU style laws. This is particularly of concern in light of the other alternative,

i.e. the accountability principle. This principle presents a modern and clear approach to who is responsible and to what extent the restriction of international data flows are important to the effective protection of privacy.

The European Commission now has the opportunity to amend its geographically-based approach in its proposed reform of European Data Protection legislation and adopt the accountability model – reflecting international best practice. The reforms are intended to resolve disharmony between Member States and make compliance more straight forward.

The international digital eco-system calls for new ways of effectively protecting personal data. The Commission could seize this moment to lead the way toward an efficient internationally harmonised approach by adopting the accountability principle in its approach to who is responsible for personal data and where that data is held.

5.2.3 Security Obligations

Data security is one of the technical and organisational measures put in place to protect personal data. Security obligations on the "controller", "processor" and "accountable party" are common and defensible across international data protection regulations.

The accountability principle puts the obligation squarely on that party to take steps to assure the practical security of personal data that it will have processed by a third party.

Based upon the current uncertain technical environment, the safest option for the accountable party is to refrain from putting personal data in its control into the cloud environment. This is not, however, a position that will promote global economic connectivity and growth.

A number of opportunities are being created by new businesses offering security, encryption, auditing and other privacy enhancing technical solutions to provide comfort to the accountable party. CSPs have a role to play in putting in place reasonable commercial terms with customers and advancing self-regulation.

A significant tension may occur between the accountable party's obligations and potential interests by some foreign governments in personal data held in their country. International policy makers and bilateral arrangements between governments should play a role in providing clarity and consistency. Though with diverse interest across the globe – harmonisation may be out of reach for the moment.

5.2.4 Applicable Law

The process of determining which country's law applies to a breach of privacy is very complicated. It is challenging within the EU itself. Again, the EU is used as an example here because its data protection structure has been in place for some time and is forming the basis for legislation in many other parts of the world.

The current position within the EU has left room for considerable uncertainty in relation to the applicable law, not just in relation to data protection, but cloud computing in general. The European Directive envisaged data processing being limited to a small number of fixed locations under the control of one organisation, but the evolution of cloud computing has left this framework outdated and redundant.

That reform in this area would be welcome, if not necessary, is clear from the responses to the recent European Consultation.[103] It is essential that a clear framework is implemented to allow both providers and customers to gain a degree of certainty and it remains to be seen how the European Commission proposals for data protection will address these concerns.

There is also a need to address the relationship between the Rome I and Rome II conventions (that govern the law applicable to contract and tort in the EU) and cloud computing. The test for the applicable law, absent choice, is not suited to the development in modern technology, particularly in relation to cloud computing. Rome II, for example, provides that notwithstanding where the events giving rise to the damage occurred, the applicable law is the law of the country in which the damage occurs. Where cloud computing is concerned, this could reasonably be any number of jurisdictions. The potential for fragmented litigation is enormous. A wholesale failure by a provider could, as things stand, result in years of unpredictable proceedings.

The matter is further complicated where multiple jurisdictions are involved. Conflicts of laws is an extremely complex topic, again one that is not suited to the evolving nature of cloud computing. As matters stand, it would

be almost impossible for a provider with customers scattered around the globe to manage its legal exposure with any real certainty. However, as the use of cloud computing continues to grow, so will the political will to implement an international framework to govern its provision and use with clarity and certainty.

5.3 Recommendations to Policy Makers and Regulators

Having established the existing and potential value of cloud services, considered current data protection and privacy regulations, reviewed the challenges to enforcement of these regulations in the cloud, differences in issues between the developed and developing economies, the need for international co-operation and set out some recommendations for future international harmonisation of laws. What are the recommendations to policy makers and regulators to address the critical challenges raised by the cloud eco-system? This agenda must include clarity with respect to applicable law.

