LAW AND REGULATION FOR A BROADBAND WORLD

MODULE THREE

3.1 Introduction

The first experience of broadband by commercial and personal users was a telecommunications standard Integrated Services Digital Network-Broadband or simply ISDN-B. The standard was adopted by the CCITT (International Telegraph and Telephone Consultative Committee) of the ITU in 1988 for the transmission of voice, video, data and other network services at speeds up of 144Kbps. The peak sub-broadband speed of ISDN was 128Kbps. As mentioned in chapter one (http://broadbandtoolkit.org/1.2)"the term broadband is generally understood to mean a dedicated or "always-on" connection to the Internet with speeds faster than dial-up."

ISDN-B offered a digital subscriber line (DSL) service over the top of a baseband analogue signal, but from the late 1980s onwards higher speed DSL communication technologies became available. Asymmetric DSL (ADSL) seen as ideal for residential customers who were assumed to need more bandwidth for Internet download than upload, whereas Symmetric Digital Subscriber Line (SDSL) was seen as more suited to the symmetrical needs of large companies sending and receiving files a regular basis between their various office locations. By the late 1990s in some markets, personal telephone connections into the home using the digital subscriber line (DSL) standard had already reached 1.5Mbps, something that only a few years earlier had not been available outside of commercial enterprise markets such as the banking and financial sectors. (See Module 5.7.1 Wireline Access Technologies for a broader discussion.)

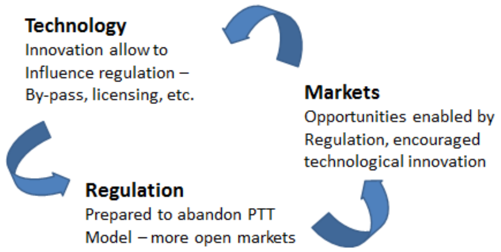
By 2008 the ITU-R (International Telecommunications Union-Radio communications sector) had endorsed the 4G LTE (Long Term Evolution) mobile cellular standard named IMT-Advanced (International Mobile Telecommunications Advanced) with potential peak download speeds of 1Gbps for pedestrian usage and 100Mbps for use in moving vehicles. Using fibre-to-the-home 1Gbps is already available to households in numerous markets around the world.

NGN Broadband

The most advanced networks have already reached the next generation network (NGN) phase, meaning they are end-to-end IP high-speed broadband networks. Compared with 144Kbps the technology and the markets for broadband have changed beyond all recognition. Yet in the 1990s and 2000s there were very mixed views from within the industry to these developments. The first was a disbelief that anyone could want or need high-speed broadband at all. As speeds increased so did the upper limit of what many observers thought was necessary to download Internet TV programmes (IPTV), movies, upload videos and photographs, etc. As it turned out, markets proved the doubters wrong: Internet users who moved to higher speeds never went back. The idea that the demand for speed was dependent upon, or derived from, the demand for content and applications was not quite right. Users wanted speed for its own sake, just as users want access to telephones even if they do not always use them. It shows that while technological advances can drive markets, so markets can drive technological advances. What economists call latent demand is often untapped and unrealized in markets where there is little competition because monopolists and dominant incumbent service providers have little incentive to invest in more modern technologies. This is a key issue for regulators wanting to see more broadband roll-out in developing economies.

The second reaction came from the more traditional telecommunications community who doubted that Internet protocol, or simply IP, would ever be able to deliver the 'carrier grade' quality of service that was expected and demanded of telecoms companies. The digital workhorse of the 1990s was the ATM (Asymmetric Transfer Mode) switch which could easily handle digitalized traffic using many different packet-switched protocols, such as Frame Relay for commercial data users and X.25 for email users, over traditional telephone circuits. The reality turned out to be different. New releases of IP routing algorithms became more reliable and routing equipment better able to handle higher capacity traffic. This allowed new entrants into telecoms markets the option of adopting next generation network (NGN) architectures and technologies giving them much lower operating costs than incumbents. For example, in the US incumbent telecoms providers were forced into accelerating the depreciation of their ATMs and associated network equipment. For policy makers and regulators this has opened up an entirely new era of issues, because they have to decide upon whether and how to license these 'disruptive' new entrants—disruptive in the sense they are employing technologies that change the face of telecoms services and service delivery. This underscores the importance of the interconnectedness of technologies with markets and with policy/regulation.

Figure 3.1
Critical Success Factors Form a Virtuous Loop



Source: Author

Interconnectedness

Equally important is the interconnectedness of networks, and probably of greater importance than the more familiar concept of convergence. Ever since the digitalization of telecoms the issue of convergence has arisen because different traffic streams, such as voice, video and data can be transmitted down the same transmission networks, known as multiplexing. However, when networks deployed IP, it meant that different traffic streams could cross between networks and that is fundamentally important from a commercial perspective because it gives rise to the possibility of by-pass. By-pass was a rising phenomenon in international telecommunications in the early 1990s as international carriers, striving to become more competitive, re-routed their overseas traffic from high-cost routes to lower-cost routes to arbitrage international accounting and settlement rates. Call-back was a related form of by-pass, again substituting or 'arbitraging' lower for higher cost routes. With the spread of the Internet and applications such as Skype, Yahoo Messenger, WhatsApp and many others, users can place phone calls, video calls, text messages and by-pass the incumbent carriers. These were the forerunners of Over-the-Top (OTT) applications, such as downloading content from third party access providers, for example TV shows over YouTube or movies from Bit Torrent.

Interconnectedness of networks raises new challenges for policy-makers and regulators because it means a proliferation of the means of access to networks. In principle, any user can access any network from any other, but local carrier and content licensing conditions that were introduced many years ago may not be consistent with this growing reality. Often carriers which were granted exclusive licences to provide access or content services now find themselves by-passed. Their options are to adapt to the new market realities and compete aggressively or to partner with overseas service providers and provide the localization of content and distribution channels. Alternatively, they may decide to lobby for restrictions on these new entrants and if they are partly owned by government they may have powerful political support. For policy-makers there may be legal obligations involved and in some cases the best way forward may be to compensate a carrier for giving up its exclusive rights, for example over international telephony. Policymakers and regulators should always keep in mind the ultimate purpose of licensing and regulation: If policies and regulations encourage innovation and diversity of service options for users, the overall value of the market is likely to grow even if some segments, such as voice revenues, decline. A more competitive and diverse market is attractive to other sectors of the economy, such as new media, advertising, online retail, mobile payments and banking services, not to mention the market for user access devices such as smartphones and tablets.

For many years the industry has talked of convergence to describe the above as information services (data), communication services (telecoms) and technologies (IT) come closer together as ICTs. However, it remains the case that just because these services can be delivered (multiplexed) down the same pipes does not necessarily imply there is commercial synergy between them as businesses. The skills required to run a telecoms network are vastly different from those needed to create a successful TV station, and the financial profiles are totally different. Investment in telecoms is lumpy over time with long periods of revenue growth to be accumulated for the next round of investment. A TV station lives or dies by how fresh its programming is on a daily basis and the purchase of new content from the studios is a continuous process. Carriers will look to complement different services, such as telecoms and IPTV, and will leverage their subscriber and billing base to market these complementary services, but they are equally likely to run up against the problem of cannibalization. This arises when the marketing of one product or service comes at the expense of another. For example, rolling out broadband may cannibalize the leased line business, and offering bundled Internet services may cannibalize voice revenues. These are essentially commercial decisions for the carriers, not for the regulator, but often permission to do any of this requires new licences or regulatory approvals. It is the interconnectedness of networks that creates the competitive impetus for all of this.

About this Module

Interconnectedness is throwing up a number of issues that were previously beyond the domain of a telecoms regulator. Issues such as data privacy and cyber security, for example, have become concerns for policy-makers and often require coordinated approaches across different regulatory bodies. Where this includes telecoms and broadcasting a number of jurisdictions, including the UK, Hong Kong, Nigeria and Thailand have decided to merge the regulators. Whether convergence of technologies leads naturally to the convergence of regulation is a question to be examined further below. So this module deals not only with issues the telecoms regulator traditionally has to deal with, such as licensing and spectrum management, but also with related issues that arise due to the interconnectedness of networks.

Module Three: Law and Regulation for a Broadband World

3.2 Licensing and Authorization Frameworks[1]

Licensing is authorization to build a network and/or to offer services of different kinds over a network. The arguments behind licensing usually relate to the need to regulate the activities of operators and service providers for the public good, such as quality of service and customer care, protection against price gouging and unfair or anti-competitive practices. Licensing arrangements are a way to ration scarce resources, but in cases where resources are not scarce other mechanisms may be used, such as authorizations, class licences that cover a variety of services to different devices, or simple registration.[2] For example, in the 1990s Hong Kong issued paging licences on-demand as long as there was spectrum available.

An Adaptable Licensing Framework Needed

In a pre-digital, pre-IP and pre-NGN era the costs of building and operating a network were very high giving rise to claims, not always justified, that a telecoms network was close to being a 'natural monopoly'. A natural monopoly occurs when the unit or average costs of output fall as output rises across the entire market until all demand is satisfied. Under these circumstances, no new entrant could be more efficient at serving even a select portion of the market. In reality, there are almost always segments of the market where a specialized new entrant can serve more efficiently and in a more innovative way. In a world of digital telecommunications and IP networks new entrants can choose to come into the market using NGN systems with significantly lower operating costs. If there are any natural monopoly elements left they are likely to be found in long-distance traffic networks, but even here if non-telecom entities such as electricity utilities and rail networks are licensed to lease their long-haul cable or microwave capacity to new entrants, competition is possible. Licensing and authorization therefore need to take into account the changing economic realities that arise from new technology paradigms.

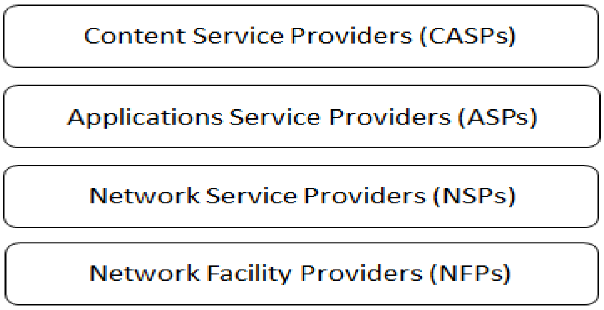
An important first step policy-makers and regulators can take towards a competitive telecommunications market is to make the licensing regime responsive to the emergence of new technologies that make new entry commercially feasible. Responsiveness to change requires a flexible licensing regime. There have been several different approaches to reforming the licensing process. One approach is to separate telecom activities into a tiered stack with infrastructure at the bottom, service delivery in the middle and applications and content as the top layers of the stack and issue different classes of license for each layer. For

[1] See also http://ppp.worldbank.org/public-private-partnership/sector/telecom/laws-regulations#sample

[2] For a summary of regulations in different countries, see http://ppp.worldbank.org/public-private-partnership/sector/telecom/laws-regulations#sample

example, the Malaysian Communications and Multimedia Commission (MCMC) issues licences according to the following categories:

Figure 3.2


Content Service Providers (CASPs)
Applications Service Providers (ASPs)
Network Service Providers (NSPs)
Network Facility Providers (NFPs)

In the case of neighbouring Singapore, facilities-based and services-based licences are also issued, but the third layer consists of individual licences and class licences. In Africa, Kenya has a similar approach (see Toolkit *Broadband in Kenya Case Study*) but with twelve licence categories embracing ancillary sectors such as contractors, vendors and even business process outsourcers under a Unified Licensing regime.[3] One of the problems with this segmented approach is that the lines of delineation between networks, services, apps and content begin to crumble. For example, cloud computing service providers may offer Infrastructure-as-a-Platform (IaaP) with more and more content accessible through apps; the licensing framework ceases to reflect the way in which facilities and services are offered.

An alternative approach to meet the needs of NGNs is the issuing of a multi-service general licence which enumerates the specific types of services the operator can provide. The most flexible form of general licence is a service and technology-neutral unified licence which permits entry to any field of service the operator wishes to invest in. This was an approach pioneered by India.[4] The most radical approach is to replace licences altogether with registrations, but this may require codes of practice to ensure good behaviour by operators and service providers.

Issuing Licences

In some jurisdictions, licenses have to be approved by the legislature. While this process may ensure a thorough vetting of the application, it can also mean lengthy delays and the involvement of policy-makers who are not specialists in the field. It is also a process that lends itself to lobbying. A better option is to remove the specifics of licensing conditions as

[3] http://www.cck.go.ke/licensing/telecoms/ULF_Register_Licensees__Nov_2012_updated.pdf

[4] See ITU case study http://www.ictregulationtoolkit.org/en/practicenote.aspx?id=630

applied to each operator from the legislative process and place them in licences issued by the telecoms regulator, even if final approval or endorsement lies with a higher authority. Legislation can then focus upon the overall principles of licensing in the sense of creating a template which the regulator can use.

Transparency and Investment

What is fundamentally important is that the terms and conditions of any licence are absolutely transparent and, ideally, available for all to see on the regulator's website. Both users and competitors should have the right to know what are the terms and conditions of service. Users need to know for the protection of consumer rights, and competitors need to know so every operator has equal access to commercially non-sensitive information. Where information is commercially sensitive, for example in the cost accounting data upon which a Reference Offer of Interconnection (ROI) is agreed by the incumbent operator, then the regulator needs to have a copy so that they can determine whether there is discrimination in case a dispute emerges between operators.

Unfortunately not all licences are given out on a transparent basis. Where corruption or cronyism is involved licences are seen as rewards and favours, with the inevitable consequence being that users and the economy-as-a-whole are denied the full benefits of competition. This will make the economy less appealing to investors, especially to investors in carrier services who see the market as being rigged, but also to investors in sectors that are heavily reliant upon broadband communications networking such as financial institutions, trading companies, business process outsourcers, call centres, and other companies that are part of the global supply chain of multinationals. A World Bank study of investment in telecoms in the Asia Pacific region in 2004 found that regulatory uncertainty was the No.1 deterrent to investors in telecoms,[5] while the availability of high quality and affordable telecommunications services is regularly cited as among the top three factors that attract overseas investment, along with the rule of law and good transportation systems. A good example from North Africa of transparent regulation was Morocco's creation of an independent *Agence Nationale de Réglementation des Télécommunications* (ANRT) in 1998. (See Toolkit *Broadband in Morocco Case Study*. http://broadbandtoolkit.org/Case/ma/2)

Ex-Ante, Ex-Post and Incentive Regulation

In many cases the conditions of the licence as they apply to different operators will depend upon whether the operator in question has been designated as dominant in any given market, such as in voice termination or in leased circuits. Dominance is usually measured by market share of users or by the share of total revenues. A widely used measure, for example

[5] See http://trpc.biz/wp-content/uploads/2004_07_Telecom_in_EAP_Telecom_Note.pdf

is the Hirschman-Herfindahl index (HHI) which is constructed by the sum of the squares of the market shares of each operator, so in an evenly competitive market of 4 players each with 25% of the market HHI = $25^2 + 25^2 + 25^2 + 25^2$ = 2,500. A number larger than this is indicative of a more concentrated market, but this is a rather static measure that in itself does not explain market behaviour.[6] A more refined measure is significant market power or simply SMP. This estimates how far a single operator can increase profitability by changing the price it charges for its services. In a highly competitive market, it will lose customers when it hikes its prices, and if it lowers its prices competitors will match it. Traditionally, where an operator has been designated as dominant, some regulatory restrictions apply; for example, an incumbent operator could be required to submit proposals of tariff changes to the regulator for approval. This is regulation *before the event* or *ex ante* regulation. However, as competitors establish a firm foothold in the market there has been a change towards regulation *after the event* or *ex post* regulation. This is appropriate when it cannot be assumed that the dominant operator is abusing its market position. It is often referred to as 'light-handed' or 'light-touch' regulation. Just as the *threat* of competition may be sufficient to deter the dominant operator from acting in an anti-competitive manner, so the *threat* of regulation may achieve the same result. If it does not, then regulation is called for.

A half-way house between *ex-ante* and *ex-post* regulation arises when competition has been introduced but is not yet well established. A good practice widely used in the US and in the UK in the 1980s came to be known as *incentive* regulation or economic regulation. The regulator would develop a formula to govern when and by how much the incumbent could change tariffs in a way that rewarded the operator for becoming more efficient. One such formula used in the UK was the price cap which allowed British Telecom (BT) to raise its prices by RPI-X, the retail price index minus X% where X is determined by the regulator. So if the rate of retail price inflation was 8% and X was set at 5%, the operator had an incentive to increase efficiency by over 3% to make more profit. The formula referenced a basket of services and within the basket there were individual sub-caps to allow BT to rebalance prices between services. X was adjusted every 3 to 5 years. This example is not to suggest that a price-cap formula is the best solution for all circumstances; it is simply a good solution if it works under local circumstances. The key point is that this was an inventive way to apply solid economic principles to a regulatory problem, combining longer-term regulatory flexibility with short term financial clarity for the investors. It is just one of several options.

Maintaining a Competitive Market

Competitive markets can become less competitive when companies exit the market and when mergers and acquisitions (M&A) reduce the number of network and service suppliers.

[6] See ICT Strategy toolkit http://www.ictregulationtoolkit.org/en/toolkit/notes/practicenote/2880

It is therefore important that the regulator is given powers by the legislature to evaluate potential M&As. This means imposing a requirement on the companies concerned or on the acquiring company to notify the regulator and seek guidance. In some cases this function may be carried out by a separate competition or monopolies commission. A good practice is for the regulator to give advanced advice to the parties concerned to smooth the process. This avoids undue delays, but identifies early on any substantial issues that may need addressing. The regulator can either aim to avoid a company becoming dominant as a result of an M&A by imposing conditions such as the disposal of assets, or can require certain behavioural guarantees such as equal access to network facilities and directory databases in exchange for *ex post* regulatory oversight. These steps may require changes to the terms and conditions of the licence before the M&A is given the green light.

3.2.1 Technology and Service Neutral

Section 3.2 emphasized the need for the licensing and authorization framework to keep pace with changes in the technological landscape because new technologies and standards can give rise to new market opportunities. The traditional problem is that licences issued many years previously may specify the technology or the standard to be used. This was often true by *default* in the case of wireless cellular telephony. If the CDMA standard was used then an allocation within the 800 MHz band was assigned by licence, and if the standard was GSM an allocation within the 900 MHz band was assigned, and so on. With 3G and 4G standards now available innovation in frequency usage enables mobile network operators (MNOs) to use a range of different spectrum bands including 900MHz, 1.8GHz, 2.1GHz, 2.5/2.6GHz, etc.

Promising changes in spectrum use are arising from the so-called digital dividend as frequencies used by analogue radio and TV broadcasts in the VHF and UHF bands are freed up with the shift to digital radio and terrestrial TV or DTT. The 700MHz band especially is seen as having excellent propagation characteristics that could mean much wider area coverage by cellular and other wireless technologies for the same or less investment. This will pose a challenge and an opportunity for policy-makers and regulators. The challenge will be how to allocate these frequencies between the claims of competing services. The opportunity will be to assign these frequencies to new services and to meet the needs of populations in more remote and rural areas. This will be discussed further in section 3.3. The point at this stage is that although regulation through licensing may be needed to ration a scarce resource such as radio spectrum, if the licensing process itself is to become ‘future-proof’ it needs to take a step back from specifying exactly which technologies and standards are to be used. For example, allowing 3G services to be offered over 2G assigned frequencies—a process known as spectrum refarming—is a step in this direction. UMTS900 networks have already been deployed by AIS in Thailand, by Digitel in Venezuela and by DNA in Finland.

No amount of licensing or regulation can predict which technologies and standards will be successful in the market. Some will come and go quite quickly. Paging for example, is not used today but was a popular and conveniently cheap method of text communication in the 1990s, before it was pushed aside by lower cellphone prices. Some standards will enter the market but fail to gain widespread adoption. Local Multipoint Distribution Service microwave or LMDS was a case in point, and the WiMax (Worldwide Interoperability for Microwave Access) may be another. Licensing policies need to be adaptable to accommodate these market experiments because no amount of regulatory foresight can predict the outcomes and, as in the case of WiMax, although it may not be adopted in its mobile version it can nevertheless play a role as a substitute for digital subscriber line (DSL) in some markets. Also a new entrant choosing the standard is more likely to develop a sustainable business plan if the licensing conditions permit it to migrate to an alternative technology (DSL) or wireless standard (4G) as it discovers the market need. This is what is meant by technology neutral regulation: it leaves the choice up to the investor to test the market.

Apps and Services

So far neutrality has been discussed in terms of technology and standards, and in terms of medium, fixed or wireless. Ultimately neutrality is about different services requiring different media and technologies. For example, most standalone MNOs are required to lease backhaul from fixed-line carriers, but they would be in a much stronger competitive position if they could invest singly or jointly (through facilities sharing) in their own lines. If needs be, their license conditions could restrict the usage of those lines to their own business so they do not compete for the retail business of the fixed line carriers; however, even that solution may be considered second-best to outright competition. Certainly unified or converged carriers offering both fixed and mobile services (triple play, including Internet) have a cost advantage in this regard. An alternative solution is to licence independent broadband wholesalers which encourages more cost-effective competition at the retail level.