- ***Facilitate Knowledge***: Regulators have the opportunity to advance and facilitate "Cloud Literacy". This will assist consumers and citizens to make informed choices about what personal information they put in the Cloud, advance their understanding of who to complain to if their information is misused and enhance their understanding of the value to businesses of their personal data and how it might be used.
- ***Develop Expertise***: Policy makers and regulators must ensure they take account of current technical and social developments in the Cloud, its usage and potential. They must also keep current by taking soundings from all stakeholders to be in a position to develop, evolve and enforce relevant laws.
- ***Adopt Fit for Purpose Laws***: We are at a cross-road where international and national policy makers must work together to develop efficient, effective, proportionate and enforceable laws to protect an individual's reasonable expectation of privacy. Responsibility should also be devolved to stakeholders developing self regulation.
- ***Clearly Allocate Responsibility***: Regulations should ensure that responsibility for compliance is effectively and efficiently allocated to the party who is in the best position to ensure compliance. Responsibility and enforcement powers should be clearly allocated between national and international regulators as well as between domestic ITC and data protection regulators.
- ***Understand and Use Technology***: Cloud technology has evolved extraordinarily quickly. Policy makers and regulators now have the opportunity to take account of the development of new PeTs, and other practical means of protecting individual privacy and enhancing security systems.
- ***Review Existing Laws***: Policy makers internationally need to review existing laws to facilitate the national and international use of cloud services. The development of common standards and interoperability requirements will facilitate information flows with appropriate security and privacy protections. The elimination of restrictions on the transborder flow of data is critical to the growth of the cloud eco-system.
- ***Raise Awareness and Promote Uptake by the Public Sector***: Cloud services and the opportunities and savings they make available to governments around the world should be actively pursued and promoted. Particularly in the developing world. Bringing awareness and opportunities will lift the economic opportunities and provide great value to citizens, consumers and businesses.
- ***Encourage Clarity and Transparency in Cloud Contracting***: Confusion caused by the inconsistent patchwork of current laws may be assisted by clear contractual arrangements. Governments and stakeholders should establish a continuing dialogue to define best practice contractual terms.
- ***Enforcement***: Because some current legislation restricts behaviour that is virtually impossible to monitor in the cloud, regulators need to establish a means of identifying breaches to ensure they are able to respond effectively. This may be effected through self regulatory mechanisms, CSPs notifying the appropriate regulator of breaches of security and ideally changes to those aspects of data protection legislation which are impossible to monitor and hence unenforceable in practice.

6 CONCLUSION

> "***It was a thing hardly to be expected that in a popular revolution the minds of men should stop at that happy mean which marks the salutary boundary between power and privilege, and combines the energy of government with the security of private rights. A failure in this delicate and important point is the great source of the inconveniences we experience, and if we are not cautious to avoid a repetition of the error in our future attempts to rectify and ameliorate our system we may travel from one chimerical project to another; we may try change after change; but we shall never be likely to make any material change for the better."***[104]

Hamilton's concerns in the 18th Century upon forming the US Federal Constitution, could equally apply today. Now is the time to consider the present governance approach as a group of countries (rather than states) who face a global rather than federal future.

We need now to combine the energy of governments with the security of private rights to take a clear, consistent, pragmatic and "internationalist" approach to a fundamentally global digital eco-system.

Domestic and international policy makers need to come together to address the issues and opportunities presented by cloud services.

A patchwork of inconsistent and largely unenforceable national and regional regulations will neither harness the opportunities presented by cloud services or secure an individuals' private rights and information. An internationally harmonised approach to the practical protection of privacy and personal data is the best way forward. We as citizens, consumers, businesses, policy makers and governments need to act together – perhaps under a new banner to move the effective protection of privacy in a global digital eco-system to the top of the international agenda.

Dedication: For my daughter Genevieve who is a digital native.

Acknowledgements:

Thanks to Charles Russell LLP for its continuing support; in particular to Oliver Price and Louise Tomlinson, new data protection experts; to Vanessa Barnett, a seasoned data protection expert; to Tom Briggs for Middle Eastern Expertise; to Zani Polson, Phillis Thompson and Alison Gaffney;

Special thanks to Dr Mike Short CBE, Peter Ingram and Campbell Cowie for their insightful comments.

References

- Association of Corporate Counsel - Article 29 Working Party issues opinion on cloud computing - McDermott Will & Emery - 8 August 2012
- Autonomy – Cloud Solutions – Autonomy Systems Limited
- Autonomy – How to Measure the ROI of Cloud Data Protection – Autonomy Systems Limited
- Autonomy – Social Media and the Shifting Information Compliance Landscape – Autonomy Systems Limited – [Undated]
- Autonomy – The Next Generation of Archiving – Autonomy Systems Limited – [Undated]
- Autonomy – Why Cloud and How to Choose a Cloud Vendor – Autonomy Systems Limited
- BroadGroup - Competing in the clouds: Emerging strategies for enterprise data centres – BroadGroup - May 2010
- BSA Global Cloud Computing Scorecard - A Blueprint for Economic Opportunity - BSA (Business Software Alliance)
- Business Computing World - Cloud Industry Forum - Launches Code of Practice - Andy Burton - 22 November 2010
- Business Computing World – Is The Cloud Safe? Kate Craig-Wood – 21 May 2012
- CabinetOffice.gov.uk – The Queen's Speech 2012 – Her Majesty's Most Gracious Speech to both Houses of Parliament – HRH Queen Elizabeth II – 9 May 2012
- Cio.co.uk – Perchance to dream… Are dreams just the brain's way of digesting the day's information into a manageable searchable package? Mike Lynch – 22 February 2011
- Cisco – Cisco Global Cloud Index: Forecast and Methodology, 2010-2015
- Cloud Industry Forum - Code of Practice for Cloud Service Providers
- Cloud Security - [Unknown] - Michael Davis - 16 August 2012
- Computer World UK: Cloud computing and EU data protection law: Part Two - On international transfers of personal data - W Kuan Hon and Christopher Millard - 23 April 2012
- Computer World UK: EU data protection regulation and cookie law - Are you ready? Thor Olavsrud - 24 May 2012
- Computer World UK: US Patriot Act - Can UK cloud customers use US cloud providers? W Kuan Hon - 29 May 2012
- Computer World UK: Who's responsible for personal data in cloud computing? W Kuan Hon - 23 May 2011
- Data Centre Management Security in the CLOUD - Nick Coleman - July/August 2012
- DataCentres.com: Cloud computing will cause 'horrible problems in the next five years' - DataCentres.com - 7 August 2012
- European Data Protection Commissioners (Spring Conference 2012) Resolution on the European data protection reform - 3-4 May 2012
- European Data Protection Supervisor – ACTA measures to enforce IP rights in the digital environment could threaten privacy and data protection if not properly implemented - [Unknown] – 25 January 2012
- European Data Protection Supervisor – EDPS general survey shows that EU institutions and bodies have different levels of data protection compliance - [Unknown] – 30 January 2012
- European Data Protection Supervisor – EDPS welcomes a "huge step forward for data protection in Europe", but regrets inadequate rules for the police and justice area - [Unknown] – 25 January 2012
- European Network and Information Security Agency – Benefits, risks and recommendation for information security - November 2009
- European Parliament - Directorate-General for Internal Policies, Policy Department Economic and Scientific Policy A - Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy - 2011
- European Privacy Association - Ofcom Traffic Management and 'net neutrality' Consultation
- European Union - Article 29 Chairman of the Article 29 Working Party: Proposals a chance for better protection – Jacob Kohnstamm – 25 January 2012
- European Union - Article 29 Data Protection Working Party European Data Protection Authorities adopt opinion on cloud computing (WP 196) - 1 July 2012
- European Union - Article 29 Data Protection Working Party Opinion - The Future of Privacy – [Unknown] - 1 December 2009
- European Union - Article 29 Data Protection Working Party Opinion - 01/2010 on the concepts of "controller" and "processor" - 16 February 2010
- European Union - Article 29 Data Protection Working Party Opinion - 08/2010 on applicable law - [Unknown] - 16 December 2010