A new dimension to technology and service-neutral regulation has arisen with the spread of web-based applications that can be accessed through a range of fixed line and wireless network devices, such as smartphones. As many of these apps are OTT and therefore potentially by-pass the tariffs of the licensed carriers' networks, carriers are tempted to restrict the bandwidth made available to their download, either by throttling bandwidth, outright blocking or by levying additional charges on their users. This is the net neutrality issue which is also referenced in module 3.7. It is a point of argument whether regulation that tries to preserve equal access to services for consumers is straying too far into the commercial pricing decisions of operators. In Hong Kong, for example, the regulator took the view that while operators could introduce tiered pricing schemes for consumers to choose from, they could not discriminate against the supply of different apps or content. In other words, once a consumer has established and paid for their chosen level of demand in terms of total broadband capacity they can use per month at the basic fee or in terms of bit rate speeds, they are entitled to access any apps and content up to their chosen limits.

3.2.2 New Authorization Options and Their Implications for Broadband

Regulation of the media and regulation of telecommunications networks and services have traditionally been separate domains of government. The spread of broadband, the convergence of technologies and the search for business synergies between publishing, broadcasting, IPTV and the delivery of content over the Internet has prompted several countries to converge their telecoms and broadcast regulation agencies, although it should be noted that this does not imply that the regulations have fully converged. For example, the FCC in the US was created in 1934 and manages the regulation of both telecoms and broadcast in separate departments. A useful 'Environment Scan' conducted by the Canadian Radio-television and Telecommunications Commission (CRTC) in 2011 cited the Australian Communications and Media Authority (ACMA) as finding that:

> Even in converged legislative frameworks that adopt an industry-agnostic approach to carriage regulation, at this point in the evolution of converged regulatory models, when it comes to content, sector-specific media regulatory measures still generally apply.[7]

However, these changes are bound to impact upon the way in which new authorizations will be made. Modules 3.2 and 3.2.1 have highlighted the important development of technology-neutral and service-neutral licensing regimes and the challenge of keeping the licensing structures relevant to developments in the marketplace. The innovation of multiservice and general licensing was noted, but even these approaches can have their red tape. The multiservice approach, for example, may require different licences for different categories of service and cross-ownership rules may restrict the licences available. In an ideal world, all services would be open to all comers, but in reality markets often support only two or three profitable ventures,[8] raising fears of dominance or, possibly, of collusion. For this reason, easing the licensing requirements for service providers and content distribution networks (CDNs) may prove an effective countervailing power within the market.

[7] Cited in CRTC (2011) 'Environmental Scan of Digital Media Convergence Trends: Disruptive Innovation, Regulatory Opportunities and Challenges' http://www.crtc.gc.ca/eng/publications/reports/rp110929.htm#s1

[8] In 1976 Bruce Henderson, the founder of Boston Consulting Group, argued empirical data seemed to show that as markets matured three companies would come to dominate in the ratio of approximately 4:2:1. The marginal company (number three or four) would be hard pressed to remain profitable. This very often seems to be the case in telecom markets. See 'BCG Classics Revisited: The Rule of Three and Four' https://www.bcgperspectives.com/content/articles/business_unit_strategy_the_rule_of_three_and_four_bcg_classics_revisited/

Much of the content today is likely to come from overseas, through broadband, through the Internet and through CDNs. Policy-makers and regulators are therefore faced with additional decisions to make: should they confine licensing and regulation to domestic-based service providers and permit open access to external services? Or, should they attempt to impose domestic conditions upon external services? If so, how? For example, in some jurisdictions, overseas service providers are required to register an official presence in the country. Vietnam has proposed this, but only as a point of official contact and not, it seems, as a means to carry liability in the case of a dispute.

The arguments for regulation usually relate to the need to screen out unacceptable apps and content. This is clearly a decision that has to be taken at the national level, but a good guideline is that if there are to be regulations and restrictions they should meet two conditions. Firstly, what is regulated and restricted should be a fair reflection of what is legal and illegal in local law, otherwise there is a danger of arbitrariness, lack of policy transparency and even of due process. Secondly, regulations and restrictions should be proportional to the threats or dangers involved. For example, content that glorifies or promotes hatred and violence is far more harmful than content that makes parody and criticism. An additional important element to consider is the *intention* of the content. For example, content that makes a damaging untrue statement about a person may be deliberate libel or it may be an unintended error. Proportionality in the application of law should be able to draw the distinction and apply that in the remedy, in this case an apology and/or a takedown rather than a prosecution.

3.2.3 Disputes Resolution Procedures

Moving from an incumbent monopoly towards an open entry and free market in telecommunications is a process that from time to time inevitably generates disputes between the regulator and the operators, between different operators and between operators and customers.[9] Disputes with regulators are most frequent when licensing conditions are being imposed such as steps to curb anti-competitive behaviour, the imposition of price controls, and the granting of permissions to market new services. Disputes between operators are more likely to centre around competition issues, such as discrimination in the cost of interconnection or in providing access to unbundled network elements (UNEs) – see Module 3.6 – and claims of misrepresentation arising during combative marketing campaigns. Billing, quality of service and waiting lists are the types of issues most likely to arise between customers and operators.

[9] See infoDev/ITU 'ICT regulation toolkit' http://www.ictregulationtoolkit.org/en/section.2069.html and ITU/World Bank (2004) *Dispute Resolution in the Telecommunications Sector: Current Practices and Future Directions,* Discussion Paper by Robert R. Bruce and Rory Macmillan (Debevoise & Plimpton*)* and Timothy St. J. Ellam, Hank Intven, Theresa Miedema (McCarthy Tétrault LLP) http://www.itu.int/ITU-D/treg/publications/ITU_WB_Dispute_Res-E.pdf

Dispute resolution procedures usually take one of two forms: either official government channels such as the regulator, a statutory arbitration court, an appeal to a minister or to the Supreme Court, or through unofficial channels – also referred to as alternative disputes resolution (ADR) – involving a voluntary process and an arms-length arbitration panel. Consumer councils often play an important role representing user interests, but they do not always enjoy an official status. Sometimes, as in Thailand, the regulator's office helps to create a consumer protection agency.

Where disputes arise over a regulator's decision it is best practice to establish some kind of telecoms tribunal, in Hong Kong called the Telecoms Appeal Board,[10] to ensure transparency. But the appeal will be confined to examining whether the regulator followed due process and not a challenge to the regulator's statutory powers to make a judgement. Like many other jurisdictions, Hong Kong has also established an ADR mechanism called the Customer Complaint Settlement Scheme (CCSS) similar to Australia, New Zealand and the United Kingdom to help resolve disputes between operators and users.[11] In 2013, Hong Kong's six mobile virtual network operators (MVNOs) agreed to join the scheme which already covered fixed and mobile network operators.[12] The importance of ADRs is they can provide fast and also less costly solutions to relatively small disputes without taking away the legal rights of the parties concerned.

Other approaches to dispute resolution include judicial or semi-judicial tribunals that adopt court-like procedures. For example, India has placed the procedure in the hands of an independent Telecom Dispute Settlement and Appellate Tribunal (TDSAT) presided over by a retired high court judge. In his assessment of the dispute resolution in India and influences upon it from around the world, R.U.S.Prasad notes the importance of Malaysia's approach, although in the latter case the tribunal's chairman, also a retired high court judge, is subject to appointment and possible dismissal by the minister.[13] In the US, where the role of litigation is more accepted as part of commercial life, the decisions of the Federal Communications Commission (FCC) are generally regarded as final. However, law judges are involved during hearings leading up the final decision of the Commissioner, and FCC rulings are frequently subject to Court of Appeal challenges.

[10] http://www.cedb.gov.hk/ctb/eng/telecom/relevant2.htm

[11] For Hong Kong see http://www.ofca.gov.hk/filemanager/ofca/en/content_793/ta_stmt_en.pdf; for Australia see http://www.tio.com.au/; for New Zealand see http://www.tdr.org.nz/; for the UK see http://consumers.ofcom.org.uk/tell-us/telecoms/adr/

[12] http://www.ofca.gov.hk/filemanager/ofca/en/content_793/press_release3.pdf

[13] R.U.S. Prasad (2008) 'Dispute Resolution Mechanisms in the Telecom Sector: Relating International Practices to Indian Experience', Stanford Center for International Development: Working Paper No. 372 (September) http://www.stanford.edu/group/siepr/cgi-bin/siepr/?q=system/files/shared/pubs/papers/pdf/SCID372.pdf

The legal and commercial histories of countries differ widely, so different approaches to dispute resolution apply, but if there is one underlying principle that should be common to all is transparency.

Module Three: Law and Regulation for a Broadband World

3.3 Spectrum Management

In the fixed line world the original ISDN-B definition of broadband was 144 Kbps; that is a bit rate or in other words the size (byte) over a period of one second of a video or audio stream download or upload. Modern broadband wireless access (BWA) networks and devices operate at bitrates that now run into Mbps and, under laboratory conditions, even Gbps.

Bit Rates and Frequencies

Although there is no direct relationship between bitrates and radio frequencies or Hertz ("wave cycles per second") it is the case that higher frequencies with shorter wavelengths occupy broader bands of spectrum. So, for example, 1.8GHz is twice the spectrum of 900MHz. By allocating higher frequencies to services such as public land mobile networks (PLMN) there is additional spectrum available for more operators and therefore more competition in the market. Because they are broader and shorter, the higher frequencies, (above 1GHz) are well adapted for densely populated urban areas, but offer less coverage for wider suburban and rural areas. This can be an important commercial issue because it means that lower frequencies offer lower costs in terms of base stations, towers and backhaul coverage to operators who are looking at less densely populated markets. As a consequence in a spectrum auction mobile network operators (MNOs) may bid more for these lower band frequencies than for the higher ones, although historically the opposite has been true because MNOs first targeted urban markets. Ultimately, 10MHz, 15MHz or 20MHz of bandwidth is the same whatever the frequency; what really matters is the technical capacity of the network equipment and of the access devices operating at these frequencies. An example of this is the development of broadband satellite services for fast Internet access and HDTV.

Policy Aims

What are the aims of policy? This question has to be the first thing to consider from a regulator's perspective when deciding the allocation and assignment of spectrum for broadband services. Different policy aims require different regulatory objectives. For example, if the policy aim is to stimulate service innovation, then the regulatory objective could be to increase the supply of unlicensed spectrum and/or to facilitate spectrum sharing. If the primary aim of policy is to ensure greater competition and consumer choice, then the regulatory objective will be to assign spectrum to new entrants and maybe to facilitate the entry of mobile virtual network operators (MVNO) – see Box 3.1.

Box 3.1

MVNOs

A Mobile Network Operator (MNO) has market power by virtue of owning radio spectrum and a network. By contrast, a Mobile Virtual Network Operator (MVNO) is dependent upon an MNO for both to provide services such as voice, SMS and data to end-users.[14] MVNOs do have full control over their branding, marketing, billing and customer care operations,[15] and compete by providing flexible plans, tailored services, loyalty programs etc. With the advent of broadband and smartphones a new range of possibilities is opening up, including m-payment services and specialized apps and content for targeted markets.

Broadband has encouraged MNOs to shift from charging high wholesale prices to MVNOs to selling 'buckets' of bandwidth. In some cases they take a revenue share from MNVOs who create new markets, such as the MNVO in the US that has started a retail portal that sells almost any brand of smartphone.[16] In other cases the MVNO is an affiliated company operating in an overseas market – see below for the example of the Philippines. Basically, broadband is giving MVNOs a new lease of life. The first MVNO was launched in 1999 by Virgin Mobile (UK) and as of late 2012 there were over 630 licensed MVNOs worldwide.[17]

PLDT and Remittances

MVNOs tend to focus on customer maintenance rather than customer acquisition, bundling value-added services (VAS) with a suit of other product offerings such as remittance and e-commerce. The Philippine Long Distance Telephone Corporation (PLDT), which links its MNVO services overseas with other offerings catered to Filipino migrant workers, is a good example. These include a remittance service called Smart Pinoy Remit and an e-commerce website called Smart Pinoy Store. The Smart Pinoy store allows Filipinos working overseas to purchase groceries, gift cheques, flowers and other items online to be sent to their families back home or pay for their family's PLDT landline or Smart post-paid bills. Through agreements with different MNOs, PLDT has been able to launch its MVNO services in Hong Kong, Singapore, Guam, Taiwan, Macau, Malaysia and the UK and has plans to launch in the Middle East, North America, Africa and other parts of Europe.

Brazil and MVNO Regulation

Brazil is a good illustration of how targeted regulation can open up a market for MVNO entry. Brazil is the largest mobile market in Latin America with more than 260 million subscriptions in 2011 of which 80% are pre-paid, and a penetration rate of over 130% as of

[14] http://www.telecomspace.com/latesttrends-mvno.html

[15] http://www.mobilein.com/what_is_a_mvno.htm

[16] http://gigaom.com/2012/06/25/why-are-mvnos-so-hot-right-now-thank-the-carriers/

[17] http://www.mvnodirectory.com/overview.html

April 2013.[18] The Brazil market is highly competitive with the four biggest mobile network operators (Vivo, TIM, Claro, and Oi) holding close to a quarter of the market each.[19]

In 2010, the telecom regulator Anatel approved regulations that would create two types of MVNOs.[20] The first is where an agent ('credential' model or *credenciado de red virtual*) of a mobile operator, with ANATEL's approval, reaches a commercial agreement with an institutional customer such as a bank, a retail chain store or a football club. By falling outside the definition of a public telecommunications service this is an encouragement to non-telecom players. The second is the traditional MVNO ('authorized' model or *autorizado de red virtual*).

The first two MVNOs, Porto Seguro Conecta and fixed-line operator Sermatel (Datora Telecom), were approved in 2011 and launched in 2012. Porto Seguro Conecta is operated by Porto Seguro, an insurance company. Its initial service offering focuses on Machine-to-Machine (M2M) communication providing vehicle tracking services owned by its insurance customers. The two MVNO licence holders have partnered with the TIM network.[21] As of March 2013, Porto Seguro reported having 41,377 subscribers and Datora 1,000, while four more MVNOs have announced their entry and three more are in the planning process.[22] Maybe not all will survive but by opening the market to MVNOs ANATEL has succeeded in stimulating investment in services competition and innovation.

MVNOs and Regulators

MNVOs offer regulators a way to increase competition at the retail level and innovative services that can cater for market minorities. They offer MNOs a way to raise more revenue from networks that have spare capacity. In China in 2012 the Ministry of Industry and Information Technology (MIIT) announced a two-year MVNO trial plan as a way to attract more private capital into its telecommunications market.[23] Unlike MNO VANS (value-added *network* services) operators, VAS operators have little or no direct control over the network, its capabilities and performance. Therefore many of the regulations regarding QoS applying to MNOs are not necessarily applied to MVNOs. On the other hand, MVNOs do control their own billing systems, so regulations safeguarding consumers can apply. Although wholesale pricing is usually left to commercial negotiations, if the ministry wishes to positively encourage MVNO entry there may be a case for regulation, but care needs to be taken that it does not remove the incentive for the MNOs to share their networks.

[18] http://www.teleco.com.br/ncel.asp

[19] http://www.gsma.com/spectrum/wp-content/uploads/2012/10/gsma_brazil_obs_web_09_12-1.pdf

[20] http://www.internationallawoffice.com/newsletters/detail.aspx?g=bffed9bb-67b7-46ce-85ee-6c14d779828f

[21] http://www.rcrwireless.com/americas/20120827/carriers/brazils-porto-seguro-launched-first-mvno-operations-country-m2m-services/

[22] http://www.teleco.com.br/en/en_mvno_br.asp

[23] http://www.zdnet.co/china-encouraging-private-investments-in-telecom-industry-2062305275/

If the policy aim is to raise revenue for the treasury, then the regulatory objective will be to design an auction in a way that maximizes the bidding prices. If the policy aim seeks to achieve is mix of the two then the regulatory objective may be to reserve some of the spectrum to be auctioned for new entrants only. A successful auction will then allow a new entrant into the market but maybe at the expense of raising less revenue than if the entire spectrum were open to all bidders.

The means of achieving regulatory objectives will vary. Auctions have become popular among regulators who look for market solutions, and are tending to replace the traditional ‘beauty contest’ approach by which regulators pick and choose the winners. One big disadvantage of the beauty contest approach is its lack of transparency, making it vulnerable to corrupt practices. But not all spectrum will be assigned by a market mechanism. Many public services, such as public protection and disaster risk (PPDR) services used by the police and first responders such as fire and ambulance services, are assigned spectrum by administrative means, also known as ‘command and control’. In many countries the armed services also control large swathes of spectrum, as do utility companies running facilities such as seaports, airports, electricity grids, roads and rail networks. Increasingly regulators are looking for ways to increase the efficiency with which these legacy assignments are used so they can free up spectrum for new broadband services. The use of ‘administrative spectrum pricing’ or ASP (sometimes called ‘administrative *incentive* spectrum pricing’) is one way to do this by assigning a price usually based upon some notion of the ‘opportunity cost’ of using the spectrum for some other purpose. Another way is to carry out an efficiency audit using radio engineers to make an assessment.

Box 3.2

Hong Kong Approves Administered Incentive Pricing

Statement published 19 June 2007: Executive Summary

This Statement follows Ofcom’s consultation on the future pricing of spectrum used for terrestrial broadcasting. It sets out our intentions in respect of:

- implementing charging for spectrum used for digital terrestrial broadcasting of television and radio; and
- extending the current charging regime for analogue commercial sound broadcasting to the spectrum used by the BBC for its radio services.

Ofcom’s decision

In July 2006, we consulted on proposals to implement administered incentive pricing (AIP) for spectrum used for terrestrial broadcasting. We did so on the principle that one of the best ways of ensuring that the opportunity costs of spectrum are fully and accurately reflected by decision-makers is for those opportunity costs to be reflected in prices that have to be paid to hold spectrum.

The consultation produced a number of responses, which this Statement outlines and which we have considered fully. Our overall conclusions are that:

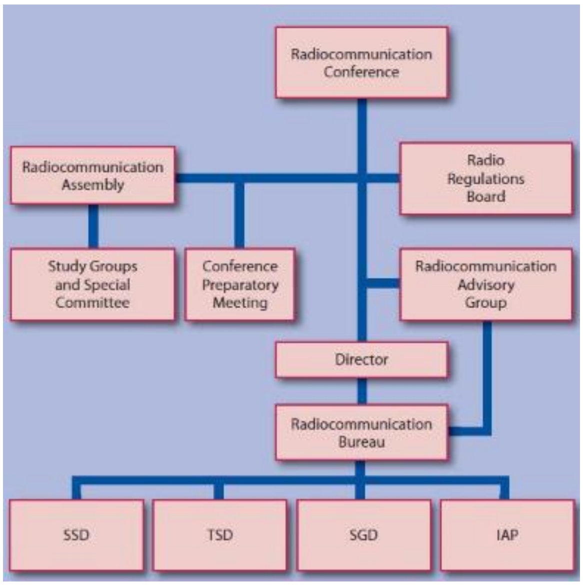
- it is right that broadcasting use of spectrum should be subject to appropriate charges in future, in the same way as almost all other uses are or will be;
- the right time to introduce charging for spectrum used for digital broadcasting – both television and radio – is the end of 2014;
- the right time to extend the existing charging regime for commercial analogue radio spectrum to that used by the BBC is 2008;
- before introducing any charges, we will consider carefully any potential effects on broadcasting output, and the right options to address or mitigate them.
- Source: http://stakeholders.ofcom.org.uk/consultations/futurepricing/statement/

Preventing Radio Interference

Given the new focus upon broadband wireless the starting point for all spectrum management policy making and regulation remains the recommendations of the ITU's World Radiocommunications Conference (WRC), held every three to four years. The topics are set six years in advance and the final agenda around three years in advance. This gives time for the Study Groups and technical standards bodies to make their recommendations.

Figure 3.3

ITU-R Sector Organization


Radiocommunication Conference
Radiocommunication Assembly
Radio Regulations Board
Study Groups and Special Committee
Conference Preparatory Meeting
Radiocommunication Advisory Group
Director
Radiocommunication Bureau
SSD
TSD
SGD
IAP

Source: http://www.itu.int/ITU-R/index.asp?category=information&rlink=sector-organization&lang=en
SSD: Space Services Department; TSD: Terrestrial Services Department; SGD: Study Groups Department; IAP: Information, Administration and Publications Department

The only *mandatory* requirement for ITU membership is a commitment to avoid radio interference with neighbouring countries. All else is about the adoption by national regulatory authorities (NRAs) of WRC and ITU recommendations on policies, standards, etc.

The avoidance of radio interference clearly should always be the number one consideration and in light of new 'intelligent' technologies, an interesting reaffirmation of this came in the US from the FCC's 2012 Notice of Proposed Rulemaking (NPRM) for broadband satellite services. FCC Chairman Julius Genachowski explained: "We're proposing to modernize, streamline, or eliminate hundreds of rules or subsections governing satellite services. Among the changes, this Notice includes a shift in the focus of the rules from a 'tell us how you built it' approach to a 'tell us how you will avoid interference' approach." [24]

Harmonization

An issue of growing significance for NRAs are efforts to achieve harmonization of spectrum allocation across neighbouring countries to gain economies of scale in the equipment standards used across the region and to facilitate roaming. Roaming was previously a voice service on mobile phones, but that is changing as broadband data roaming services using smartphones, tablet computers, etc., become more popular. Important past initiatives by the ITU have included the 'Harmonization of the ICT Policies in Sub-Sahara Africa' (HIPSSA) with EU support[25] and a joint programme with the Caribbean Community and Common Market (CARICOM) named 'Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures' (HIPCAR).[26] Both these programmes have now concluded.