- European Union - Article 29 Data Protection Working Party Opinion - 11/2011 on the level of protection of personal data in New Zealand - 4 April 2011
- European Union - Article 29 Data Protection Working Party Opinion - 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing – 13 June 2011
- European Union - Article 29 Data Protection Working Party Opinion - 04/2012 on Cookie Consent Exemption - [Unknown] - 7 June 2012
- European Union - Article 29 Data Protection Working Party Opinion - 05/2012 on Cloud Computing - 1 July 2012
- European Union – Reform of the data protection legal framework
- European Union – Setting up the European Cloud Partnership – Neelie Kroes – 26 January 2012
- European Union – The clear role of public authorities in cloud computing – Neelie Kroes – 25 March 2011
- Federal Ministry of Economics and Technology (Germany) - The Standardisation Environment for Cloud Computing Federal Ministry of Economics and Technology (Berlin) - February 2012
- G-Cloud c1 - Cloud Legal Project's Analysis - W Kuan Hon, Prof Christopher Millard and Prof Ian Walden - 23 April 2012
- Gigaom.com - Will using Dropbox put your CEO in jail? Janko Roettgers - 21 June 2012
- Giving bite to the EU-U.S. data privacy safe harbour - model solutions for effective enforcement - Daniel R. Leathers - 1 January 2009
- HM Government - G-Cloud Information Assurance Requirements and Guidance - [Unknown] - 10 May 2012
- IBM Global Business Services – IBM Institute for Business Value – The power of cloud, driving business model innovation – Saul Berman, Lynn Kesterson-Townes, Anthony Marshall and Rohini Srivathsa – February 2012
- Industry Recommendations to Vice President - Neelie Kroes on the Orientation of a European Cloud Computing Strategy - [Dr. Eugene Sweeney, Iambic Innovation Ltd] - November 2011
- Information Commissioner's Office (ICO) – Personal information online code of practice – July 2010
- Information Commissioner's Office (ICO) – Privacy by design
- Intel - Security in the Cloud - [Unknown]
- International Chamber of Commerce - The Digital Economy - Cross-border law enforcement access to company data – current issues under data protection and privacy law - International Chamber of Commerce - 7 February 2012
- International Conference of Data Protection and Privacy Commissioners – International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution) – 5 November 2009
- International Data Privacy Law – Oxford Journals - Who is responsible for 'personal data' in cloud computing? – The cloud of unknowing, Part 2 - W Kuan Hon, Christopher Millard and Ian Walden - 6 December 2011
- ITU - ICT Regulation Toolkit – 2.4 What is the Role of Regulators? – 2012
- ITU - ICT Regulation Toolkit – Module 6. Legal and Institutional Framework – [Unknown] – [Undated]
- ITU-T Technology Watch Report - Privacy in Cloud Computing - Stephane Guilloteau and Venkatesen Mauree - March 2012
- Kuppinger Cole - 10 Rules for Securing the Cloud - Martin Kuppinger - 7 March 2011
- Kuppinger Cole - Data Protection and the Cloud - Martin Kuppinger - 14 February 2012
- Kuppinger Cole – Is cloud computing worth the hassle? 17 November 2011
- Kuppinger Cole – Top Trends 2012-2013 – Martin Kuppinger – April 2012
- Loeb & Loeb LLP - Data Protection - United States - Ieun Jolly - 1 March 2012
- London Economics – Study on the economic benefit of privacy-enhancing technologies (PETs)
- Mondaq – European Union: New Data Protection Regulation – How Will It Affect Your Business? John Menton, Rob Corbet, Caroline O'Gorman, Chris Bollard, Colin Rooney and Olivia Mullooly – 28 February 2012
- Mondaq – European Union: Reform Of Data Protection Laws - Colin Rooney – 23 April 2012
- Mondaq – Germany: German Data Protection Authorities Broaden Application Of German Data Protection Law To Foreign Social Networks And Attack The Use of Social Plugins And Fanpages – Fabian Niemann – 17 April 2012
- Mondaq – Germany: New EU Data Protection Regime Will Bring Significant Changes – Jurgen Hartung and Dr Marc Hilber, LL.M. – 2 March 2012
- Mondaq – Netherlands: Personal Data Protection Act Amended Jacqueline Van Essen – 20 February 2012
- Mondaq – United Kingdom: Draft Data Protection Regulation – Alan Meneghetti, Andrew Horrocks and Manoj Vaghela – 22 May 2012
- Mondaq – United States: Data Protection: Frequently Asked Questions – Goodwin Procter LLP – 13 January 2009