In Asia, the ASEAN group of nations is also working towards harmonization, including freeing up the spectrum in the VHF and UHF bands through the switch from analogue to digital terrestrial TV (DTT), known as the digital dividend. Asia somewhat lags behind other regions in making progress towards harmonization as the paper 'The Digital Dividend in Asia' explains.[27] One of the most influential organizations in the region promoting a common approach towards the digital dividend is the Asia Pacific Telecommunity or APT based in Bangkok.[28] However, as each ASEAN country has its own legacy of spectrum allocations which include military and government as well as commercial bands, harmonization is not easy to accomplish. ASEAN has its own general policy document for the harmonization of ICT developments within South East Asia—the 2010 *Masterplan on ASEAN Connectivity: One Vision, One Identity, One Community (MPAC)* [29]—with a roadmap called the *ASEAN ICT*

[24] http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-12-117A2.pdf
[25] http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/
[26] http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/
[27] http://trpc.biz/wp-content/uploads/2012-07-17_IICAsiaForum_DigitalDividend_BriefingPaper.pdf
[28] http://www.aptsec.org/AWG-Spectrum
[29] http://www.aseansec.org/documents/MPAC.pdf

Masterplan 2015.[30] Both are discussed in 'ASEAN ICT Masterplan 2015: IIC Asia Forum, April 2012'.[31]

Spectrum Scarcity Debate

Alongside the rising demand for spectrum for broadband services there has been an accompanying debate over whether or not there is a spectrum supply shortage. The arguments consist of several different points. There is a straightforward view that demand has outstripped supply, especially with the rise of social media and video streaming, massive multiplayer online gaming (MMOG), etc. Equipment vendors and operators typically argue this point.

There is another view that too many operators are not using their spectrum fully and efficiently and if they did so there would be little or no shortage. This view was put forward in a report by two CitiGroup researchers in 2011 who argued that in their estimation in the US only about 35.7% of spectrum set aside for wireless communications was being used for that purpose.[32] Those with spare spectrum, they argued, lacked the capital to invest in networks, while those with networks lacked the additional spectrum to expand their services. Others have pointed out that at least some of the spectrum held in reserve by operators is not necessarily inefficient but rather good investment management, ready to take advantage of emerging new technologies and standards. It is also the case that under-used spectrum can be held by non-telecom bodies such as the armed forces, the emergency services, public utilities such as power and transportation companies, etc.

In the US the FCC (Federal Communications Commission) takes the view that there will be a shortage as demand outpaces supply unless more spectrum is released as part of the 2010 National Broadband Plan. The FCC also considers that a lot of spectrum is being under-utilized and that smart regulation should find a market solution to this problem. The FCC "needs to create new incentives for incumbent licensees to yield to next-generation users"[33] and proposes 'incentive auctions' as one way to do this. In an incentive auction the licensee who gives up the spectrum to the highest bidder either keeps the revenue and pays a commission to the FCC for running the auction, or shares the revenue with the FCC. The reason why incentive auctions may be necessary is because historically the cost and time of

[30] http://www.scribd.com/doc/111870071/ASEAN-ICT-Masterplan-2015

[31] http://trpc.biz/the-asean-ict-masterplan-2015/

[32] Jason Bazinet and Michael Rollins (2011) 'Wireless Data: Supply and Demand Spectrum Control, Not Availability, Is the Real Constraint' Citi Investment Research & Analysis

[33] http://www.broadband.gov/download-plan/ chpt 5, p.11

clearing entire bands of spectrum from previous occupants and reallocating them are too high and takes too long, sometimes beyond 10 years.[34]

Allocating additional spectrum is one issue; how to assign it to users is another. The most valuable spectrum below 1GHz has been assigned by methods such as 'command and control', 'beauty contest' and increasingly through market auctions, but an alternative approach is to release spectrum for free as a public commons. This already happens in many frequency bands as unlicensed spectrum, but a public commons approach implies higher emissions and therefore the need for some form of regulation. These issues are discussed in the next modules.

Conclusion

Making judgements about the future supply and demand for radio spectrum is precisely that, a judgement, and one that will require continuous revisiting. On the supply side, new technologies are rapidly increasing the efficiency of frequency usage, yet which technologies will succeed in the marketplace can never be known with certainty. On the demand side, service innovations and changes in user preferences also happen quite quickly, especially over broadband wireless networks. Given this reality, regulation needs to become smarter, that is to say: it needs to mimic market incentives as far as possible; it needs to be transparent so that investors and users can plan ahead; and, it needs to become more flexible to take account of changing conditions and requirements. The rest of this section of module 3 will further explore these issues.

3.3.1 Spectrum Licensing Regimes

The growing demand for spectrum for broadband covers a range of wireless technologies and standards. Each category lends itself to different regulatory approaches.

Low-powered short-to-medium range communications

The broadband era is seeing the coming of the 'Internet of things'. Every object, whether it is a device such as a mobile phone, a TV or a refrigerator, a vehicle or even a piece of clothing, can be connected to the Internet or directly to another object by short-range radio using Internet Protocol. Different technologies, such as Bluetooth and Zigbee, have been developed to provide the communications standards. The spread of these machine-to-machine (M2M) communications will grow exponentially and are becoming the central component of smart cities. Already smart cars send system alerts to mobile phones and

[34] http://www.broadband.gov/download-plan/ chpt 5, p.8 Exhibit 5-C. The National Telecommunication and Information Agency (NTIA) concluded it would take 10 years and cost US$18 billion to clear a 95 MHz band http://frankrayal.com/2012/08/26/exclusive-versus-shared-spectrum-scarcity-to-abundance/

computers. Electronic Road Pricing (ERP) schemes, as used in Singapore, deduct payments from stored value cards displayed on vehicle windscreens each time the vehicle passes under a gantry. Hundreds of millions of electricity meters, water meters, early warning sensors ready to detect earth tremors or fires are operational; because the power emission from these devices is extremely low and radio interference is not an issue the frequencies do not need to be licensed.

Along with these developments there will be an increasing level of innovation surrounding the 'Internet of things'. New devices and new services will emerge and in some cases this may call for a raising of the limits on power emissions. In such cases, an alternative to licensing is to allow industry to adopt its own codes of conduct with respect to frequency sharing and frequency hopping, but the regulator needs to be reassured that this is technically possible and presents no risk to public health. It is important that regulators have access to the independent technical expertise necessary to make these judgements, for example, by establishing a Radio Advisory Committee or by bringing in a consultant.

Mass wireless communications

The licensing of MNOs (mobile network operators) to build PLMNs (public land mobile networks) has traditionally followed the contours of the technology standards being used, but this is starting to change. 2G standards typically used 800MHz (CDMA) and 900MHz (GSM) bands, while UMTS standards for 3G used a variety of bands for W-CDMA, notably 2100MHz (Band l) and 900MHz (Band Vlll) in most of Europe, Africa and Asia, 1900MHz (Band ll) and 850MHz (Band V) in the Americas, 1700MHz (Band lll) in the USA, etc., while WiMax, a different standard, is typically allocated 2.3 GHz, 2.5 GHz and 3.5 GHz frequencies and WiFi 2.4GHz. The equipment itself can be manufactured to be tuned into whatever frequencies are allocated, and licences were linked directly to these allocations.

With the arrival of 4G LTE and LTE Advanced and Mobile WiMax a new stage has been reached in spectrum management. On the one hand, these standards are meeting the demands for greater bandwidth or frequency capacity driven by the growing demand for bandwidth-hungry applications. This puts regulators under pressure to find additional spectrum. On the other hand, the digital dividend which frees up large amounts of bandwidth from analogue radio and TV in the VHF and UHF bands offers regulators a once-in-a lifetime opportunity to re-allocate 150MHz or more spectrum. In addition, regulators are searching for spectrum that is either unused or under-used in other frequencies. The result is an opportunity for 4G MNOs to occupy and operate from a variety of frequencies as suits local circumstances and increasingly regulators are starting to look towards multi-frequency auctions called, somewhat clumsily, Combinatorial Clock Auctions or CCA auctions where bidders can combine ranges of frequencies from different bands.[35] Frequency aggregation techniques (discussed later) are an advanced method by which MNOs can use these frequencies in combination.

With all these changes regulators need to revisit their licensing regimes to allow MNOs greater flexibility in their use of frequencies from different bands, because licensing that links an MNO's network to a specific band simply will not work in this situation. This is discussed further under 3.3.3 Allocation and Assignment.

Flexibility has arisen in another aspect of licensing of MNOs where they need to buy or build backhaul capacity to manage the growing demands of traffic across their cellular networks. Leasing backhaul capacity from a fixed-line incumbent can be very costly while the lack of such capacity threatens the quality of service that can be offered to the public. Regulators would seem to have at least six options to choose from to relieve this bottleneck problem.

First, where the incumbent fixed line operator also has a licence to provide wireless mobile services a unified licence can be issued to replace the separate licences and thereby encourage greater network integration or fixed-mobile convergence. India was the first jurisdiction to introduce this innovation. However, this does not solve the problem if the incumbent is permitted to discriminate against competing MNOs. Equal access is an important part of maintaining free and fair competition. A second option is to licence MNOs to build their own fixed-line or microwave backhaul networks but limit the use either to own-services or to wholesale services; the latter of these options has the virtue of introducing greater competition into the wholesale market. A third option is to allow MNOs to share backhaul facilities such as towers, as well as to share cell sites and thereby spread the costs. A fourth option is to licence a separate wholesale network provider who can serve the entire market in competition with incumbent fixed-line operators. A fifth option is to licence non-telecom entities such as utility companies to lease their own fixed-line or microwave capacity to MNOs. A sixth option is to allocate spectrum to WiFi, which can be used to offload data traffic from congested cellular networks. In addition, public-private partnership (PPP) arrangements can sometimes help in each of these cases where there is a need to reduce operational and capital risk, but as one former finance minister warned there is a danger of them escaping "both the discipline of effective state (i.e. Treasury) control and the discipline of the marketplace."[36] PPP may be especially helpful in areas

[35] See a discussion of the advantages of the combinatorial clock auction in the UK by OFCOM http://stakeholders.ofcom.org.uk/binaries/consultations/1452design/summary/1452design.pdf

[36] Nigel Lawson 'How flawed government policies and state backing for home loans led to disaster in the US housing market', Seeds of Subprime Review Article, 16th November 2012, *The Financial:* http://www.ft.com/intl/cms/s/2/b78369aa-2a8e-11e2-99bb-00144feabdc0.html

which are serving national policy interests such as providing access to rural and remote locations.

Long-distance terrestrial backbone and backhaul microwave technologies

Licensing non-telecom companies such as national rail and road systems and energy grids to lease their long-haul capacity is an obvious step towards greater capacity for MNOs and for competition in the wholesale market. Licensing to permit facilities sharing such as towers, ducts and leased circuits is another way to solve the bottleneck problem and is being adopted in many countries.

Extra-terrestrial satellite microwave

Broadband satellite services currently offer fast internet connections to many areas that are not served by terrestrial connections. They will become even more important in the coming era of ‘connected TVs’, television sets with Internet connectivity enabling viewers to download movies, watch live sports, view videos, play MMORPG, etc. In many low income countries these developments may seem an age away, but in the metropolitan centres of countries that are well integrated into the global economy these are the new consumer products of the present day. In many rural areas, mountainous landlocked countries and remote small island economies, satellite remains the only way to gain access.

Traditionally, C-band satellites requiring receiver dishes several feet in diameter were used mostly for broadcast services, and as a back-up for telecom services. L-band is used for GPS and more and more devices use GPS. Ku-band satellites offer higher bandwidth and a narrower footprint and are widely used by Vsat transceivers to provide commercial access mainly to data services. Now Ka-band satellites, which operate at speeds 100 times faster than Ku-band, are offering high-speed broadband Internet access to areas previously unreachable, although attenuation problems often arise on these higher bands due to tropical rainfall. Many countries cannot afford a satellite of their own, but they can licence local service providers who lease satellite channels. Licences need the flexibility to take advantage of technologies such as dynamic frequency allocation that can supply different levels of service to different locations.

Licensing and Innovation

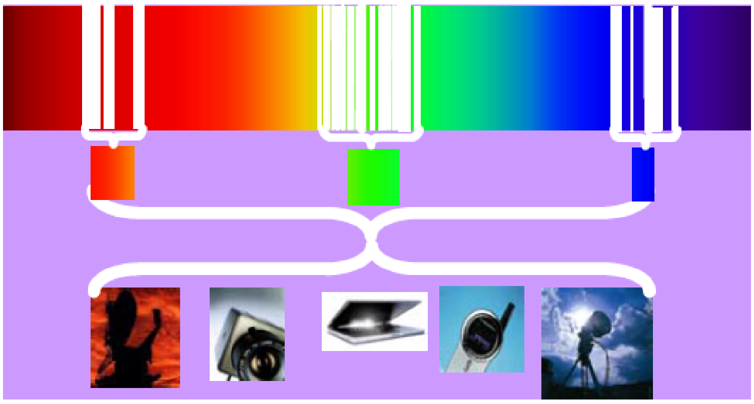
Flexible licensing policies can help unlock innovation. With the coming of the ‘Internet-of-things’ and the real possibility of smart cities that can, among other things, help address the issue of energy consumption, carbon emissions and climate change, the role of licensing has extended beyond its initial aims of imposing strict operational requirements upon service providers, and even beyond the aim of making competition work. It is now addressing the issue of how to stimulate and facilitate innovation in the use of spectrum and in the provision of new services. This affects the competitive advantage of an economy and helps to create jobs and revenues: regulation, technologies and markets are all interconnected, each affecting the other. The demands of the market spur on technology innovations such as cognitive radio for spectrum sharing, intelligent antennae for better radio coverage, and spectrum aggregation techniques for a more efficient use of available spectrum. The changing role of licensing is therefore an important facilitator of this virtuous cycle and necessary to encourage investment in these new network services. (See also Kim, Kelly and Raja (2010) 'Building Broadband: Strategies and Policies for the Developing World' http://www.infodev.org/en/Article.454.html)

3.3.2 Flexible-Use Technical and Service Rules

The management of radio spectrum is an area of policy and regulation that has greatly expanded in recent years. This module is focused upon broadband which, in the early years of wireless telecommunications, was more or less synonymous with the higher shorter frequencies. For example, 1GHz is a band of spectrum twice as broad as 500MHz. The disadvantage of the limited propagation characteristics of shorter frequencies was offset by the fact that broadband cellular services, notably 3G and beyond, were focused upon dense clusters of customers in urban areas. Dual-band handsets allowed handoff to lower frequencies when users roamed from urban to suburban and rural areas. In more recent years another dimension has become important, the vastly increased bitrates cellular and other wireless networks and devices can now handle.

In addition to these two dimensions – the propagation effects that determine coverage and the uplink and downlink speeds that determine traffic loads – there have been a multitude of other technological advances. These include: cognitive radio (CR), which is software-defined radio (SDR) that allows devices to detect other users to avoid radio interference; intelligent antennae and the use of multiple antennae or MIMO (multiple-input and multiple-output), which give radio signals greater sight around obstructions; and, spectrum or frequency aggregation techniques, which allow service providers to operate across several different spectrum bands simultaneously. This increases the efficient use of under-utilized or isolated frequencies which may have resulted from an earlier fragmentation of frequency assignments. Figure 3.4 below illustrates the principle of spectrum aggregation.

Figure 3.4
Spectrum Aggregation



The concept of spectrum aggregation is to exploit spectrum fragments simultaneously to create wider bandwidths for communications systems.

Source: Dr Anil Shukla, Brian Willamson, John Burns, Eddie Burbidge, Alan Taylor, David Robinson (2006) '*A Study for the Provision of Aggregation of Frequency to Provide Wider Bandwidth Services*' QINETIQ http://www.aegis-systems.co.uk/download/1722/aggregation.pdf

Efficiency and Innovation

Rapid technological advances in network capabilities and a growing demand for broadband access (network availability) and usage (network capacity) are starting to throw up major challenges for regulators. There is only so much spectrum available, so using it efficiently has become an issue of prime concern. Promoting innovation is one way to do this. It is also a way to raise the efficiency and competitiveness of the economy-in-general, create jobs and new services. The regulator's job is becoming much broader in its scope than before.

As the number of services that can be offered across BWA networks has multiplied, regulators often took to licensing networks and services separately in recognition that some services would be provided by MVNOs (mobile virtual network operators) or by third parties such as content aggregators and application service providers. This distinction is now more complex with the interconnectedness of the Internet because many services can be provided from outside the country OTT (over-the-top of the network). Technically, everything from making telephone calls to downloading movies to installing apps on a smartphone or a tablet can be done OTT without a licensing regime in sight. While these developments are more advanced in the most developed economies of the world, they are rapidly establishing themselves as global trends and they make many of the old regulations look outdated, which means they can become obstacles, or in some cases irrelevant, impossible to apply or enforce.

A good example of innovation is the growing interest in 'white space' or 'TV devices'. These are transceivers that either use SDR or cognitive radio, or consult a master database, to detect frequencies that are not being used by others and are available for use to provide 'white space' service such as 'super WiFi' (also known as White-Fi and as the IEEE 802.22/IEEE 802.11af standard for Wireless Regional Area Network or WRAN). Their name comes from their use of the unused or 'white spaces' between TV channels in the UHF 700MHz frequency band and as and when analogue TV shifts to digital terrestrial TV broadcasting (DTT) these frequencies become available for re-allocation. However, to make *unlicensed* use of these frequencies there needs to be agreement with the regulator and a set of acceptable standards in place to ensure non-interference with primary users, namely radio and TV broadcasters.

Box 3.3

TV Devices: White Spaces - Super WiFi

IEEE 802.22/802.11af WiFi standards have a wide area range that can provide local community hotspots offering free Internet access far beyond ordinary WiFi. In addition, local operators could offer local apps and services but if business revenues are generated a licensing regime is likely to follow.

In the US, the FCC has already allocated spectrum for white space 'super WiFI' services in the 700MHz "digital dividend" band. Although one way for white space devices to avoid interference with other users of shared spectrum is to scan the frequencies with CR, the method remains in its early stages and the preference in the US is to license companies to run databases of users which can be scanned at regular intervals.

As of 2013, trials have been ongoing in Canada, the UK, Ireland, the Netherlands, Japan, Korea, Philippines, Singapore, South Africa, Nigeria, Kenya and Tanzania with some trials commencing in South America. In South Africa, for example, in Cape Town Google is collaborating with a number of international wireless vendors and local educational research bodies to offer Internet access on a trial basis to 10 schools. Using white space radio devices across 400MHz of fragmented TV spectrum that supports up to 15 broadcast channels, the school furthest away from the transmitter (6 kilometers) is still able to receive 6Mbps when the signal is uncontested allowing the school for the first time to download computer programme and anti-virus upgrades. In the highly urbanized environment of Cape Town, Google is demonstrating the value of its database that instructs white space devices which frequencies are available without causing interference to TV broadcasting and other users. (http://gigaom.com/2013/07/03/inside-googles-innovative-african-broadband-trial/) In the northern and rural province of Limpopo, Microsoft in partnership with the Council for Scientific and Industrial Research, the University of Limpopo and a local network contractor, is demonstrating how WSDs can provide broadband coverage to a population thinly spread over a wide area. (http://www.microsoft.com/en-us/news/Press/2013/Jul13/07-274AWhiteSpacesPR.aspx)

Spectrum Markets

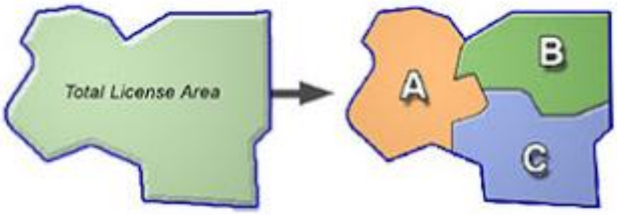
The push towards market-oriented solutions is most evident in the use of auctions. Since the first auction in 1993 in the US they have become a frequently used instrument in the regulator's toolkit. However, auctions do not always produce the desired results. This is sometimes due to the way they are designed and conducted, sometimes to a lack of investor confidence in the market, and sometimes to the opposite, over-bidding by investors. General economic conditions play a large part in investor perceptions, and changes in markets and in coming technologies also have an impact. So just as regulation impacts upon technological innovation and markets, so they impact upon regulation and, in this case, one answer is to allow secondary markets to operate which have the advantage of allowing market conditions rather than regulation determine the most efficient use of the spectrum. Allowing spectrum trading can be less time consuming and less expensive of regulatory resources. Also secondary trading markets can be operated as online spectrum exchanges run by independent third party specialists, subject to regulatory oversight.

Box 3.4

Spectrum Trading

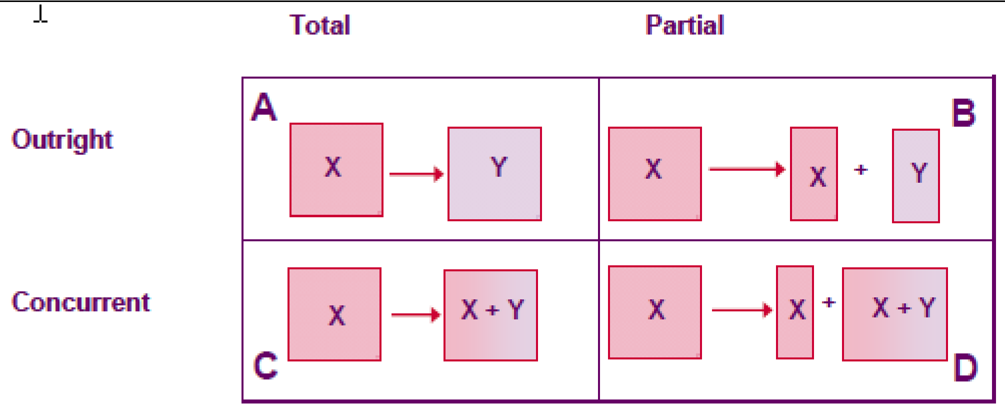
In 1989 New Zealand became the first country to introduce a property rights approach to spectrum by establishing a management rights regime, mainly for cellular and data line services. The radio licensing regime remained a 'command and control' system but spectrum mangers were given the right to privately negotiate between themselves trades in spectrum. The trades had to be centrally registered. In the US, the FCC has been experimenting with "flexible licences" since the 1990s.

Markets thrive upon liquidity and volume which means spectrum trading has been most successful in public land mobile networks. Trades can take different forms. They can be geographical:



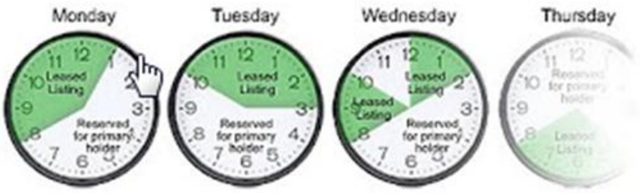
http://spectrumbridge.blogspot.sg/2010/02/new-spectrum-solutions-allowed-by-fccs.html

They can be outright transfers or leases or shared arrangements:



http://stakeholders.ofcom.org.uk/binaries/consultations/simplify/statement/statement.pdf

The sharing could be a simultaneous joint use of network resources, for example an MVNO, or time-sharing:



http://spectrumbridge.blogspot.sg/2010/02/new-spectrum-solutions-allowed-by-fccs.html

Countries that are encouraging trading include Australia, New Zealand, Canada, US, Guatemala and El Salvador. All of the EU member states and Norway are required to enable spectrum trading under the Common Regulatory Framework (CRF). In Asia, Hong Kong is considering it, and India’s 12th Five-Year Plan (2012-17) also includes a provision for spectrum trading but there is a debate as to whether the market is mature enough.

Globally, trading has been rather slow to take off. For example, in Australia where trading has been encouraged, between 1998-2009 on average less than 8% of licences to use spectrum were traded annually. There are a number of possible reasons. Initial assignments may have proven relatively efficient, or the incentives to hoard under-used spectrum may outweigh the gains from selling or leasing it, or possibly the transaction costs of engaging in secondary markets are be too high or there is insufficient access to information about spectrum for sale. The need to examine the reasons and look at new ways to facilitate trading is stated in the FCC’s 2010 National Broadband Plan.[37]

If spectrum trading is assigned by market forces, then an even more radical approach is spectrum liberalization or allocation by market forces. Liberalization means an operator who

[37] http://www.broadband.gov/download-plan/ chpt 5, p.15

buys spectrum on a secondary market can change its use, for example, from BWA to digital TV. This may undermine harmonization of allocation across country borders and disrupt roaming services. The GSMA defines liberalization in a slightly narrower sense, as applying when different technologies are used to provide cellular mobile services in different frequency bands, such as "UMTS or HSPA could be deployed in spectrum bands where traditionally GSM, CDMA or TDMA has been used."[38] The main issue is radio interference that may require masking controls over emissions or protection for receivers. This interpretation of liberalization is virtually equivalent to a technology neutral approach.

In practical terms a hybrid approach is being tried. In the EU a *Radio Spectrum Policy Programme* was agreed by the European Parliament in 2012[39] which requires all Member States within five years to allocate at least 1200MHz of spectrum to mobile services and to create harmonized bands within which liberalization in the use of technologies and the services offered can flourish. So, for example, advanced high-speed Internet mobile services can be offered in the same bands as first-generation IP mobile network services.

Over time it may well be that intelligent systems using SDR, CR and spectrum hopping techniques will overcome many of the problems of radio interference and the boundaries of liberalization will spread across a wider range of bands. For unlicensed spectrum, liberalization is already a reality since anyone can use the spectrum for any innovative idea that they come up with. The white spaces example above is a case in point.

3.3.3 Allocation and Assignment

The upcoming challenge facing all telecom regulators is the need to ensure sufficient spectrum for the exponential growth in demand for BWA services. An important part of the supply-issue will be to provide BWA to rural and remote areas where the costs of service provision may not be covered by customer revenues. The first part of the problem will be to find ways to increase the spectrum available. The second part will be to consider ways in which more flexible licensing of services to under-served areas can help in meeting demand.

Finding sufficient spectrum is an allocation issue. Following the recommendations of the WRC is the first step towards providing BWA either as UMTS 3G services or IMTS-Advanced 4G services for two reasons. First, by adopting international and regional spectrum standards the cost of procuring network equipment and mobile devices is lowered. Second, it promotes mobile roaming services. The work of the ITU and other regional bodies in promoting cross-country harmonization of spectrum allocations is referenced in Module 3.3 above.

[38] http://www.gsma.com/spectrum/band-overview/liberalisation

[39] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:081:0007:0017:EN:PDF

Finding the spectrum will possibly involve re-farming spectrum from earlier uses. For example, as 2G mobile services run down so frequencies can be re-allocated to 3G or even to 4G services. This is what the GSMA refers to as liberalization as discussed in Module 3.3.2. It may also involve reallocation of spectrum freed up by the digital dividend, also discussed in Module 3.3.2.

It is also possible to reassign frequencies from under-used to in-demand services. The regulator can seek ways to encourage public and private entities such as utility companies, the armed forces and emergency services, government agencies, etc., to yield up some of their frequencies. One way is by a 'command and control' method, but this can be a blunt instrument leading to disputes over how to audit the efficient use of spectrum. Another way is to introduce some form of spectrum pricing which may encourage cost savings and the return of unused frequencies. In the US, the FCC is advancing a third way, which is an 'incentive auction' as described in Module 3.3.

the FCC in 2013 is experimenting with a third way which is an 'incentive auction' as described in Module 3.3.

A policy to bridge the digital divide and support universal BWA to people in rural and remote areas is taking universal access to the next level, a level appropriate to next generation ICTs. This is where the argument for allocating part of the digital dividend in the UHF 700MHz band becomes compelling. The propagation qualities of this band are ideally suited to providing wide-area coverage over more sparsely populated regions of a country. When accompanied by other measures, such as the liberal use of unlicensed spectrum for local initiatives such as super WiFi and with licence conditions that encourage the sharing of infrastructure and of spectrum, a new momentum towards interconnectedness can be created.

Assignment by Auction

Spectrum auctions are now a well-established part of the regulators' toolkit. By the end of 2012, the only continent that had not organized an auction was Africa, although Ghana, Nigeria and South Africa each had plans to do so.[40] In South America, auctions have either taken place, in Chile and Columbia, or are planned for BWA in most countries. In the Asia-Pacific region, Australia was the first to announce an auction in 1998 and since then more than 30 auctions have taken place or are planned in at least 9 countries. In Central Asia auctions have not yet been used. In Eastern and Western Europe the majority of countries have used auctions and plan to do so in the future.

[40] *Global Mobile Spectrum Auction Tracker* http://telecomspectrumauction.blogspot.in/2012/08/africa-spectrum-auction-overview.html

Auctions of 2G and UMTS 3G licences were confined to single bands of frequencies but with IMT-Advanced 4G standards and the growing pressure upon regulators to find additional bands and to re-farm and reassign existing frequencies, auctions are tending towards multi-band. 4G operators are also pressurizing for wider bandwidths to be made available as contiguous blocks, for example 2x25MHz, to cater for the growth of data traffic. A further complication is the demand for FDD (frequency division duplexing) and TDD (time division duplexing) in markets where the TD-LTE and WiMax standards are being used such as Brazil, in much of Asia and the US.

The danger of multi-band auctions is that some carriers may end up with stranded frequencies. There are different ways to overcome that problem. If a traditional simultaneous multiple round ascending auction (SMRA) is used, the frequencies can be arranged into contiguous bandwidths before the bidding begins. In an increasing number of cases the combinatorial clock auction (CCA) is being used, for example in Austria, Denmark, Ireland, the Netherlands, Switzerland and the UK, and as of 2013 Australia, Canada and Singapore had plans to use it . In the CCA auction one round of bidding determines how much spectrum is bid for by each contestant, and a final round determines which contiguous blocks of frequencies match those bids. The regulator makes the final decision based upon the combination that maximizes the sum of the bids, which may mean that some blocks do not go to the highest individual bidder as Table 3.1 illustrates.

Table 3.1

Hypothetical Combinatorial Clock Auction (CCA)

Bidder	**Lot A**	**Lot B**	**Lot C**	**Highest Bid**	**Highest Value**
1	10	9	8	10	9
2	9	7	8	7	9
3	7	6	9	9	9
Value				**26**	**27**

Source: Author

In this hypothetical case the regulator maximizes value (27) by assigning lot A not to the highest bidder 1 but to the second highest 2.[41]

But auctions may not always be appropriate and even where they are they require resources in terms of expertise to design and conduct the auction. For example, they are not appropriate for frequencies that are to be assigned to emergency services or essential government functions. Their outcomes are subject to many variables, including the current state of investor confidence in the economy, and unless spectrum caps are introduced or spectrum set aside for new entrants, the bidding can be dominated by powerful incumbents who may be motivated in part by hoarding. If excessive prices are bid and if subsequent

[41] http://trpc.biz/wp-content/uploads/TRPC_BriefingPaper_SpectrumPolicy_Nov2012_v2.pdf

competition in the market is not sufficiently strong higher prices can hurt consumers, either through higher tariffs or by lack of investment in infrastructure.

In theory spectrum trading should be able to correct any incorrect valuations that were bid in the auction, but trading has its own problems to resolve as seen in Module 3.3.2. In some cases, for example in Singapore, the regulator stipulates that trading will not be allowed until the bidders have met their performance targets, such as network coverage. This is to prevent speculative bidding for spectrum that the bidder has no intention of using but wants to resell later at a higher price.

As a general rule, auctions have an important part to play if the aim of policy is to ensure transparency in the assignment of frequencies to competitive companies and to achieve an efficient use of spectrum. But the resources required by the regulator to ensure that the auction itself is efficient are often in scarce supply. An easier way to ensure competitive bidding is through a 'beauty contest' which can require bidders to state their non-monetary targets such as coverage, quality and scope of services, but this does less to guarantee efficiency and may end up as a windfall for the chosen winners. The simplest procedure is through administrative assignments, which are low cost and fast but also least transparent and still leave open to dispute what the price of spectrum should be. There are therefore two parameters to consider. The first is efficient spectrum pricing which is where the market is important. The second, which is the most important of all for the industry and consumers, is competition. Getting the second one right will tend to correct over time any mistakes made in the first one.

3.3.4 Licence Renewal

Although granting licences in perpetuity is not unknown, most spectrum licences have a finite life, typically around 15 years in the case of mobile cellular licences. Many of the original 900MHz 2G cellular licences issued in the 1990s either have or are coming up for renewal, and the same will soon apply to many 1800MHz UMTS 3G licences and some in 2.1GHz. Commercial sector broadcast spectrum licences are another category where the issue of renewal often has substantial implications for investment, although whereas most of the investment in telecoms is in the network most of the investment in broadcasting is in the production and purchase of content.

A number of important issues surround the question of how to renew licences. Where the performance of an MNO has proved satisfactory there is a strong case to renew. One indicator will be the number of subscribers on the network who will be inconvenienced if they have to change their operator, their billing details and their telephone numbers. As an MNO upgrades from 2G to variants of 3G and then on to 4G, substantial investments are put at risk, and uncertainty over renewal can remove the incentive to put in more money. Legally, if the original licences stipulated that there was no guarantee of automatic renewal the regulator is probably safeguarded against appeals to the courts, but legal challenges have become part of the process. In the face of objections from incumbents, the regulator does have a legitimate responsibility to ensure a competitive market and to ensure that additional efficiencies are squeezed out of existing spectrum use and automatic renewal may not be consistent with that aim.

In many cases, for example in the US, there is a "renewal expectancy" for cellular licences subject to the fulfillment of certain targets.[42] Portugal and the UK have gone for renewal and it is the presumption in Canada. In Australia the regulator has taken the opposite view that all renewable spectrum will be auctioned. In Germany and France renewal has also been assured, but with the regulators taking back some of the spectrum for administrative reassignment to allow for new entrants and further competition. The Netherlands regulator extended the period for renewal by a few years and then committed the frequencies to auction with spectrum caps imposed to allow for new entrants. Under the EU's Common Regulatory Framework (CRF) and its recent Radio Spectrum Policy Programme (RSPP) NRAs are required to include competition policy in their policy decisions, which means NRAs must at least consider the option of reassigning spectrum to new entrants, although not necessarily by auction. In New Zealand MNOs were given the opportunity to renew some of the spectrum if they agreed the regulator's new administered incentive pricing (AIP) and if not all the spectrum would go to auction.

Box 3.5

Administered Incentive Pricing

Charging for unauctioned spectrum needs to use a form of 'shadow pricing' to mimic the market if it isn't to be completely arbitrary. The ideal way is to find a measure of what price the spectrum would be worth in the next most profitable employment, known as the 'opportunity cost'. If the AIP is significantly below that level then the incentive to use the spectrum more efficiently will be weak. One method is the Optimum Deprival Value (ODV) or 'least cost alternative' model which answers the question: if the present asset was removed what is the least cost system that could provide current level of service? Alternatively, if the MNO were denied the additional spectrum, what would be the additional cost of squeezing out the additional level of service from the existing spectrum or of adding more base stations? By awarding the additional spectrum these extra costs are avoided and therefore represent the value of the additional spectrum.

The Best Alternative Use (BAU) method measures the value other users will place upon the spectrum based upon a modeling of their likely costs and revenues. Used in combination, BAU can be used to set the price within a lower and upper range approximated by ODV.

[42] See http://www.wikinvest.com/stock/United_States_Cellular_%28USM%29/Licensing-commercial_Mobile_Radio_Service

The Hong Kong regulator adopted a hybrid approach in 2013 by offering to renew some of the spectrum and auction the rest with additional spectrum for new entrants, although this was hotly contested by the incumbents. As in Ireland and some other jurisdictions, Hong Kong also regularly imposes performance bonds when issuing new licences, related to geographical coverage within a specified timeframe, usually up to 3 years.

When mergers and acquisitions (M&A) take place, if the regulator fears that competition will be reduced it is common practice to impose conditions such as surrendering some of the spectrum of one of the operators involved. This happens in the EU and in North America. Another method of encouraging competition is to encourage the merged operators to allow MNVOs into the market, although this is usually not specified in the conditions of the licence. [See Module 3.3]

3.3.5 Unlicensed Spectrum and a Spectrum Commons

The rapid changes overtaking broadband wireless services affect both licensed and unlicensed spectrum, and a key component of this is the phenomenal rise in M2M communications. Until the Internet-of-things, unlicensed spectrum applications were mostly associated with microwave ovens, radio car keys, Bluetooth connections and various industrial uses. Now the Internet-of-things connects potentially all devices and has given rise to the concept of 'smart' as in smart cities, smartphones, smart networks, smartcards in devices, etc. What is smart? In this context it refers to the use of algorithmic-driven software applications, such as sensors and alarm systems that automatically connect alerts to command centres, electricity meters that automatically monitor *and regulate* consumption, vehicles that can be tracked-and-traced through GPS systems, public bus stops that are connected to oncoming buses to inform waiting passengers of times and routes, home appliances that can be switched on and off remotely. Some forecasts suggest *cellular* M2M connections may reach 300 million people? by 2015.[43]

In most cases these applications are used by businesses and utilities as a means of delivering a service and cutting costs and not to generate a revenue, and as such they are usually not subject to a licence. They may, however, require to be registered on a database of users if there is any likelihood of radio interference, excessive power emission or a sharing of spectrum with other users. This arises especially in the case of the white space/TV devices as discussed in Module 3.3.2

[43] http://www.berginsight.com/ReportPDF/ProductSheet/bi-globalm2m3-ps.pdf

Spectrum Commons

Unlicensed spectrum implies spectrum sharing among users. For short range devices this will not normally cause interference, but advocates of a spectrum commons argue that it is entirely possible to open up swathes of spectrum for common usage and manage the issues of interference and emission levels collectively. This view is the opposite of the view that all spectrum should be sold to property rights owners who can then own or trade spectrum as they do land according to market principles. There has been an extensive debate, especially in the US, as to what conditions may be required to make a public commons approach manageable in the future.

Box 3.6

Public Commons Conditions

Two diametrically opposed approaches to the spectrum management are the property rights or exclusive licence approach and the public commons approach. [44] They both stand in opposition to the traditional approach of 'command and control', but in practice most regulators use all three approaches for different parts of the spectrum. A paper in 2005 by William Lehr (MIT, USA) and Jon Crowcroft (Cambridge, UK) set out the following conditions that might be necessary to make the commons approach manageable:[45]

* No transmit-only devices – a receiver function provides a control loop
* Power restrictions
* Common channel signaling (and/or use of single out-of-band signaling channel)
* Congestion rules
* Rule enforcement mechanism
* Rules consistent with security and privacy

In contrast to the property rights approach, which is governed by market principles such as secondary trading, the commons approach needs to be governed by protocols or an etiquette. If the protocol fails this gives rise to selfish behaviour and an inefficient use of spectrum or what has been called the 'Tragedy of the Commons'. Advocates of the commons approach point to the emergence of new technologies such as UWB, spread spectrum techniques, mesh networks, smart antennae, MIMO, CR and SDR which offer intelligent networking (including 'ad hoc' and PAN networks) and dynamic frequency

[44] Two names that are famously associated with these opposing approaches are economist, the late Ronald H. Coase (University of Chicago) who advocated property-rights and Lawrence Lessig (Harvard University) who advocates a spectrum commons. See Coase (1959) 'The Federal Communications Commission' Journal of Literature and Economics, and Lessig (2001) *The Future of Ideas: http://www.the-future-of-ideas.com/download/*

[45] "Managing Access to a Spectrum Commons," with Jon Crowcroft, paper prepared for IEEE DySPAN Conference, Baltimore, MD, November 2005: http://people.csail.mit.edu/wlehr/Lehr-Papers_files/Lehr%20Role%20Unlicensed%20in%20Spectrum%20Reform.pdf

selection, and suggest that regulation could be ultimately distilled down to a minimum of certifying the conformity of equipment standards. Writing from the property rights perspective, a paper in 2007 by Jerry Brito (George Mason University, US) on the contrary reiterates the views of Ronald Coase that because the regulator has no direct knowledge of market costs and revenues there will be no incentive for the regulator to provide the same level of rule-making and rule-enforcement that private owners would undertake between themselves.[46]

Regulators need practical approaches that are suitable for different bands of spectrum. What is important is that regulators are fully conversant with the options that are available to them.

Unlicensed Spectrum for Underserved Areas

Besides the issues of interference and spectrum sharing, unlicensed spectrum has a role to play in addressing the issue of universal access in sparsely populated areas. There is often little commercial incentive for MNOs and ISPs to provide services to these areas, yet there may be community groups, NGOs, local enthusiasts and village entrepreneurs more than willing to put time, money and energy into building local networks based upon white space and other technologies. Licensing spectrum at a price may kill off these initiatives. This is another example of where regulation needs to be flexible to achieve the objectives of innovation in access and in services.

3.3.6 Re-farming and the Digital Dividend

As the previous Modules have stressed, regulators today are facing the challenges of finding new spectrum from old uses. For BWA this is assisted in part by the expiry of many 2G licences issued in the 1990s, but if these networks still service many subscribers then the opportunity to refarm the spectrum is limited. One answer to this problem has been to set trigger points, so when 2G users fall below certain numbers part of the spectrum becomes available for refarming. The refarming in this context will usually imply the incumbent is allowed to migrate users to a UMTS standard and does not imply a reassignment of the spectrum to another MNO.

By far the biggest opportunity for regulators, what has been called a once-in-a-lifetime opportunity is the digital dividend as reviewed in Module 3.3.2. In some cases as much as 150MHz or over could be available for reassignment as analogue TV switches off and digital TV switches on, but the transition period may take a decade to complete. The biggest hurdle

[46] ' The Spectrum Commons in Theory and Practice' Stanford Technology Law Review, 2007: http://stlr.stanford.edu/pdf/brito-commons.pdf

is the percentage of the population who are unable to change their TV sets to digital. Many families may not be able to afford the cost which means government has to make a decision whether to subsidize lower income groups and possibly provide assistance to broadcasters to switch over their transmission equipment. The cost of doing this would need to be weighed in the balance against the gains from auctioning swathes of 700MHz of frequencies.

Module Three: Law and Regulation for a Broadband World

3.4 IP-based Interconnection

Interconnection for Internet traffic over IP networks operates according to a different set of rules from telephony. However an increasing proportion of telephone traffic is carried over IP-enabled carrier networks. There are now many different operators offering network capacity to send, transit and terminate traffic, ranging from traditional telecom carriers to third party vendors, from Internet Access Providers (retail) to Internet Backbone Access (wholesale) carriers, from content distribution networks (CDNs) to utilities with spare capacity to wholesale. The commercial terms and ways in which interconnection is offered varies considerable. For example, carriers traditionally interconnect at network Points of Interconnection (POIs) whereas CDNs and cloud computing service companies interconnect in data centres, and Internet Access Providers at Internet Exchanges. Nevertheless, despite its origins and the fact that Internet traffic was never subject to the same regulatory regime as telecoms, certain common practices have emerged.