- Mondaq – United States: The USA Patriot Act and the Privacy of Data Stored in the Cloud – Alex C. Lakastos – 24 January 2012
- National Institute of Standards and Technology - Guidelines on Security and Privacy in Public Cloud Computing - Wayne Jansen and Timothy Grance - December 2011
- OECD – OECD Guidelines for the Security of Information Systems and Networks – Towards a culture of security
- OECD – OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Oppenhoff & Partner Rechtsanwalte - Germany: Employees Off Into The Cloud? Dr Marc Hilber, LL.M. and Gilbert Wurth - 16 May 2012
- Oppenhoff & Partner Rechtsanwalte - Germany: German Data Protection Authority Forbids Certain Facebook Features - Jurgen Hartung - 29 August 2011
- Oxera (Agenda – Advancing economics in business) - Global-local: European telecoms regulation in the 2020s - Richard Feasey - July 2012
- PerspecSyS - Cloud Security Issues – [Undated]
- PerspecSyS - Gartner Highlights the Growing Importance of Cloud Security Brokers to Protect Sensitive Information in the Cloud - David Canellos - 7 August 2012
- PerspecSyS -Information and Privacy Commissioner Ontario, Canada – Ann Cavoukian
- PLC - Software as a service (SaaS) - Roger Bickerstaff, Barry Jennings of Bird & Bird - 13 March 2009
- PLC & Baker & Mackenzie LLP – Overview of EU data protection regime – Robbie Downing
- PLC & Bird & Bird – What is cloud computing - Roger Bickerstaff, Barry Jennings, Tessa Finlayson
- PLC IPIT & Communications – Article 29 Working Party adopts opinion on applicable law
- PLC IPIT & Communications – Cross-border transfers of personal data
- PLC IPIT & Communications – EU data protection regime proposals: analysis and noter-up
- PLC IPIT & Communications – European Commission proposes new data protection framework
- PLC IPIT & Communications - General counsel briefing: privacy and data protection
- PLC IPIT & Communications – ICO analysis of new EU data protection proposals
- PLC IPIT & Communications & Baker & McKenzie LLP – Data protection and the internet - Robbie Downing - [Undated]
- PLC IPIT & Communications & Baker & McKenzie LLP – Overview of UK data protection regime - Robbie Downing - [Undated]
- PLC Media - Cloud computing and EU data protection laws: a work in progress - [Unknown] - 25 May 2012
- Privacy Identity Innovation.com – Videos – PII 2012 Conference – [Undated]
- Privacy International - Privacy in the developing world: a global research agenda - Carly Nyst - 14 July 2012
- Public Service Europe – Can we trust cloud computing, ISPs and social networks? – Ross MacDonald – 2 April 2012
- Public Service Europe – Cyber-space now seen as 'fifth dimension of warfare' – Chris Hardy – 9 February 2012
- Public Service Europe – Getting to grips with the EU data directive – David Gibson – 18 April 2012
- Public Service Europe – New EU laws to protect data in the cloud – Daniel Mason – 7 December 2011
- Rundfunk & Telekom Regulierungs – GmbH: European regulators face new challenges - Regulation 2.0 - Georg Serentschy - 9 August 2012
- Scripted - Data Export in Cloud Computing - How can Personal Data be Transferred Outside the EEA? The Cloud of Unknowing, Part 4 - W Kuan Hon and Christopher Millard - 15 April 2012
- SearchCloudSecurity.TechTarget.com – Article 29 Working Party cloud computing opinion: Blow to Safe Harbor?
- Society for Computers & Law – G-Cloud v1: Cloud Legal Project's Analysis – [Undated]
- Society for Computers & Law - In Defence of the Cloud - Eduardo Ustaran - 22 May 2012
- Society for Computers & Law - The 12 Cs of Cloud Computing: A Culinary Confection - W Kuan Hon - 16 April 2012
- Taylor Wessing - Why the Clouds of Suspicion? Data Protection and Cloud Computing - January 2011
- Telegraph.co.uk – Facebook's Mark Zuckerberg says privacy is no longer a 'social norm' – Emma Barnett, Technology and Digital Media Correspondent – 11 January 2010
- The African File - The Cloud and Africa Indicators for Growth of Cloud Computing - Alex Laverty - 18 May 2011
- The New York Times - New European Guidelines to Address Cloud Computing - Kevin J. O'Brien - 1 July 2012
- Thomson Reuters – An Overview of Cloud Computing and its Legal Implications in India – Naqeeb Ahmed Kazia – Issue 2, 2012
- TILT (Tilburg Institute for Law, Technology, and Society) - Law & Technology Working Paper Series Regulation of Transborder Data Flows under Data Protection - and Privacy Law: Past, Present, and Future - Christopher Kuner - October 2010