From its beginnings telecoms was a state-regulated industry, often part of a Post & Telecoms Department, later to be incorporated as a state-owned telecom enterprise (SOTE). Interconnection at the international level was mandated, and under ITU guidelines an accounting rate and a settlement rate system between international carriers was established. With market liberalization came competing networks and the need for interconnection. Often regulators required the incumbent to register a ROI (Reference Interconnection Offer) to ensure equal treatment among carriers. No such system has ever existed for Internet traffic.

University research funding from the US Department of Defence in the 1950s and 1960s and early trials by universities to establish a network of peering devices using IP/TCP protocol matured in the 1980s and 1990s into the first commercial services by Internet companies. These early developments connected computer networks. These were later connected indirectly using capacity from carriers to transit traffic between IT devices such as computers and terminals. As Internet services, for example e-mail, became mass market products for business users and residential customers, access was increasingly over telecom systems. The spread of the World Wide Web in the 1990s created a platform for the exchange of documents and then for the development of down-loadable and up-loadable content and applications.

The Internet had become big business, posing ever growing demands for network capacity on the telecom industry. This posed both a threat and an opportunity for carriers, and most of the dominant ISPs that emerged from the competition were subsidiaries of the carriers. Often by charging high wholesale prices to *all* ISPs, telecom companies could squeeze the profit margins of independent ISPs without breaking any equal access regulations. The market power of the carriers lies in their ownership of the backbone networks over which IP packets have to travel irrespective of the route they take, and although the use of least-cost routing will save some money, that only works if there is a competitive wholesale market.

ICAIS (International Charging Arrangements for Internet Services)

It is slightly ironic that the big dispute over IP interconnection that arose in the 1990s, and which still echoes to this day, for example, it resurfaced at the 2012 ITU WCIT-12 in Dubai, was not between ISPs and telecom companies as such but largely between the telecom companies that own most of the ISPs. Overlaying the dispute was the fact that the Internet originated in the USA. In 1995, the US government decommissioned the US National Science Foundation Network (NSFNET) which had been the backbone for most IP traffic in the US and handed over interconnection to four Network Access Points (NAPs). Since then other entities have arisen, some serving academia as education and research networks, others commercial networks including specialist Internet Backbone Access providers. Academia peering arrangements are not difficult to agree, but for commercial service providers peering arrangements are all about market power. The basic rule is that smaller ISPs either cannot peer with larger ISPs in which case they have to find ways to aggregate their traffic to reach critical mass, or reach special agreements with carriers, or pay premium rates for interconnection.

Internationally the same rules apply, but the larger ISPs have for historical reasons been in the USA, and later to a lesser extent in Europe. There is no accounting rate or settlement rate procedure for ISPs and the *de facto* position is that the major US carriers have always been free to charge the full cost of the international links to ISPs outside the US. In the 1990s there were intense arguments between carriers and even between states over this apparent inequality. For example, in 2000 Telstra's Managing Director of Global Wholesale Business claimed that up to "70% of an Australian ISP's costs are due to the international segment to the US." [47] In reality the issue is an old one: regulated rates versus market rates.

The way markets work is that imbalances between supply and demand will be reflected in prices, and high prices should act as an incentive to remove the supply bottlenecks. In this case the bottleneck was outside the USA where domestic IP traffic, in the absence of a local Internet Exchange Point (IXP), had no option but to route through the US. To justify the expense of a local IXP there needs be a critical volume of IP traffic. All markets thrive on liquidity, and in this case the liquidity in the Internet market means traffic volume. Unless there are structural impediments to the growth of local Internet traffic, such as a monopoly provider, the market mechanism should result in more local IXPs. This should result in more balanced flows of international traffic which in turn should allow more ISPs to enter into

[47] Stewart Taggart, 'Fed Up Down Under', *The Industry Standard* No. 5, 260 (Feb. 14, 2000)

peering arrangements with their US and European corresponding networks. The spread of IXPs seems to be exactly what is happening as explored in section 3.4.1.

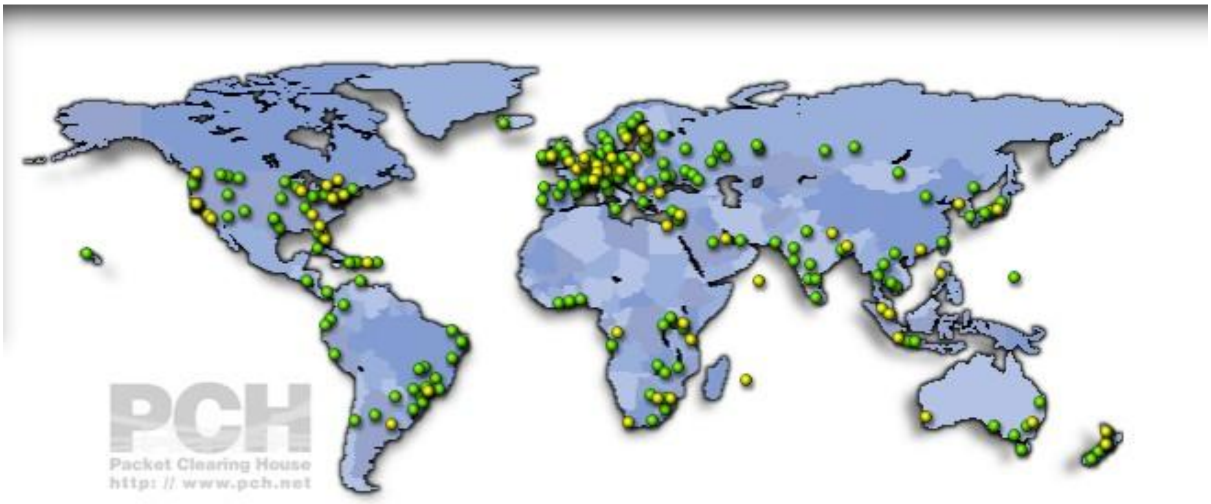
3.4.1 Internet Interconnection and IXPs in Developing Countries

To be cost-effective, interconnection between circuit-switched TDM (Time-Division Multiplexing) telecom networks requires points of interconnection (POI) that minimise route distances. For price arbitrage reasons service providers may choose a more round-about routing of traffic, but technically the more direct the routing the more efficient it is and the less latency involved. In a packet-switched world of Internet Protocol (IP), a different set of principles operate. Because different packets of the same transmission are routed over different networks there is no single POI. ISPs do not always own their own networks and there is no guarantee of the quality of the networks over which the packets will route. So unless the network was 'managed' and its quality assured, Internet traffic from its earliest days was only 'best effort'. Investment in broadband in recent years means network quality has generally improved and with more sophisticated routing algorithms 'best effort' is now often of very high quality. For example, over-the-top (OTT) voice and video services like Skype and Yahoo Messenger, Facebook and Google that are transmitted internationally over broadband networks can be crystal clear with minimal latency. In addition, a range of specialist managed Internet networks have arisen such as CDNs that guarantee quality of delivery.

ISPs come in three tiers: Tier One ISPs are usually affiliated with a licensed carrier having direct access to an international network, although some of the larger Internet-based companies have begun to build their own networks. For example, Google is ranked third in the carriage of global traffic behind Level 3 and Global Crossing. Tier Two ISPs own or have direct access to local networks and may serve a regional market but require IP transit for international routing. Tier Three carriers have to lease lines and peer with larger ISPs, in some cases as paid peering, to achieve end-to-end delivery of traffic or IP transit. The larger ISPs also provide the connecting networks for IP transit which are known as Autonomous Systems (AS) and are assigned an Autonomous System Number (ASN). The ASN identifies them as using the appropriate routing protocol for IP transit traffic, also known as the Border Gateway Protocol (BGP). When using IP transit, ISPs provide and receive from each other routings to facilitate traffic to and from the customers of the ISPs involved.

Unless the ISP is affiliated to a licenced carrier there is no guarantee of interconnection. Large carriers such as incumbents may reject interconnection with smaller providers for commercial reasons, not technical or regulatory reasons. Alternatively they may impose draconian interconnection charges or high prices for leased lines resulting in profits squeeze of independent ISPs. The lack of domestic interconnection forces ISPs to route their domestic traffic through Internet Exchange Points (IXPs) or to pay for peering to send traffic overseas. Their traffic becomes transit IP traffic which they have to 'trombone', that is send over several different networks before it reaches its destination. Naturally, this adds to its cost and to the latency problem.

Figure 3.5
Map of Active IXP



Source: https://prefix.pch.net/applications/ixpdir/

In the 1990s, IXPs were typically in the US and it is still the case that many countries route much of their domestic traffic through the US. According to Packet Clearing House (PCH), as of May 2013, about half of the world's 199 countries are without IXPs'[48] By contrast, only four European countries are without IXPs, while in Asia Pacific the countries without IXPs are largely Pacific Islands. Most South American countries have IXPs, but there are fewer in Central America and the Caribbean islands. "At present only the British Virgin Islands, Haiti, Grenada, St Maarten, Curacao and Dominica have IXPs. In conjunction with the Caribbean Telecommunications Union, PCH is currently assisting several other Caribbean countries, including Barbados, Jamaica and St Kitts and Nevis in establishing local IXPs." (See Toolkit *Broadband in St Kitts and Nevis: Case Study*.) Mexico is the only OECD member country not to have an IXP.[49] In Africa there are upwards of 20 or more countries with IXPs, but most are small and serve only very localized markets.[50] According to one source, 85% of Africa's

[48] Packet Clearing House Report 2nd May 2013 see https://prefix.pch.net/applications/ixpdir/summary/

[49] OECD (2013) 'Broadband Networks and Open Access' OECD *Digital Economy Papers* No.218 http://www.oecd-ilibrary.org/science-and-technology/broadband-networks-and-open-access_5k49qgz7crmr-en

[50] Not all ISPs participate in local IXPs, for example only 5 of the 9 ISPs in Rwanda connect to RINEX – see http://www.rura.gov.rw/docs/Rwand_IXP_Positives_Steps.pdf

traffic routes through Europe and only 1% stays within the region.[51] South Africa is the major hub, but at least 16 East African and Southern African countries also use the KIXP in Kenya. (See Box 3.7 and also the Toolkit *Broadband in Kenya Case Study*.) One report also suggests that Nigeria's IXPN is preparing to provide peering for West African countries.[52] In North Africa and the Middle East, Egypt has three IXPs in Cairo, and others countries with IXPs include Lebanon, Israel, the United Arab Emirates (UAE), and a state-run IXP in Saudi Arabia. However, the region remains under-served as does Central Asia where, as of the first half of 2013, only Kazakhstan, Mongolia and Uzbekistan had established IXPs.[53]

Box 3.7

The Success of IXPs in Kenya

Kenya has two IXPs: the first , known as Kenya IXP (KIXP), opened in Nairobi in 2000 and the second in Mombasa in 2010. They were set up with the assistance aid from CISCO and UNESCO, and are operated by the Telecommunications Service Providers Association of Kenya (TESPOK) which is a non-profit organization representing ISPs and telecom service providers.[54] KIXP operates a Multi-Lateral Peering Agreement (MLPA) whereby ISPs are required to interconnect free of charge, but each pays a usage fee to KIXP.

The success of these IXPs is in evidence from a number of measures. By April 2013, membership of KIXP had reached 30, up from 25 in April 2012 and included the mobile and fixed line operators, an educational network called KENET, the National Bank of Kenya, and government agencies such as the Kenyan Revenue Authority (KRA). Aggregate traffic throughput has jumped from 64kbit/s at opening in 2000 to over 1Gbit/s today. One estimate of the cost savings to Kenyan ISPs from not having to pay the cost of international transit and trombone is $1.44 million per year.[55] ISPs from other African countries are starting to use Kenya's IXPs; 56% of the ASNs routed through KIXP in the six months to January 2012 were from 16 foreign countries.

Cache and the Digital Economy

The most important step up in usage came after the installation of a Google Global Cache (GGC) in April 2011. Traffic volumes rose more than ten-fold within the year, the lion's

[51] Tim Kelly and Carlo Maria Rossotto (2012) *Broadband Strategies Handbook* World Bank, Korean Trust Fund, *Info*Dev, p.106 http://www.infodev.org/En/Publication.1118.html

[52] AnalysysMason (2012) 'Assessment of the Impact of Internet Exchange Points – empirical study of Kenya and Nigeria' Report for the Internet Society http://www.internetsociety.org/ixpimpact

[53] Wikipedia lists some countries not listed by Packet Clearing House, see http://en.wikipedia.org/wiki/List_of_Internet_exchange_points#Middle_East

[54] http://www.tespok.co.ke/index.php/aboutus/members.html

[55] Based upon an estimated $120 per Mbit/s for international transit. See Analysysmason/Internet Society (April 2012) 'Assessment of the impact of internet Exchange Points – empirical study of Kenya and Nigeria' http://www.internetsociety.org/ixpimpact

portion of it was streamed video, for example from YouTube, as latency dropped by 20% on top of the initial fall in latency when the KIXP was first opened from 1,200-2,000 milliseconds (via satellite) to 60-80 milliseconds. [56] The caching capability builds a foundation for local content generation and distribution at affordable prices. Improved latency also bolsters the IXPs capability to become the driver of growth in cloud computing in Kenya.

Conditions for Success

Despite the success of KIPX, it almost faltered in 2000 when it had to close business pending a decision by the Communications Commission of Kenya (CCK) to grant a licence to operate a telecommunication service. This followed a complaint by Telkom Kenya that its monopoly over international traffic was being violated.[57] KIPX argued it only directly handled domestic traffic (see the Toolkit Kenya Case Study) and the decision to grant a licence has served Kenya well.

3.4.2 The Economics of IXPs and Wholesale Charging

Having to trombone traffic adds to cost and to latency, from between 200 to 900 milliseconds in the case of African ISPs.[58] In the early years the cost factor was the most important consideration for two reasons. Firstly, the cost of international circuits was high and US carriers in particular required overseas ISPs to pay for the full cost of the circuits. By contrast, among carriers transmitting telecom traffic, including packet data such as frame relay, the ITU-approved accounting rate system was used in splitting the costs 50:50 between transmitting and receiving carriers. The settlement rate system could vary the split ratio in certain cases; for example the split between Hong Kong and Mainland China before Hong Kong returned to Chinese sovereignty in 1997 favoured the Mainland. However, Internet traffic never became part of the accounting rate system, and in the US for regulatory purposes the Internet was defined as an information service rather than a telecommunications service.

The second reason is that in the early years the main Internet service was email for which latency is less of a problem. By contrast, a service such as search is highly sensitive to delays. A study in 2009 found that a two second delay on Microsoft's Bing search engine caused the

[56] Google, cited Analysysmason (2011) 'Overview of recent changes in the IP interconnection ecosystem' pp.35-40 http://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/Indonesia-12/pdf/Session5_Kende_IXP.pdf

[57] Tim Kelly and Carlo Maria Rossotto (2012) *Broadband Strategies Handbook* World Bank, Korean Trust Fund, *Info*Dev, p.106 http://www.infodev.org/En/Publication.1118.html

[58] Tim Kelly and Carlo Maria Rossotto (2012) *Broadband Strategies Handbook* World Bank, Korean Trust Fund, *Info*Dev, p.106 http://www.infodev.org/En/Publication.1118.html

number of queries to drop by 1.8% and revenue by 4.3%, and a 400 millisecond slowdown caused a fall of 0.59% of queries through Google.[59]

Since the collapse of the dot.com bubble in 2000, international circuit costs in submarine cables have dropped to a fraction of their former price, a trend that was reinforced as cable capacity soared following the recovery in financial markets in the mid-2000s. The trend was uneven. In some regions both cable capacity and satellite services remain limited and costs relatively high, such as in the Pacific Islands; in other regions the changes are more recent, as in Africa where new cables are now coming online.[60] Reduced international prices have had a major impact upon the cost of Internet traffic. An OECD assessment of the voice-equivalent cost of Internet transit traffic in 2013 is "USD 0.0000008 per minute – five orders of magnitude lower than typical voice rates."[61] However, as the report also points out, local access charges levied by telecom companies consistently seem to account for between 30%-40% of total international transit costs.[62]

At the same time, Internet businesses have undergone a complete transformation to create a digital economy, everything from search to e-commerce, from social media to e-Government, from online video content to online gaming. In 2011, it was estimated that the Internet-based digital economy contributed 3-4% GDP to the G-8 nations plus Brazil, China, India, South Korea and Sweden.[63]

If a flourishing local Internet can generate so much local economic activity and contribute so much to social welfare, for policy-makers and regulators these statistics are just too important to be ignored. The danger is that smaller ISPs can be easily hindered from reinvesting in their business due to high wholesale prices and profits squeeze and the local Internet economy will suffer. There may be a need for regulatory intervention if wholesale charges are clearly discriminatory against ISPs not affiliated to the telco. However, this can be a difficult policy to pursue because a telco may also squeeze its own ISP so that downstream margins are sacrificed to maintain upstream margins and market dominance. In fact most IXPs have not come about through regulatory intervention but by voluntarily market agreements.

[59] See: http://perspectives.mvdirona.com/2009/10/31/TheCostOfLatency.aspx, cited in Analysysmason (2012) 'Assessment of the Impact of Internet Exchange Points – empirical study of Kenya and Nigeria' Report for the Internet Society fn. 8. http://www.internetsociety.org/ixpimpact

[60] The The *Eastern Africa* Submarine *Cable* System (EASSy) for example now links South Africa with landing stations all the way up the East coast of Africa.

[61] OECD (2013)) 'Internet Traffic Exchange' OECD Digital Economy Papers No.207 http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826

[62] Before NGN developments in recent years, it was a common observation within the industry that local loop costs always seemed to average out at around $1,500.

[63] McKinsey Global Institute (2011) Internet Matters: The Net's sweeping impact on growth, jobs and prosperity' http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters

In some cases the state itself establishes an IXP, which can be motivated by the need to address market failure, but the motives could be more political. Much more often IXPs are established either as non-profit entities, sometimes by universities or NGOs or associations of ISPs, or as commercial businesses. Most IXPs in the US are commercial, most in Europe, Latin America and Africa are non-profit and there is more of a mix in Asia. For example most commercial IXPs are in Australia, China (including Hong Kong), Japan and Singapore and non-profit IXPs are mostly in India, Nepal and the Philippines.

The commercial IXPs usually co-locate ISPs in data centres, with various charging schemes including charging for ports or capacity usage, rack space, connection fees and/or a range of management and security services. They can be carrier-related or carrier-neutral, co-location neutral or ISP-specific. The non-profit IXPs are usually dedicated operations which only charge cost-recovery fees and facilitate peering between members, likely to be at no charge between ISPs, although in some cases it can be paid peering if the balance of traffic is too one-sided. A study by the OECD covering 86% of the world's Internet carriers in 96 countries found that 99.51% of peering agreements were made by "handshake".[64] Peering arrangements can be single-hop, bilateral or multilateral, and occasionally the latter can be a condition of joining an IXP, as it is to join Kenya's KIXP or in Chile where peering is mandatory.[65]

What is common to all of these arrangements is that, even where peering is mandatory, the terms and conditions are not. Regulators have seen the advantages in leaving developments to voluntary agreements between ISPs and other parts of the Internet ecosystem such as CDNs, major content producers, Internet search and social media companies, OTT service providers, etc. The over-riding reason why this has been the right way to do things is because these are all fast-moving and rapidly developing businesses with a need to innovate and experiment with what works best for them. Regulation that addresses market failure might justify mandatory peering if there is a real fear that the ISP attached to the incumbent can prevent new entrants from entering the market. There is little evidence to suggest that discrimination is sustainable as substitutes emerge for network connectivity and Internet access and for the delivery of apps and content. These substitutes include mobile networks, satellite networks, CDNs, WiFi networks, IP 'connected' TVs, etc. In a developing country where these substitutes may still be in a nascent stage, market failure could be a barrier to growth in the digital economy; the work-around market failure is to reform regulations to facilitate new entrants into the Internet ecosystem.

[64] OECD (2013)) 'Internet Traffic Exchange' OECD *Digital Economy Papers* No.207 p.9 http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826

[65] Internet Society (2007) *Report from the IGF Rio -Best Practices Session: Internet Traffic Exchange in Less Developed Internet Markets and the Role of Internet Exchange Points* p.9 http://www.cabase.org.ar/backend/upload/File/igf-ixp-report-2007.pdf

3.4.3 Future Charging Arrangements and Developments of IXPs

When Internet companies such as Yahoo! and Google and major content distribution networks (CDNs) such as Akamai, Amazon and Limelight invest in a local server to cache content from overseas the stimulus to the local IXPs is immediate.[66] This is especially significant for developing countries where international connectivity remains a problem, because a cache connected to an IXP reduces latency and thereby encourages local demand and usage. In the example from Kenya (see Box 3.7) following the installation of a Google Global Cache in April 2011 traffic at the KIXP rose from just over 100 Megabits every second to well over 1 Gigabits every second in just over two months, most of this accounted for by YouTube downloads.[67] This in turn can create a market and act as a stimulus to local developers of apps for entertainment and for practical use, such as financial and locational apps for use on mobile phones, and to producers of content. In this way a digital economy gets built up.

As the digital economy grows, so will the number and type of parties connecting to IXPs. In Europe between 2008 and 2010 the percentage of connections to IXPs from content providers increased from 85% to 96.3%, by VoIP providers from 36.8% to 48.1%, by enterprises such as airlines and banks from 30% to 46.2%, by search engines from 25% to 48% and by governments from 50% to 77.8%.[68] For developing countries, these are trends to take note of as IXPs have an important role in triggering and accelerating the local digital economy.

P2P, OTT and Cloud

While peering or P2P delivery of Internet traffic was the major growth trend of the late 1990s, it has been overtaken by direct download of apps and video content which comes OTT of the fixed and public land mobile networks (PLMNS). A particularly important part of this development is the growing use of cloud computing. Many email servers, for example, are now based in the cloud where emails are stored and retrieved by users instead of being downloaded and stored in computer hard drives. Cloud computing has given rise to a whole new generation of cloud-based services, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Application-as-a-Service (AaaS) and even Infrastructure-as-a-Service (IaaS). Specialist cloud service providers have joined CDNs, content creators, application service providers and others in locating in an ever increasing numbers of data centres and countries

[66] A study by Atlas Internet Observatory in 2009 found that the top five 'pure play' CDNs accounted for nearly 10% of Internet traffic – see Labovitz, et al, Atlas Internet Observatory, *2009 Annual Report* p.15 at *www.nanog.org/meetings/nanog47/presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf*.

[67] AnalysysMason (2012) 'Assessment of the Impact of Internet Exchange Points – empirical study of Kenya and Nigeria' Report for the Internet Society http://www.internetsociety.org/ixpimpact

[68] Stephanie Silvius (2011)' Internet Exchange Points: A closer look at the differences between continental Europe and the Rest of the world.' https://www.euro-ix.net/documents/894-ixp-research-pdf?download=yes

now directly compete with each other to host these data centres. Countries with reliable broadband infrastructures and appropriate personal privacy and data protection laws in place to safeguard the international transfer of commercially sensitive data between jurisdictions have a competitive advantage.

Charging in an NGN Internet World

More of all of these services are being accessed by mobile wireless devices such as smartphones and tablet computers over PLMNS and WiFi networks. These trends have important implications for the business models of the traditional telecom providers; their pricing models in particular are being redesigned. The idea of charging by-the-second or by-the-minute of usage does not work in an Internet world. Charging by capacity makes more sense and as voice traffic declines as a revenue earner, and as OTT substitutes such as social media chat services and texting become ever more popular, telecom companies are moving towards bundled voice and data services. Bundles are frequently offered at flat rate charges, sometimes with tiered flat rates: each tier with its own capacity ceiling.

The old model of charging termination fees to networks for the delivery of their traffic also comes into question in an Internet environment, for two reasons. First, because there are now many ways for users to access the Internet. Second, as networks upgrade to broadband, telecom companies may be tempted to charge both sides of the market—the providers of services over the Internet and the users—in what is called a ‘two-sided market’. This goes the nub of the net neutrality issue. (See Module 3.7)

In practice most carriers, fixed line and mobile wireless, will make the transition cautiously, not wanting to cannibalise their existing lines of business, such as call services, too early as long as they continue to generate revenues. But as they invest more in all-IP NGNs their billing arrangements are likely to come closer to the charging mechanisms between ISPs, which are mostly Sender-Keeps-All (SKA) – also called Bill-and-Keep (BAK). Where interconnection charges are levied, for example where the balance of traffic is very uneven, it is likely to be capacity-based charging as the marginal costs of sending a packet are very close to zero.

3.5 Regulation versus investment debate

There are at least two reasons why regulators and policy makers are concerned about the source of investment necessary for broadband: universal access is needed to close the digital divide, and broadband is crucial to a digital economy. These two concepts combine into the over-arching concept of *inclusive* economic and social growth.

There are four primary sources of investment funds. First, network investment by the incumbents; second, by new entrants including domestic and foreign service providers; third, public funding; and fourth, by financial investors using leveraged buyouts of poorly performing companies by venture capitalists. It is usual to view telecoms markets according to geographical segments, namely the local loop, the metropolitan area, national long distance and international. But a service-based typology might instead look at 'basic' fixed and mobile voice and text-related services, broadband and Internet related services, content and broadcast services such as IPTV, and enterprise managed network services.

Box 3.8

Broadband in Japan

During the time when Japan was working towards achieving its national target of eliminating all broadband zero areas (= make broadband service available to all the households nationwide) by the end of FY2010 (March 2011),[69] the five types of role-sharing between private and public sectors were identified, based on builders and operators of broadband facilities.

Type 1: Broadband facility is built and operated by the private sector. Since broadband should be deployed on a commercial basis in principle, this type 1 is the correct basic model.

Type 2: This type 2 is the same as type 1 in that both building and operation are conducted by the private sector. There may be some areas where the operator is not sure if there exits enough demand and thus cannot make the business decision to start broadband service in the area. In this situation, neighborhood communities or local governments can prepare a list of potential broadband service subscribers and hand this over to the operator.

[69] The national target was set in both (1) the New IT Reform Strategy, which was formed 2006 by IT Strategic Headquarters (headed by the Prime Minister) and (2) the Digital Divide Elimination Strategy, which was formed in 2008 by the Ministry of Internal Affairs.

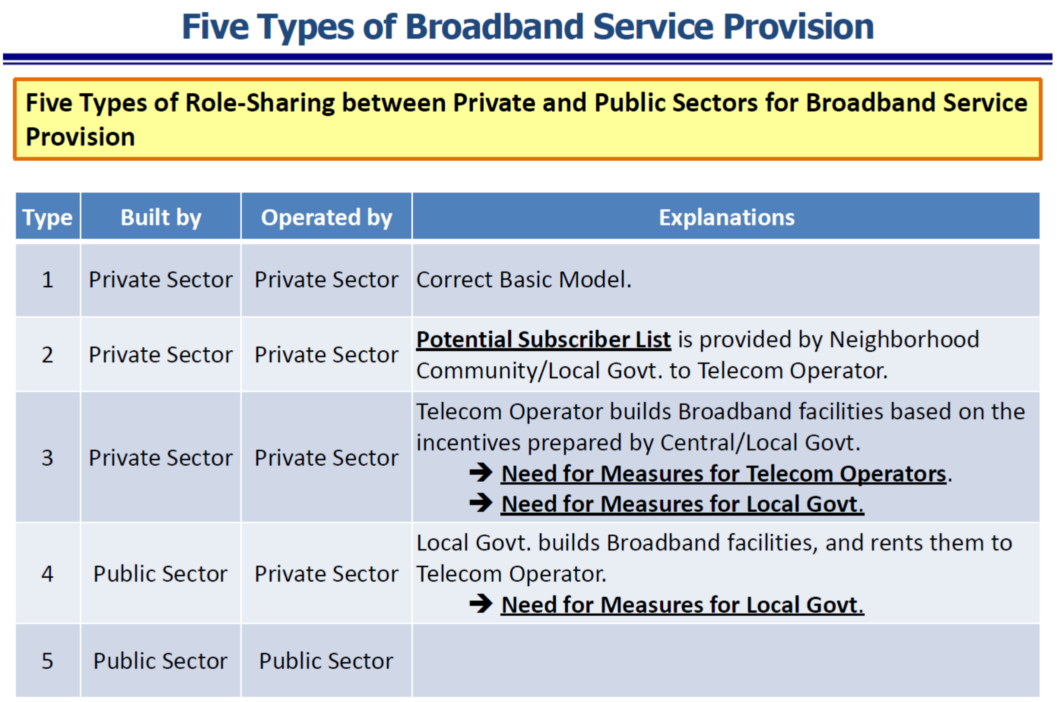
Type 3: This type 3 is also the same as type 1 in that both building and operation are conducted by the private sector. However, central or local government partially subsidizes the broadband facilities installation cost and this makes much easier for the operator to start broadband service.

Type 4: Local government builds broadband facilities, then a telecommunications operator provides broadband service. This means that the operator does not have to prepare initial investment of broadband facility. In many cases, local government rents the facilities to the operator on IRU contract (see page 51). Under the typical IRU, the operator can use the facility for 10 years for free of charge, but it has to provide the service for the period and maintain the facility at its expense.

Type 5: Local government builds broadband facilities and operates them.

In order to eliminate Broadband Zero Areas, Type 3 and Type 4 were important and the Government of Japan prepared several promotion schemes, which included grants/subsidies for local governments and interest aid, debt guarantees and tax breaks for telecom operators.

Figure 3.6



Five Types of Broadband Service Provision

Five Types of Role-Sharing between Private and Public Sectors for Broadband Service Provision

Type	Built by	Operated by	Explanations
1	Private Sector	Private Sector	Correct Basic Model.
2	Private Sector	Private Sector	**Potential Subscriber List** is provided by Neighborhood Community/Local Govt. to Telecom Operator.
3	Private Sector	Private Sector	Telecom Operator builds Broadband facilities based on the incentives prepared by Central/Local Govt. ➔ **Need for Measures for Telecom Operators**. ➔ **Need for Measures for Local Govt.**
4	Public Sector	Private Sector	Local Govt. builds Broadband facilities, and rents them to Telecom Operator. ➔ **Need for Measures for Local Govt.**
5	Public Sector	Public Sector	

Source: http://www.itu.int/ITU-D/asp/CMS/Events/2010/ITU-MIC/S5-06_Mr_Atsushi_Ozu.pdf

3.5.1 Local, National and international Networks

The Local Loop

The major costs of building an extension to the traditional local loop arise less from the cost of the equipment and more from having to seek planning permission and the labour costs of road digging, ducting, wiring and cabling, installing distribution cabinets outside buildings and main distribution frames (MDFs) in the telecom rooms of multi-tenanted buildings. The local loop is therefore not easy to replicate using traditional methods, and for this reason regulators should examine ways to reduce the costs. Measures can include infrastructure sharing, simplify the procedures and lower the cost of issuing of permissions, review regulations governing rights of way and access to buildings.

Over recent years, subscribers have been signing up in larger numbers to networks using broadband wireless known as fixed-wireless access (FWA) for the house and office telephone. FWA offers a means for non-fixed line service providers to enter the local market. Another technology standard that has been used in some markets, Indonesia and Malaysia for example, to provide fixed-wireless broadband access is WiMax.

The most compelling competition for local loop providers has come from mobile network operators (MNOs) and the rapid deployment of 2.5G and 3G networks has spread broadband wireless access (BWA) to many metropolitan, smaller urban areas and many rural areas in most countries. As a result, in the world today there are many more mobile users than fixed line subscribers. This has changed the local landscape for regulation. When the fixed line phone was of paramount importance, regulators were faced with a choice of either supporting the continuation of a monopoly by the incumbent operator or unbundling the local loop. Unbundling was incorporated into the laws and regulations of the US, most of Europe, Australia and India among others. It is done by mandating the right of a new entrant to connect to the incumbent's local access network at one of three places: at the roadside distribution point or MDF, on the customer-side of the MDF in the incumbent's exchange building or central office, or on the network-side of the MDF. The last of these three is called co-location and minimizes the need for the new entrant to build their own local access network.

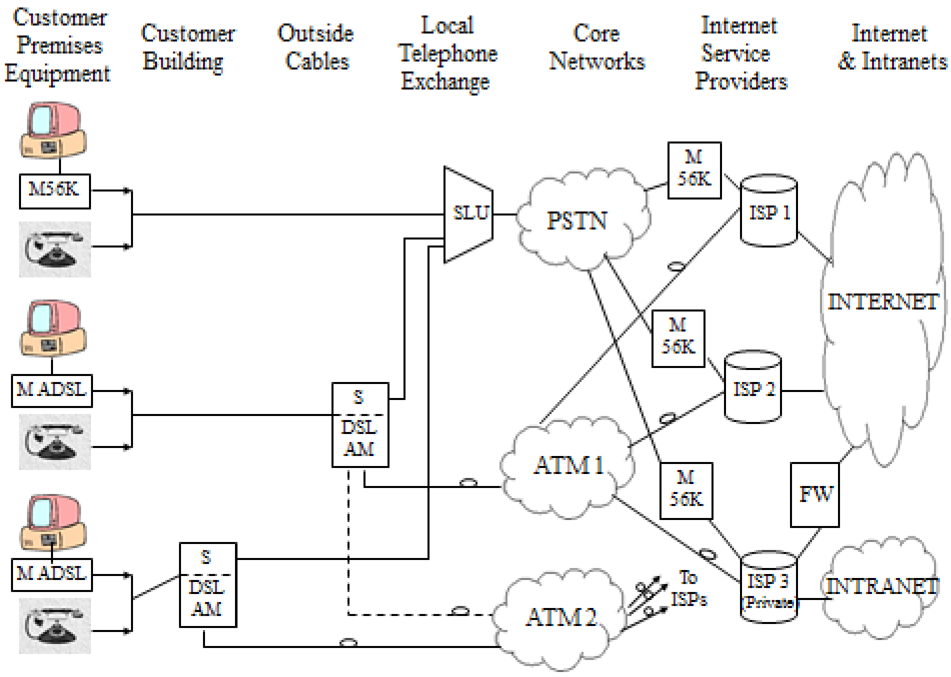
Unbundling is always a hotly contested issue because unlike other forms of interconnection, it involves the incumbent surrendering the use of its own lines to a competitor. There is less controversy when the facility to be unbundled is an essential 'unbundled network element' (UNE)[70] such as a bottleneck facility or an essential service, such as a numbers registry. The

[70] Defined in the Telecommunications Act of 1996 of the USA

advantage of local loop unbundling is that it gives the new entrant an immediate footing in the market, but achieving long-term competition on a sustainable basis may require the new entrant to invest in their own network. One way to encourage this is to place a sunset clause on unbundling after which local loop interconnection becomes unregulated and subject to commercial agreement. This was done successfully in Hong Kong.

Figure 3.7 illustrates pre-NGN architectural and commercial options for local loop unbundling. The first horizontal illustration shows a circuit from the customer to a subscriber line unit (SLU) which identifies the call as either voice or data, routing the first through the switched network and the latter to an Internet service provider (ISP1, ISP2 or ISP3 in the Figure) and out into the public Internet, or possibly via ISP3 to a private Intranet. In the second scenario, the new entrant has collocated their digital subscriber line access modem (DSLAM) and the call from the customer now transverses a splitter (S) which routes voice traffic to the old switch and data traffic to the digital ATM switch of either the incumbent (ATM 1) or the new entrant (ATM 2) according to the customer's preferences. From the ATM data is passed to an ISP and then to the Internet or to an Intranet.

Figure 3.7
Local Loop Unbundling Options



Source: TRPC Pte Ltd

In the third scenario, the new entrant interconnects at or near the customer's premises. In the figure it is assumed that voice traffic will still transit by way of the incumbent, but this need not be the case. Scenario 3 requires the new entrant to build a network out towards the edge of the local service area, so its total investment will be higher, but it becomes less dependent upon the incumbent carrier for the quality of network services.

In the case of NGN networks unbundling, where this has arisen, poses a different set of issues .[71] In part this is because the architecture is very different. An NGN uses an architecture of a dual fibre backbone ring, for example Metro-Ethernet, for broadband transmission of high speed data, and sub-loops of fibre to serve local buildings, running the fibre-to-the-Curb (FTTC) or fibre-to-the-building (FTTB). This does away with the need for many exchange buildings or central offices, while digital switches are replaced by Gigabit routers located at strategic nodes around the core network. Subscriber line electronics which identify the individual needs and preferences of subscribers, such as their choice of bandwidths and services such as IPTV, are moved to the edge of the network closer to end

[71] For example, in the UK one study has found that unbundling the broadband local loop does not increase penetration rates but rather increases the quality of service. See Mattia Nardotto, Tommaso Valletti and Franck Verhoven (2102) ' Unbundling the incumbent: Evidence from UK broadband' http://www.econ.kuleuven.be/public/ndbad83/frank/Papers/LLU%20first%20draft.pdf

users while still being controlled from the centre. Because optical fibre does not conduct electricity an NGN network operator must also invest in their own parallel power grid. At the subscriber end this means unlike the conventional PSTN telephone, a house or office telephone that works off the Internet needs to have its own source of power, which could of course be the telecom company if it is also a power company.

Six out of 10 broadband lines in the USA were Digital Subscriber Lines (DSL) with fibre optic FTTx and FTTH accounting for 16.7% of the market in 2012.[72] This tells us that fibre, and NGNs at the core, is establishing a foothold in the market, and many developing countries have an opportunity to leapfrog straight into it as a more efficient telecoms platform that supports the digital economy.

Metropolitan Networks

New entrants without any legacy networks can move straight to an NGN whereas an incumbent needs to shift over in phases, often using a hybrid of fibre cables and copper wiring. In many cases, the shift requires the write-down of fixed capital assets using accelerated depreciation accounting. For example, an ATM switch may have many years of service left in it, but to achieve a more competitive cost base the incumbent has to replace it. Instead of depreciating the ATM over a period of 15 or 20 years, depreciation will be compressed into maybe 3-5 years. This could cause a problem with regulatory estimates of costs used for financial assessments and price control measures because costs will appear to have increased and this may need to be reviewed by the regulator.

The pressure to accelerate depreciation comes from competition. The arguments that competition will depress the revenues of the incumbent, making it more difficult to commit capital for investment, are not convincing. To become commercially successful on a sustainable basis incumbents have to go through a period of adjustment, even if that means issuing debt to finance change. Without competition, investment in new technology is bound to be slower and the benefits to the digital economy delayed.

One of the conditions for effective competition in metropolitan areas is tariff rebalancing. Traditionally, tariffs for international and long distance traffic were high and often cross-subsidized local call charges. Competition and new ways to communicate, especially over the Internet, have brought long distance tariffs down but without much increasing local tariffs because competition for mobile operators has changed the landscape. The revenues for the future in any case will not be coming from traditional voice traffic, but rather from the demand for broadband access and broadband services such as IPTV, movies-on-demand, and in the corporate sector, cloud computing services. Once the process of competition begins it tends to take on its own momentum, but for markets still dominated by

[72] Broadband Commission (2012) http://www.broadbandcommission.org/Documents/bb-annualreport2012.pdf

incumbents, regulators have to ask themselves what will make the market attractive to investment from new entrants and frame policies accordingly. When that happens, the local digital economy has a chance to grow.

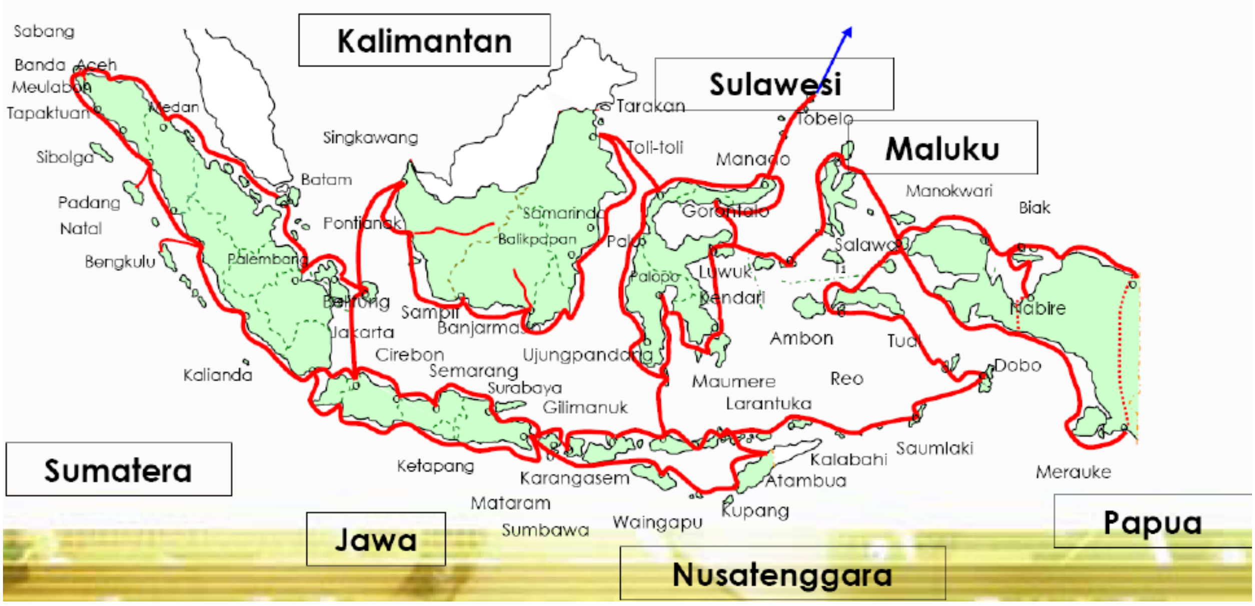
Closely associated with the growth of a digital economy is the spread of BWA which creates a demand for smartphones, tablet computers and other smart devices. This in turn creates an avalanche of data traffic that often networks cannot easily handle. Regulators can assist the industry and subscribers by placing sufficient radio spectrum on the market and by removing obstacles to lower prices for backhaul capacity. For example, MNOs should be allowed access to the capacity of the fixed line networks, some thought should be given to licensing MNOs to build their own backhaul networks and, following the regulations in India for example, to sharing facilities.

National Long Distance

For geographically large countries a domestic backbone network is an essential facility for linking centres of population and until it exists a country cannot effectively address issues of universal access and the digital divide. It should therefore be a priority objective of policy and regulation.

A range of technologies are available, from landlines to satellite, from long-distance microwave to coastal submarine cables.

Figure 3.8
Indonesia's Submarine Cable System



Source: http://www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/POLY_WB_GeneralReport_v3%5B1%5D.0.pdf

For example, there is now more than 25,000 km of coastal cable now linking the 18,000 islands of the Indonesian archipelago.[73] Figure 3.8 maps Indonesia's Palapa ring.