- TRUSTe - TRUSTe CEO Testifies Before Congress - John Gamble - 19 June 2012
- U.S. * EU Safe Harbor Framework - Guide to Self-Certification - March 2009
- West Law - Computer and Telecommunications Law Review 2010 – China's personal data protection on the internet – Hong Xue
- West Law - Computer and Telecommunications Law Review 2010 – Collecting data online: what is best practice? Oliver Bray and Paul Joseph
- West Law - Computer and Telecommunications Law Review 2010 – EU applicable law: clarification on some practical issues relating to data protection – from Article 29 Working Party's Opinion 8/2010 – Pierre-Andre Dubois
- West Law - Computer and Telecommunications Law Review 2010 – United States: electronic commerce – ethics
- Who's Who Legal – Cloud Computing and Data Protection - Dr Ursula Widmer, Dr Widmer & Partners – July 2009

[1] This paper and the comments herein are of a general nature, not to be relied upon in connection with any specific circumstances and no liability is accepted by the author, Charles Russell LLP or the ITU.

[2] James Madison, The Federalist, no 10, 1787. James Madison, Jr was an American statesman and political theorist. He is credited as being the "Father of the US Constitution" for being critical to the drafting of the Constitution and author of the US Bill of Rights. He was also the fourth president of the United States. The Federalists were the first American political party who fashioned a strong new government and approach to drawing the individual states together in the late 18th Century. The Federalist Papers are a series of essays promoting the adoption of the US Constitution.

[3] The power of Cloud: Driving business model innovation, IBM Global Business Services by Saul Berman, Lynn Kesterson-Townes, Anthony Marshall and Robini Srivathsa.

[4] Enhancing the broadband investment environment – policy statement by Vice President Kroes, Brussels, 12 July 2012.

[5] Cisco Global Cloud Index: Forecast and Methadology, 2010-2015.

[6] The power of Cloud: Driving business model innovation, IBM Global Business Services by Saul Berman, Lynn Kesterson-Townes, Anthony Marshall and Robini Srivathsa.

[7] See further the GSR paper on "Demystifying Regulations in the Cloud: Opportunities and Challenges for Cloud Computing."

[8] Computer and Telecommunications Law review 2010, Cloud Computing, Mark Taylor and Matko Matteucci, CTLR 2010, 1692), 57-59.

[9] WK Hon and C Millard, "Data Export Cloud Computing – How can Personal Data be Transferred Outside the EEA? The Cloud of Unknowing, Part 4", (2012) 9:1 SCRIPTed 25. http://script-ed.org.

[10] The power of Cloud: Driving business model innovation, IBM Global Business Services by Saul Berman, Lynn Kesterson-Townes, Anthony Marshall and Robini Srivathsa.

[11] See the GSR paper on "Demystifying Regulations in the Cloud: Opportunities and Challenges for Cloud Computing" for an in-depth discussion of cloud computing.

[12] Cave, Robinson, Schindler, Bodia, Kool van Lieshout; "Does it help or hinder? Promotion of Innovation on the Internet and Citizen's Right to Privacy: European Parliament: Directorate-General for Internal Policies; Policy Department A; December 2011. http://www.europarl.europa.eu/committees/en/studies.html

[13] Global Data Privacy Laws: 89 Countries, and Accelerating; Social Science Research Network; 6 February 2012.

[14] EU Directive 95/46/EC.

[15] 'Data, data everywhere, A special report on managing information', The Economist, 27 February 2010, at 3.'.

[16] BSA,"Global Cloud Computing Scorecard": A Blueprint for Economic Opportunity, 2012.

[17] ITU, "Privacy in Cloud Computing," ITU-T Technology Watch Report, March 2012, http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx

[18] 2002/58/EC.

[19] Article 5(3).

[20] Subject to the application of the Personal Information Protection and Electronic Documents Act.

[21] Article 29 Working Party WP196 on Cloud Computing, 1 July 2012.

[22] Article 17(1), Data Protection Directive.

[23] Article 29 Data Protection Working Party Opinion 05/12.

[24] Court of Appeal – Michael John Durant v Financial Services Authority [2003] EWCA.

[25] Act 78-17, 6 January 1978.

[26] Commission nationale de l'informatique et des libertes.

[27] Jorg – Alexander Paul, Bird & Bird, as quoted by Kevin J O'Brien, "New European Guidelines to Address Cloud Computing", July 1, 2012.

[28] European Commissions: Commission proposes a comprehensive reform of the data protection rules, 25 January 2012.

[29] Uniting and strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (2001), Public Law 107-58 (***US Patriot Act***).

[30] See for example, Katz v. United States, 389 U.S. 347 (1967).

[31] PLC, Data Protection, USA.

[32] 15 U.S.C.

[33] Controlling the Assault of Non-Solicited Pornography and Marketing Act.

[34] Telephone Consumer Protection Act.

[35] California A.B. 1980 Data Security Law.

[36] California 5.B. 27 "Shine the Light" Law.

[37] SAFE Data Act, H.R. 2577.

[38] Data Accountability and Trust Act of 2011, H.R. 1841.

[39] S.8.

[40] See, Hunter v Southam (1984) 2 SCR 145 (CA).

[41] Jones v Tsige (2012) ONCA 32 (CA).

[42] Article 5, X and XII.

[43] Article 12, Law 10 406/2002.

[44] Article 21, Law 10, 406/2002.

[45] Under Article 43.

[46] S.69.

[47] Article 21 of the Constitution, see Kharaj Singh v State of UP (Air 1963 SC 1296).

[48] S.43.

[49] S.72-A.

[50] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[51] Specifically, the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements".

[52] See Economist, Private data, public rules, 28 January 2012.

[53] PLC, Data Protection – Japan, Brazil, South Africa and India.

[54] Act No. 57 of 2003.

[55] Articles 21 and 22.

[56] BSA Scorecard, pg 3.

[57] Gartner has indicated Europe is two years behind the US in adopting cloud services because of the confusion and concerns over privacy.

[58] See section 3.

[59] See section 3.1.

[60] See section 3.3.3; and London Economics; "Study on the economic benefits of privacy – enhancing technologies (PETs); Financial Report to The European Commission, D G Justice, Freedom and Security.

[61] Practice Note: PLC General Counsel briefing: privacy and data protection.

[62] International Chamber of Commerce; "Cross-border law enforcement access to company data – current issues under data protection and privacy law; Document NO. 373/507 – (7 February 2012).

[63] See Section 5.

[64] ICC (as above).

[65] International Conference of Data Protection and Privacy Commissioners, "International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution", 5 November 2009.

[66] Oracle, IBM, Hewlett-Packard, Walt Disney, Microsoft, Accenture, Google, Intel, Proctor & Gamble and General Electric.

[67] Speech/12/38; 26/01/2012 Neelic Kroes, Vice President of the European Commission responsible for the Digital Agenda; "Setting up the European Cloud Partnership".

[68] ITU, "Privacy in Cloud Computing," ITU-T Technology Watch Report, March 2012, http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx

[69] Some examples of other privacy principles: OECD (Privacy Principles 1980), Generally Accepted Privacy Principles (GAPP) from AICPA, FTC Fair Information Practice Principles (FIPPs) (ref: United States Privacy Act of 1974), Consumer Privacy Protection Principles (CPPPS), Asi-a Pacific Economic Cooperation (APEC) Privacy Framework – Information Privacy Principles (2005) and International Security, Trust & Privacy Alliance (ISTPA) Privacy Principles.

[70] Kuhn, (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law – Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing.

[71] Google Transparency Report, August 2012.