Although it may be difficult for new entrants to achieve the economies of scale enjoyed by the incumbent, the very act of connecting up towns and villages countrywide is the surest way to bring the benefits of a digital economy to these areas. That is an economic development issue, and development will generate traffic revenues for the future. It therefore makes good sense for regulators to remove as many barriers to entry as possible.

There are well known ways to do this. Allowing utility companies to lease their spare network capacity to new telecom companies is one step. Promoting the sharing of facilities like telecom towers and power generators is another. Requiring incumbents to adopt open access policies is another, as well as regulating both their leased line and interconnection policies. Allowing unrestricted access to the Internet and to OTT services such as voice and text is yet another.

The ultimate objective is to create national NGN high speed broadband networks that offer ubiquitous coverage. A typical core network transmission technology is GPON (Gigabit Passive Optical Network) which consists of dark fibres until they are lit using DWDM or dense wave division multiplexing. Economies of scale play a role here and governments often see advantages to the national economy of some public subsidy. In Australia, AUD43 billion has been set aside for a network to be built by Telstra on an open access basis. In Malaysia, Ringgit 2.4 billion will be used to subsidize Telekom Malaysia's High Speed Broadband Network (HSBN) again on an open access basis. In Singapore, SGD1 billion of public funds are being invested in a consortium (NetCo) to build the GPON and an independent wholesaler (OpCo) to operate the network. The incumbent SingTel will retain the right to compete separately.

Box 3.9

Dark Fibre

Optical fibre that has not been lit is dark fibre. Originally this term applied to the unlit capacity of carriers but now it also applies to capacity that is leased to other parties who light it up for their own use. It is not uncommon in the US, for example, for local exchange carriers or LECs to swap capacity with carriers in other districts so as to extend their coverage to areas they previously could not reach. Utility companies, such as railways, road highway networks and electricity grids, will often have spare capacity in their long-distance fibre systems which can be leased out as dark fibre. On the demand side, besides carriers looking for the bandwidth there are multi-site corporate businesses, data centres, universities and government departments looking to lease fibre connections to form closed-user group wide area networks (WANs). For example, in Brazil the government-funded Rede

[73] http://www.slideshare.net/mulimuljati/indonesia-domestic-fibre-optic

Nacional de Ensino e Pesquisa (RNP) colleges and universities network uses leased dark fibre.[74]

The quantity of dark fibre has grown exponentially, especially within oceanic submarine cable networks. The cost of laying of a cable on land or in the sea is literally a sunk cost which to all intents and purposes is invariant to the strands of fibre in the cable. Unlit fibre is cheap, so it makes economic sense to pack in many fibres. The expense arises when the electronic components are added and the fibre is lit. Increasingly DWDM or dense wavelength division multiplexing is used to transmit light signals along different frequencies or 'colours' of the spectrum, but because of the risk of interference between the light paths the dark fibre that is leased is often 'managed' in the sense that a 'coarse' WDW (CWDW) light path of 20nm (1 nanometre = one billionth of a metre) is maintained as a guard band.

International Connectivity

No sector of the market has seen a more dramatic increase in capacity and fall in prices than international submarine cables. This originally came about in the late 1990s as "irrational exuberance" in response to the dot.com bubble when the industry regularly over-estimated the rate of growth of Internet traffic.[75] Investment became detached from the facts on the ground, or on the seabed, and gave rise to a number of online secondary capacity markets in the spirit of the Internet revolution. Prices collapsed following the bursting of the bubble from 2000 onwards and changed the landscape of the international carrier market. Some major players went into receivership, many global carriers partially withdrew from all but their most important regional markets, and when they ventured back in the late-2000s it was often to lease rather than buy or build their own capacity.

From the mid-2000s new cables of terabit capacity began to appear. Some of these are consortium cables involving carriers from the countries with landing stations who buy 'indefeasible rights of usage' (IRUs) giving them the right to a certain capacity within the cable. Traditionally consortia were very conservative about IRUs but because of the supply overhang they have become more open to leasing to third parties. Part of this new wave of investment has come from carriers in developing countries, for example from Indian carriers Tata and Reliant in the Asia-Pacific. The bandwidths are humungous, but often less than 10 per cent of capacity is actually lit, but as CDNs spread throughout the world and data centres spring up with the rise of cloud computing the demand will grow.[76] In areas previously underserved capacity is rising. In Africa it now stands at over 22 terabytes for the

[74] http://www.ifi.unicamp.br/osa/telecom/Michael_Stanton.pdf

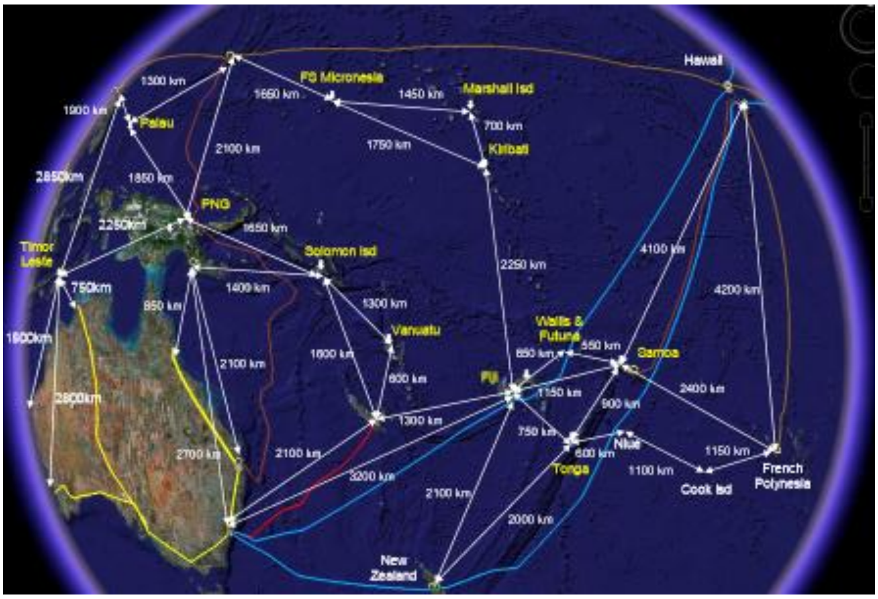
[75] Andrew M. Odlyzko (2003) 'Internet Traffic Growth: Sources and Implications' http://www.dtc.umn.edu/~odlyzko/doc/itcom.internet.growth.pdf

[76] See global view at http://www.samhamilton.co.uk/images/Equinix_Submarine_TGMap_MTS_15.pdf

East coast, 107 terabytes for the West coast and over 9 terabytes for the Mediterranean coast in the North.[77] In the Caribbean, four major cable systems are now providing connectivity,[78] while Latin America has been described as "the leading undersea market in 2013."[79]

Most challenging economically is to bring submarine cable connectivity to small island developing states (SIDS) such as the Pacific Islands. Satellite services are relatively expensive, even when used on a shared capacity basis, and do not provide the bandwidth of a submarine cable. A World Bank study in 2009 analyses in detail the options for cables.

Figure 3.9
Connectivity Across the Pacific Islands



Source: World Bank[80]

[77] http://manypossibilities.net/african-undersea-cables/

[78] An inter-active map of the world's submarine cables is available from TeleGeography at http://www.submarinecablemap.com/

[79] http://www.lightwaveonline.com/articles/2013/02/new-submarine-cable-systems-target-latin-america.html

[80] World Bank (2009) *Regional telecoms backbone network assessment and implementation options study: For a better Pacific Connectivity* *http://www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/POLY_WB_GeneralReport_v3%5B1%5D.0.pdf*

The original drivers of demand used to be international voice calls and commercial data traffic. That has changed. Many voice calls now go by OTT voice, video and text services such as Skype and Yahoo Messenger and commercial data traffic by Extranets. The driver today is principally the resurgence of Internet traffic, notably media video streaming and data traffic in the cloud between data centres. For example, according to the Cisco Internet traffic forecast for 2012, "51% of all Internet traffic will cross content delivery networks in 2017 globally, up from 34% in 2012."

Other notable metrics from the Cisco forecast are that "IP traffic is growing fastest in the Middle East and Africa, followed by Asia Pacific. Traffic in the Middle East and Africa will grow at a CAGR of 38% between 2012 and 2017" and that "In 2017, global IP traffic will reach 1.4 zettabytes per year, or 120.6 exabytes per month. Global IP traffic will reach 1.0 zettabytes per year or 83.8 exabytes per month in 2015."[81] These figures, even if only partially accurate,[82] spell the transformation of international telecommunications. Regulators have to be aware of them, have to prepare their markets to sustain the carriage of this data into and out of their jurisdictions. No one single landing station, satellite earth station or international gateway will be adequate to provide the quality of service and the redundancy required to make the economy competitive. Ways must be found to allow investment, competition and diversity into the market for international traffic.

[81] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

[82] But note that Cisco's forecasts are at the higher end of the scale of similar industry forecasts

Module Three: Law and Regulation for a Broadband World

3.6 Opening Vertically-Integrated Markets

In vertically integrated companies, the management has upstream and downstream control of the procurement, production, distribution/marketing and sales processes.

3.6.1 Benefits and Costs of Vertical Integration

Economic Theories

Economists have different theories as to why firms vertically integrate. A common theme is economies of scale which can result in lower prices for the consumers. The Chicago School of thought argues that if management is rational then it will only choose vertical integration if the economic incentives support that way of doing business. This has been termed *internalize complementary efficiencies*, the implication being that most forms of regulation will simply distort the incentives and force the firm to operate at a sub-optimal level. They go on to point out that in technologically fast-changing industries, monopolies rarely survive for long.

The New Institutional school, closely associated with the original work of Chicago economist Ronald Coase [83] and with University of California economist Oliver Williamson, suggests that vertical integration gives firms access to information along different points of the supply chain and across different markets that would otherwise not be easily available to them. The alternative would be incurring transactions costs of dealing with different suppliers, wholesalers or retailers. Vertical integration can save on these costs. By contrast, the older Institutional School takes its original inspiration from the work of nineteenth century American economist and sociologist Thorstein Veblen and later from the work of economist John Kenneth Galbraith. It points to the personal incentives and psychological motivations of managers preferring to manage larger than smaller corporations.

In reality all these theories can be correct to some degree. For example, the Chicago School would see the case studies of the Institutional School as examples of managers not doing what is in the best interests of their companies. This would mean they are not acting rationally in terms of the firm, while on the other hand the Institutionalists would see them acting rationally in their own terms. What all these schools of thought have in common is that they do not just describe *how* firms come to be large and vertically integrated, but *why*

[83] His seminal work *The Nature of the Firm* was publish in Economica, November 1937 when at the London School of Economics, see http://onlinelibrary.wiley.com/doi/10.1111/j.1468-0335.1937.tb00002.x/pdf

they do so, what motivates their management, and why they remain integrated or why they may choose not to.

Regulators

Why is this important to regulators? Two reasons. First, because regulators have to take into account the possibility that the firms are using their control of the supply chain to discriminate in terms of price, quality and timeliness of supply of upstream products and services to downstream competitors. This can result in 'profits squeeze' for competing retail service providers forcing them to withdraw from the market. If vertical integration undermines competition then investment, innovation and consumer welfare will suffer. Second, regulators need to understand how economic incentives influence the behaviour of the firm. Regulation that is poorly designed may do more damage than good. For example, policies that try to cap the profits of a dominant vertically-integrated company may simply result in that company shifting its investments from its regulated to its unregulated lines of business. Or, a price-cap that is linked to the rate of inflation and designed to encourage a firm to cut costs if it wants to boost profits (see Module 3.2) may result in the firm meeting its demand targets and then under-investing in efficiency-enhancing capital expenditure while it waits for the next round of price-cap adjustment. This example is given by Cave and Doyle who suggest the regulator "offer firms a menu of increasing investment levels, associated with progressively lower allowable rates of return."[84]

The opposite problem of 'gold-plating' arises when rate-of-return regulation allows the firm the same rate-of-profit whatever its level of investment. This is also known as the Averch-Johnson effect.[85] In the United States, where anti-trust rulings by the Federal Communications Commission (FCC) are regularly tested in the law courts, economic arguments have become compelling, or as Judge Richard Posner, a leading anti-trust economist and jurist put it "an economics-based approach has won in antitrust."[86] For this reason, regulators need to have a good understanding of what drives and motivates the companies under regulation.

[84] Martin Cave and Chris Doyle (2007) 'Network Separation and Investment Incentives in Telecommunications' Warwick Business School, University of Warwick http://www.kigeit.org.pl/FTP/ap/sot/07_11_12_podzial_2.pdf

[85] Averch, Harvey; Johnson, Leland L. (1962). "Behavior of the Firm Under Regulatory Constraint". *American Economic Review* v.52.5: pp.1052–1069.

[86] Joseph Farrell and Philip J. Weiser (2003) 'Modularity, Vertical Integration and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age' *Harvard Journal of Law & Technology* V.17.1 Fall 2003: pp.116 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=452220

3.6.2 Remedies to Anti-Competitive Conduct by a Vertically-Integrated Operator

Anti-Competitive Behaviour

Anti-competitive behaviour can arise from many different situations. Some example are collusion between equal competitors, or 'price-leadership' when unequal competitors prefer the easy life of living under the shadow of the incumbent who fixes the price. Different causes of anti-competitive behaviour call for different remedies. Anti-competitive behaviour that arises from an operator exploiting the advantages of vertical integration has many historical precedents.

Remedies a regulator can use include the following:

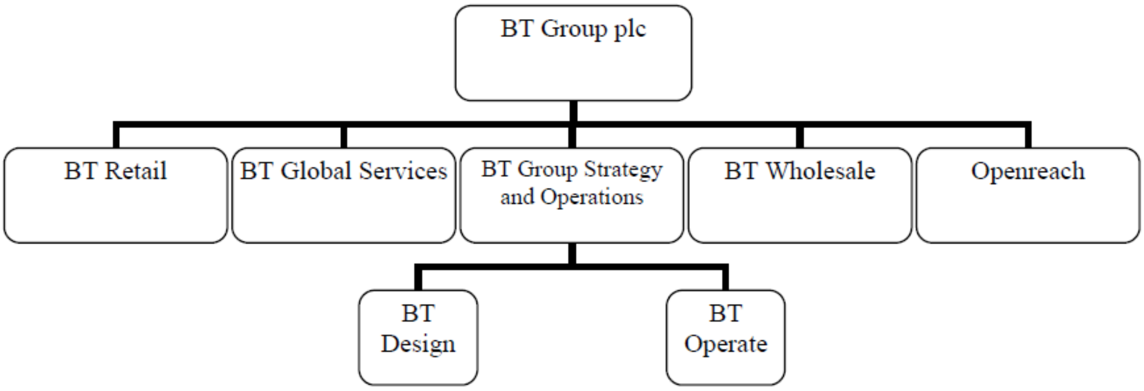
- Open the doors to new entrants and assist them in establishing a foothold in the market, for example, by unbundling the local loop, by regulating interconnection agreements, by allowing them to share facilities, by introducing number portability, etc.
- Encourage the adopting of new technologies, including Internet-based services that can offer consumers a real choice
- Require the regulated operator to offer equal access to competitors, if necessary along with incentives to comply
- Enforce separations if other measures are ineffective, either accounting, functional or structure separation
- Use a public subsidy for an independent network construction company and/or wholesale operator with an equal access obligation

There is no question that competition from new entrants using the most up-to-date and cost-effective technologies associated with all-IP broadband NGNs is the most effective way to combat anti-competitive behaviour by vertically-integrated incumbents. The important caveat is that policy-makers must support competition, if necessary by revising the terms and conditions of the incumbent's licence and the telecommunications laws under which it is issued. This process may require a compensation agreement to cover the loss of exclusive rights conveyed by the licence. Compensation can be in the form of cash, as was the case when the Hong Kong policy maker took back the exclusive international telecoms licence from Hong Kong Telecommunications to open up the market. Alternatively, the new licence can give the incumbent access to markets it could not previously enter. When AT&T in the US was broken up ('divested') through structural separation in 1980s into seven independent Regional Bell Operating Companies (RBOCs) otherwise known as Incumbent Local Exchange Carriers (ILECs), it was given the right for the first time to compete in call international markets.

Separations

Separations are a radical step for a regulator to take. In the UK in the 1990s, British Telecom (BT) voluntarily agreed to a functional or operational separation of its various business units in order not to lose the economies of scale that come from sharing some of its overheads and investment in R&D, including vital strategic business information. The restructuring was approved on an *ex post* basis, meaning that regulator agreed to a light-handed touch to see how well the new structure worked. See Figure 3.10 for BT's new structure.

Figure 3.10
BT's Functional Restructuring



No one has more detailed information about operational costs, markets and investments than the operators themselves, and this places regulators in a difficult position. To be effective the regulator needs the full compliance and cooperation of the regulated operator. This cooperation can come at a cost if the regulated operator manages to 'capture' the regulator, meaning the regulator becomes beholden. If the incumbent operator has close ties with high-level policy makers, which is quite likely, then the issue of transparency becomes very important.

Regulators who examine the case for separations need the cost accounting information of the operator to determine what would be the most cost-efficient means of separation. For example, if the wireless cellular operation is part of a competitive market but the fixed line PSTN is not, then the argument for an accounting or financial separation may be sufficient to ensure mobile prices are not cross-subsidized from fixed line rentals and usage charges. But that may not be sufficient if, for example, backhaul is provided to the mobile business unit but not for competitors on an equal basis, unless the competitors are also full service operators.

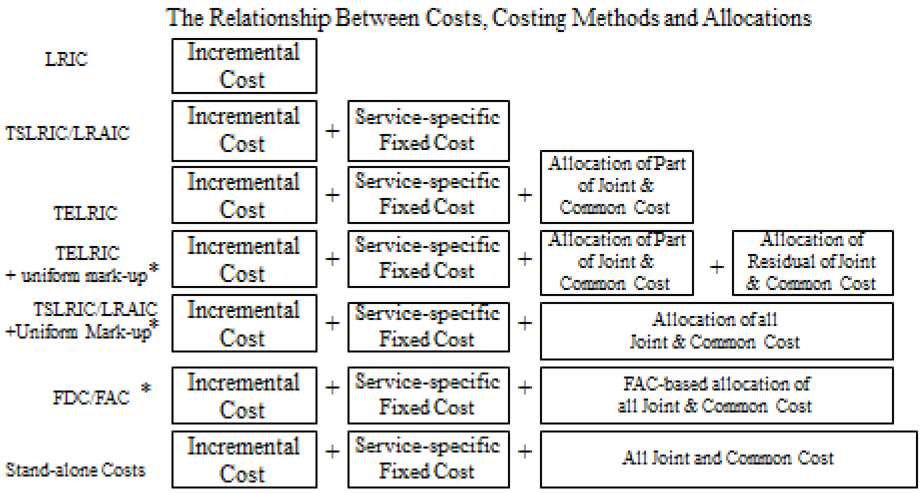
Box 3.10

Costs, Prices and Vertical Integration

Vertical integration is not by its nature transparent. Even an incumbent operator may not know the true cost of its many activities simply because under the traditional regime of monopoly pricing it never needed to know them. The traditional way an incumbent set prices was to allocate or distribute costs across a range of services based upon what the market would bear. In more competitive markets, where the elasticity of demand will be higher, the prices would be lower, while in more captive markets where the elasticity of demand will be lower, the prices would be higher. This is also known as Ramsey pricing.

The following Figure, from the World Bank's *Telecommunications Handbook* summarises the different cost allocation methods available to operators and regulators alike.

Figure 3.11


The Relationship Between Costs, Costing Methods and Allocations
LRIC
Incremental Cost
TSLRIC/LRAIC
Incremental Cost
+
Service-specific Fixed Cost
TELRIC
Incremental Cost
+
Service-specific Fixed Cost
+
Allocation of Part of Joint & Common Cost
TELRIC + uniform mark-up*
Incremental Cost
+
Service-specific Fixed Cost
+
Allocation of Part of Joint & Common Cost
+
Allocation of Residual of Joint & Common Cost
TSLRIC/LRAIC +Uniform Mark-up*
Incremental Cost
+
Service-specific Fixed Cost
+
Allocation of all Joint & Common Cost
FDC/FAC *
Incremental Cost
+
Service-specific Fixed Cost
+
FAC-based allocation of all Joint & Common Cost
Stand-alone Costs
Incremental Cost
+
Service-specific Fixed Cost
+
All Joint and Common Cost

Notes: 1. For TSLRIC/LRAIC the increment is defined as the total service. Hence, indirect cost elements are shaded while direct cost elements are not shaded.
2. In this example, FDC/FAC is assumed to be calculated based on forward-looking economic cost methodology.
3. The total costs of the 3 cost concepts identified by an asterisk (*), do not necessarily have to be equal as shown in this example.
4. Note the relative sizes of the costing concepts are indicative only and should not be taken as an approximation of an actual costs

Source: Hank Intven (2000) ed. *Telecommunications Regulation Handbook* The World Bank

From the bottom-up the Figure illustrates the following:

1. **Stand-alone** costs when there is one output or service and all the costs must be covered in the sales price.

2. **Fully Distributed/Allocated Costs (FDC/FAC)**: when there are two or more service outputs, for example local, long distance and international voice services, the costs of any of them consists of an apportionment of common costs, e.g., property taxes, and of joint costs, e.g., the cost of the switch used for both services, such that *all* common and joint costs are covered by each of the services in combination, plus the fixed costs

specific to that service, such as the costs of the cable landing station or satellite station, plus the incremental costs associated with that service, such as the total of marginal costs of switching or routing traffic.