[72] WP179.

[73] UK Information Commissioner's Office.

[74] CNIL, 32nd Annual Activity Report 2011.

[75] Data Protection and Privacy, Jurisdictional Compensations 2012.

[76] BFDI, Annual Activity Report 2009/2010.

[77] August 2012, http://mashable.com/2012/08/09/ftc-google-22-5-million/

[78] Office of the Privacy Commissioner of Canada.

[79] The seven principles include commitments as to Notice, Choice, Onward Transfer of data, Security, Data Integrity, Access and Enforcement. "US-EU Safe Harbour Framework", Guide to Self-Certification, March 2009.

[80] Burton, A, "Cloud Industry Forum launches Code of Practice", Business Computing World, 22 November 2010. Members of the CIF include UK PLC, APMG-International, Channel Cloud, Citrix, Claranet, Concorde Databarracles, Dell, etc. For a full list of members and more information see www.cloudindustryforum.org.

[81] The CSA members include ASTRI, US Dept of Defense, Ericsson, Adobe, Accenture etc. For a full list of members and more information, see www.cloudsecurityalliance.org.

[82] Schellman, C. "SOC 2 For Cloud Computing", October 10, 2011.

[83] Autonomy Cloud Solutions – Product Brief.

[84] WP 196.

[85] Privacy Enhancing Technologies : A Review; Yun Shen & Siani Pearson, HP Laboratories; HPL-2011-113.

[86] Other examples of PETs can be found at Stanford's Center for Internet and Society. http://cyberlaw.stanford.edu/wiki/index.php/PET

[87] London Economics; Study on the economic benefit of privacy-enhancing technologies, pg xi.

[88] Ibid.

[89] Laverty, A; "The Cloud and Africa – Indicators for growth in Cloud Computing; The Africa File"; 18 May 2011.

[90] Nyst, C: "Privacy in the developing world: a global research agenda"; Privacy International, 14 July 2012.

[91] Kuner, C. (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing.

[92] European Commission.

[93] London Economics; "Study on the economic benefits of privacy-enhancing technologies (PeTs)"; Final Report to The European Commission D G Justice, Freedom and Security; July 2010.

[94] Special Eurobarometer 359/Wave 74.3 – TNS Opinion and Social : Attitudes on Data Protection and Electronic Identity in the European Union (July 2011). The Eurobarometer research also reported that six in ten Internet users usually read privacy statements (68%) and that majority (70%) that did so adapted their online behaviour. Levels of trust in companies active on the Internet was reported to be low: less that one-third (32%) trust (mobile) phone companies or Internet Service Providers and just over one fifth (22%) trust other Internet companies like search engines, social networking sites and e-mail services. The research further discovered that 70% are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected. A majority (75%) wanted to delete personal information on a website whenever they decide to do so.

[95] London Economics.

[96] "The natural person, public authority, agency or any other body which alone or jointly with others determines the purposes and means the processing of personal data" – European Directive, Art. 2 (d).

[97] Working Party (WP169).

[98] Examples include OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); APEC Privacy Framework (APEX Secretariat, 2005); and The Madrid Resolution (2009).

[99] Christopher Kuner has considered these issues thoughtfully and in detail. See: Kuner, C. (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Laws: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing; and for more detail – Kuner, C. "Regulation of Transborder Data Flows under Data Protection and Privacy Laws: Past, Present and Future"; TILT Law & Technology Working Paper No. 016/2010 and Tilburg University Legal Studies Working Paper No. 016/2010.

[100] a World Trade Organisation treaty that came into force in 1995

[101] GATS Article XIV (c)(ii).

[102] For example, the PIPEDA expects the accountable person to have received some assurance that personal data transferred will continue to receive protection; and the EU recognises exceptions if binding corporate rules or standard EU contractual clauses are put in place.

[103] European Consultation: Cloud Computing – Public Consultation Report dated 5 December 2011.

[104] Alexander Hamilton, The Federalist, no. 26, 1787. Like James Madison, Alexander Hamilton was a "founding father" of the United States. He was a soldier, economist, political philosopher, as well as the first US Secretary of the Treasury.