3. **Total Service Long-Run/Long-Run Average Incremental Cost (TSLRIC/LRAIC) with uniform mark-up**: the same as FDC/FAC with two exceptions. Costs are forward-looking (not historical) based upon new technologies, and the allocation of common and joint costs is done on some defined proportionality basis, such as the percentage volumes of traffic or revenues.

4. **Total Service Long-Run Incremental Cost (TSLRIC) with mark-up**: the same as TSLRIC/LRAIC except mark-ups distinguish between common and joint costs shared by services, and residual costs that arise even at zero output, sometimes referred to as "keeping the lights on."

5. **Total Service Long-Run Incremental Cost (TSLRIC)**: the same as TSLRIC/LRAIC except that the allocation of common and joint costs only includes those that are genuinely common or joint costs of the services under consideration.

6. **Total Service Long-Run/Long-Run Average Incremental Cost (TSLRIC/LRAIC)**: same forward-looking costs as above without the mark-up, so only incremental (variable) direct costs and a proportion of fixed costs are included.

7. **Long-Run Incremental Cost (TSLRIC):** only forward-looking incremental (variable) direct costs are involved.

An example of regulatory costs accounting is the emphasis the FCC placed upon 'modularity' or open access following the Telecommunications Act of 1996. The FCC ruled that vertically-integrated RBOCs or Incumbent Local Exchange Carriers (ILECs) would be required to offer various 'unbundled network elements' (UNEs) as separate modules to local competitors at a cost-based price. For example, access to the registry of residential and business telephone numbers. This was to ensure that if the LECs offered interconnection to their competitors they did not force them to pay for network elements they did not need. The FCC used a methodology called total element long run incremental cost (TELRIC) to determine an appropriate price of UNEs.[87]

Going Vertical: Mergers & Acquisitions

Vertical integration works well for firms with a relatively narrow-range of products, but as the range get wider the challenges of management coordination grow and the efficiencies get called into question. If the products and services are complimentary then the

[87] http://www.techopedia.com/definition/26165/unbundled-network-element-une

advantages of becoming big probably outweigh the disadvantages. However, if the product range is diverse, includes substitutes or competing services, and results in the need for a variety of different investment and marketing strategies, then big can spell trouble. For example, the merger of a telecoms and a cable or IPTV business may seem to be a case of convergence, but the investment profiles and management skills required by each are entirely different. For these reasons, in some some industries mergers and acquisitions (M&As) may end up destroying more value than they create. In other cases, such as when an incumbent acquires an innovative start-up which has recently entered the market, the big question is whether what is being acquired are the inventors and innovators behind the start-up or just the intellectual property. Whether M&As add value or destroy value is something that can only be tested in the marketplace; for regulators that is not the issue, rather it is whether there is or is not a high probability competition, and therefore innovation and customer choice, will be reduced.

This presents regulators with a range of issues. First, is a vertically integrated telecoms company dominant because it is efficient or because it is abusing its market power and discriminating against weaker competitors? Second, when an M&A is proposed, will it significantly reduce competition in the market, or will it increase efficiency and present consumers with better value services? Third, even without discriminatory behaviour, is the vertically-integrated company in any way 'dominant' and if so does it wield 'significant market power' (SMP) such that it can independently influence market prices for itself and its competitors? Dominance is only a measure of potential market power. Whether the company exploits that power in anti-competitive ways is a judgment call by the regulator who has to decide whether to regulate *ex-ante* (on the presumption of anti-competitive behaviour) or *ex-post* (on the basis of observation and assessment) – see module 3.2.

These are essentially economic issues, but there are also issues of political power and social influence. Cross-ownership rules are designed to curtail the concentration of power in too few hands and are usually part of an M&A assessment process. There are further issues, such as a concentration of foreign ownership if a country identifies some of its telecom services as national economic or security concerns. But it is important that trade commitments made under the WTO are honoured to achieve the greatest possible benefits from investment in open markets. The telecoms regulator may not be the final arbiter on whether an M&A is allowed to proceed, but where the merged companies involved a telecoms operator the view of the regulator on the possible outcome is important.

Vertical Value Chains

Over recent decades in the supply chain for the fast-growing mobile sector of telecoms equipment there has been something of a tug-of-war between the vendors who manufacture the handsets and the operators who connect them to their networks. Although vendors may decide to sell their handsets through retail outlets the bulk of their sales is often to the carriers. Through bulk purchases of handsets the carriers get important discounts which they can pass onto their subscribers, adding their own discounts to attract new customers in cases where the mobile services markets are highly competitive. But there is also competition between the vendors and the operators to determine which of them secures the larger share of the value along the supply chain.

Branding, designs ('form factors') and operating systems have been the key areas of competing demands. Vendors want to their name as the band. As with other products, better known branded handsets sell at a premium over lesser brands. But equally, operators such as Vodafone and DoCoMo and Hutchison's "3" benefit from name recognition if the handset carries their brand. Bulk-buying has sometimes swung the balance of branding power towards the carriers, especially those who won licences to pioneer the next generation of mobile services, such as 3G. With branding power (the logo on the phone) often went the power to dictate the designs or 'form factor' of the phones, such a flip-tops, slide phones, swivel phones, touch screens, their colours and shapes. But the power of operators tends to diminish as the carrier market itself becomes more competitive. Their power is further eroded if they are unable to dominate the market by 'locking' the handsets they connect to the network so that only their SIM cards can be used in those phones. This erosion can arise from regulation which outlaws the practice, or by customers shifting to the unlocked services of their competitors which may happen, for example, when cheaper phones are bought in increasing numbers by lower-income and often pre-paid users.

Apple is a vendor that has traditionally locked its phones and made agreements with carriers to keep them locked. The iPhone, launched in 2008, is widely accepted to have been a game-changer for the industry. For the public its brand name and designs were major attractions, in particular its touch-screen features, but behind both was Apple's innovative iOS operating system. Operating systems (OS) determine which apps can be run, their screen appearance as well how to navigation a phone's many functions, which are themselves apps. Like the now defunct Symbian OS used by Nokia, Ericsson and others, they may be owned by a consortium of vendors, or like iOS they may be vendor-specific, or like Google's Android OS they may be owned by one vendor but freely available to all. They constitute a vital part of the intellectual property of handset manufacturers and, where they are under a commercial licence, an important source of royalty revenue.

The outstanding feature of the handset market today is how fast the technologies develop, the apps develop, the form factors change. This has resulted in market leaders of yesteryear falling behind or even exiting the market. It has resulted in component manufacturers and original engineering and manufacturing (OEM) companies entering into alliances with one or other of the major vendors, or in some cases, such as HTC vying to become a major vendor in its own right by selling direct to large carriers, for example, in China. This underscores how quickly the balance of market power can shift horizontally between vendors and vertically between vendors and carriers. After the iPhone kick-started a radical shift towards smartphones, Apple held enormous market power, for a short time catapulting the company into being the largest in the world by value. Apple could more or less dictate terms to the carriers it selected to market the iPhone, with previously unheard of commercial agreements which included the carriers to guarantee a local subsidy to iPhone retail prices and even a revenue-sharing agreement. That power was derived from the strength of consumer demand for, and loyalty towards, each new iPhone release. [88]

But the market has never ceased moving on, seeing new vendors including social networks like Facebook moving into the mobile market. In many ways it is appropriate that this is the case. The very last part of the traditional telecommunications market to face competition and to see innovation was the telephone receiver. Only in the 1980s was there widespread opening of the consumer premises equipment (CPE) markets, which began with non-black plastic telephone designs, and then telephones with additional functions such as stored numbers, call holding, recall, etc., which could be bought in supermarkets at low prices. The OS of mobile handsets has set new standards of innovation because they are linked to the Internet. For regulators, the issues raised are many, but they mostly revolve around competition and consumer protection issues to be with pricing, locking, blocking of apps and net neutrality.

[88] See, for example, ‘Vertical Integration Works for Apple -- But It Won’t for Everyone’ http://knowledge.wharton.upenn.edu/article.cfm?articleid=2959 and Chantal Tode ’Can Apple’s vertical integration work for others in the mobile space?’ *Mobile Commerce Daily*, 9 July 2012 http://www.mobilemarketer.com/cms/news/manufacturers/13262.html

3.7 Net Neutrality

The common understanding of net neutrality is a regulatory stance against any form of discrimination by telecom networks against users of the Internet, whether as suppliers of services and content or as consumers. On the supply side, this implies that Internet companies should not be charged for delivering their products to end users unless they have come to a commercial agreement with the network. For example, to act as a local billing agent or as a content distribution network (CDN). On the demand side, this implies that customers should not experience any blocking of sites that has not been sanctioned in law, nor any throttling or quality degradation of the bandwidth that they are entitled to, nor charged discriminatory fees. What is normally permitted is a layered tier of bandwidth prices for customers to choose from and each customer can choose their preferred package. It is relevant to note that when consumers buy access devices, such as tablet computers, they come at different prices according to the speed of the networks they can access, thus equality of consumer choice seems to be consistent with different price levels for different levels of service.

On top of this, regulators usually recognize that telecom companies, most of whom are also Internet service providers (ISPs), have the right to manage their networks in the most cost-efficient manner to ensure quality of service obligations. The quality of service standards for available access to a network stands ideally stand at over 99%. For example, the Infocomm Development Agency (IDA) in Singapore requires 99.85% for the narrowband and 99.9% for broadband,[89] while in Chile the standards for narrowband are set at 97% in urban areas and 90% in rural areas.[90] By contrast, in the 1990s, Internet traffic was seen as 'best effort' unless it was sent over a public or private managed network. In the broadband era, the public expect consistently high access rates, although the speeds will differ widely from market to market. The quality of service is vital also to the success of the digital economy.

The issues at stake are principally two-fold. First, whether the network operator is using the need for quality-of-service network management as a cover for bandwidth throttling or degradation of some services such as peer-to-peer communications. Second, whether they should have the right to charge fees to Internet companies for the use of their networks as a way, as they will argue, to raise the funds required to invest in new network capacity. To confront these issues regulators need to examine their own policy goals.

[89] http://www.ida.gov.sg/Policies-and-Regulations/Industry-and-Licensees/Standards-and-Quality-of-Service/Quality-of-Service

[90] http://www.itu.int/ITU-D/ict/newslog/CategoryView,category,Quality%2Bof%2Bservice.aspx

3.7.1 Goals of Net Neutrality

In 2011, a study by the Body of European Regulators for Electronic Communications (BEREC) found that the blocking of voice-over-Internet protocol (VoIP) and peer-to-peer traffic by telecom operators and Internet service providers was a common practice. In 2013, the EU Commission announced it would proceed to require all telecom carriers to observe net neutrality, meaning no throttling, no degradation of Internet services and unrestricted access to Internet content providers by users without discrimination between low and high volume users. What is permitted is the practice of charging users different prices for different bandwidth packages.

In many developing economies there are no effective regulations and the incumbent operator pretty much does as it pleases. For example, a study of the Union of the Comoros off the East Coast of Africa reveals that Comores Telecom (CT), which holds a monopoly in both fixed-lines and mobile telephony, and acts as the sole Internet Service Provider (ISP), is threatened with declining international call revenues from competing OTT voice services such as Skype and Viber.[91] Its strategy has been to deliberately degrade the quality of the internet service it provides to its subscribers, on both fixed and mobile networks. By increasing the latency, or delay, in internet traffic, it makes VoIP effectively unusable. This has proved to be a highly controversial policy because it also affects other legal internet services, such as webmail or instant messaging used by Comorian citizens. Clearly, this is not a sustainable long-term solution for CT or for the Union of the Comoros.

In the US, the Federal Communications Commission (FCC) accused cable TV operator and Internet service provider Comcast of selectively blocking connections to peer-to-peer (P2P) applications. Comcast was found guilty, but a ruling by the Court of Appeals in 2010 found that the Commission did not have legal jurisdiction over the Internet services of Comcast. Subsequently, the FCC published in 2010 an Open Internet Report & Order, guidelines to keep the free and open nature of the Internet, around the three basic principles of transparency, no blocking and no unreasonable discrimination. But beyond these guidelines there is no legislation or formal regulations for Internet neutrality.

Besides the commercial interests of the carriers and the Internet companies involved, there are opposing camps of the ‘deregulationists’ including property rights advocates *versus* supporters of the ‘open access’ and ‘commons’ approach. For property rights advocates, carriers should retain a right to manage their networks to their own best advantage with minimal interference from regulators. This argument works best when there is well established competition for consumers to choose from. Consumer advocates of the ‘open

[91] "ICT Sector policy note on Comoros", 2013, Tim Kelly and Clara Hervaz-Lezcano (unpublished World Bank policy note).

access' approach point to the lack of competition that results from violations of net neutrality, and to the adverse effects this has upon investment in, and growth of, the digital economy.[92]

3.7.2 Regulatory Approaches

The FCC, in considering the Comcast case, issued a consultation paper asking what were ISPs using traffic management techniques trying to achieve; was it to prioritize latency-sensitive applications, to avoid network congestion, to block unwanted traffic, to implement parental controls, or was to gain advantage over competitors. For regulators concerned that network management may be used as a pretext for discrimination against sources or users of services over the Internet, the devil lies in the detail. Network management tools can do blocking, traffic shaping and quality of service functions. Each can be used for discriminatory and non-discriminatory purposes.

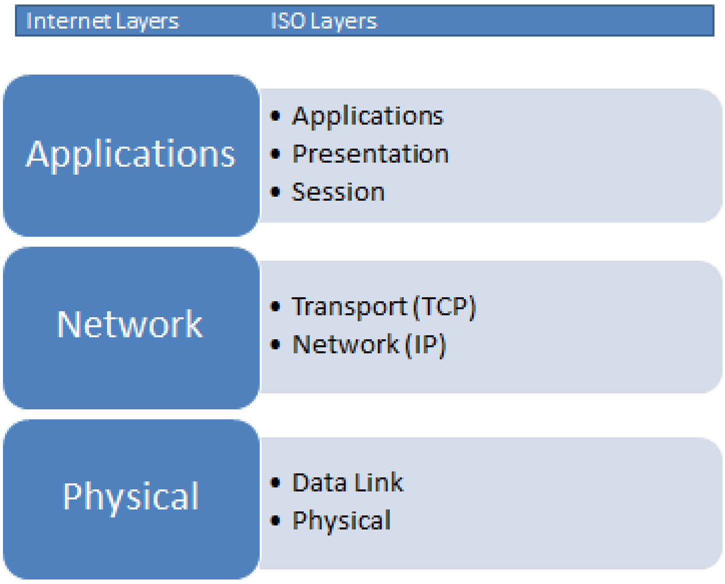
The question asked by the FCC was whether the network management in question was 'reasonable', although the definition of 'reasonable' is itself open to question. In other words, the concept of net neutrality in operational terms is often arrived at only after a judgement has been made on what actual network management practices are reasonable and unreasonable. There is a huge literature debating the finer points of net neutrality along these lines, and a useful approach, although not the only one, has been put forward by Scott Jordan and Arijit Ghosh of the University of California, Irvine.[93] They start their analysis using the three-layered stack of the Internet as compared with the standard seven-layered stack ISO model traditionally used by telecom engineers. (See Figure 3.12).

[92] For a short review of these positions and advocacy of a 'nondiscriminationist' middle approach, see Scott Jordan (2007) 'A Layered Network Approach to Net Neutrality' *International Journal of Communication* v.1 pp.427-460 http://ijoc.org/ojs/index.php/ijoc/article/view/168

[93] Scott Jordsan and Arijit Gjosh (2009) 'How to determine whether a traffic management practice is reasonable'   http://www.ics.uci.edu/~sjordan/papers/tprc09.pdf

Figure 3.12

A Layered Model Approach to Net Neutrality



They suggest that four criteria could be used by regulators to judge whether or not network management practices raise red warning flags.

- **Where** within the network are the network management tools applied: in typical Internet design it is assumed that management techniques are applied *above* the transport layer if possible. If they are applied in the transit between the different networks (source network and the carrier network) in the routers below the transport level this should raise a red flag.
- **What** type of tool is applied: if network congestion is short or medium term (for example, less than one minute) then tools such as traffic shaping and queuing are effective, for example at endpoints in the network. The delay occurs at final delivery, but for congestion over one minute access control may be required. If this involves blocking or termination as opposed to quality of service degradation this should raise red flag.
- **Who** decides which tool should be applied: it may be at the request of the Internet source or the end user, but if it is a unilateral decision of the ISP then this should raise a red flag.
- **When** and on what basis is a tool applied: it may be applied to (i) an application, (ii) the source/destination, (iii) the service provider, and/or (iv) the payments processor.

> Tools applied to traffic on the basis of (ii) or only to traffic based on (iii) should raise a red flag.

What is useful about this framework is that it is not deterministic because the red flags are only alerts that can help regulators. However, this does focus attention on the fact that in an interconnected world the old distinctions between what were telecoms services and what are services over the Internet can no longer be a good guide to policy. For the 'deregulationists' these red flags will be redundant and for some advocates of 'open access' they may not go far enough, but regulators do need some practical points of reference going forward.

3.7.3 Net Neutrality and Wireless Networks

Under the FCC's *Open Internet Report & Order* (2010) "Fixed and mobile broadband providers must disclose the network management practices, performance characteristics, and terms and conditions of their broadband services" but excludes mobile from restrictions on blocking and "unreasonable discrimination".[94] Broadband wireless sector was exempted because it was seen as a young growth sector. Unlicensed spectrum services are not covered by the Order.

As noted above, many wireless broadband devices place limits on what services can be received, for example, Apple's iPhone does not download Adobe files and restricts the types of apps that can be downloaded, and certain devices will not stream YouTube. The device vendors often have partnerships with different telecom networks, with CDNs and even have their own networks. Mobile networks are often converged with fixed (FMC), and these crossovers do not lend themselves to universal net neutrality regulations. For regulators the important issue is to keep the mobile wireless market as competitive as possible so consumers always have choice.

3.7.4 Governance Issues

Governance of the Internet is fundamental to its openness. The Internet began as an American creation that has now become part of the everyday life of the modern world. That means it also becomes part of every country's national interest. It can only be hoped that a multi-stakeholder approach does not politicize the Internet which would be detrimental to the damage the digital economy. Good regulation should guard against that danger.

Two issues in particular have featured significantly in recent debates, and they relate to the respective roles of states and other stakeholders in Internet governance. The first issue

[94] http://www.fcc.gov/document/preserving-open-internet-broadband-industry-practices-1

concerns the rights of states within their own borders to govern the use of Internet domain names at the country level. The Domain Name System (DNS) evolved for technical reasons using Latin script for Top-Level Domain Names (TLDs) such as .cn for China and .com for company. Later it became possible to use non-Latin scripts such as Cyrillic, Hebrew, Korean, Thai, etc., which have been adopted by many countries for their country code TLDs or ccTLDs, also known as Internationalized Domain Names of IDNs.[95] Over time search engines may adapt to these as well, but until they do searching for materials in non-Latin languages will remain an obstacle. For many states this raises both cultural and political concerns. The second issue concerns agency. Some Internet issues, such as the DNS and Internet engineering protocols are handled within internationally recognized bodies, such as Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) but as of 2013 there is no international agency that deals with other issues such as cyber-security over the Internet. Some states have suggested the ITU could extend its reach into the area, a suggestion quite vigorously opposed by others, including some other states and by many in the Internet community itself, who do not see an inter-governmental telecommunications organization as being the appropriate forum. Whatever the outcome of this debate, the issues it raises are very real and ways need to be found that are genuinely multi-stakeholder with no-one claiming to have all the answers. The Internet is a continuously evolving technology-based mode of communications which is having truly profound economic and social consequences, and the role of regulators is probably best described as two-fold: to regulate with a light touch in order to encourage continuing innovation and the benefits that brings, and encourage the active involvement of all stakeholders to address the various challenges the spread of the Internet has for society.

[95] "For technical reasons, support for non-Latin scripts was treated as a design and deployment problem whose solution was intended to minimise change to the domain name resolution infrastructure. This was debated in the Internet Engineering Task Force more than once, but the general conclusion was always that requiring a change to every resolver and domain name server, rather than changes on the client side only, would inhibit deployment and utility. This led to the development of so-called 'punycode' that would map Unicode characters representing characters from many of the world's scripts into a ASCII characters (and the reverse)." Vinton G.Cerf *Foreword: EURid-UNESCO World report on Internationalised Domain* http://www.eurid.eu/files/publ/insights_2012_idnreport.pdf
Names deployment 2012

Module Three: Law and Regulation for a Broadband World

3.8 Security in Cyberspace

All societies are vulnerable in cyberspace due to the growing interconnection of networks, of people through emails and social media, etc., and increasingly of 'things' such as machines, sensors and consumer goods, through the Internet using cables, Ultra Wideband (UWB) and other wireless technologies.

The vulnerabilities exist at all levels. For analysis it is useful to think of three levels: high-level attacks on critical information infrastructure (CII) which can bring parts of a country to a standstill and are likely to come from a terrorist assault or political cyber-warfare; cybercrime which can range from industrial scale espionage of state or commercial secrets, to massive financial theft and fraud, and to so-called 'white-collar' crimes such as tax evasion moving online from offline; and third, crimes against persons such as child abuse, cyber-bullying, online defamation, etc.

3.8.1 Security of Critical Information Infrastructure

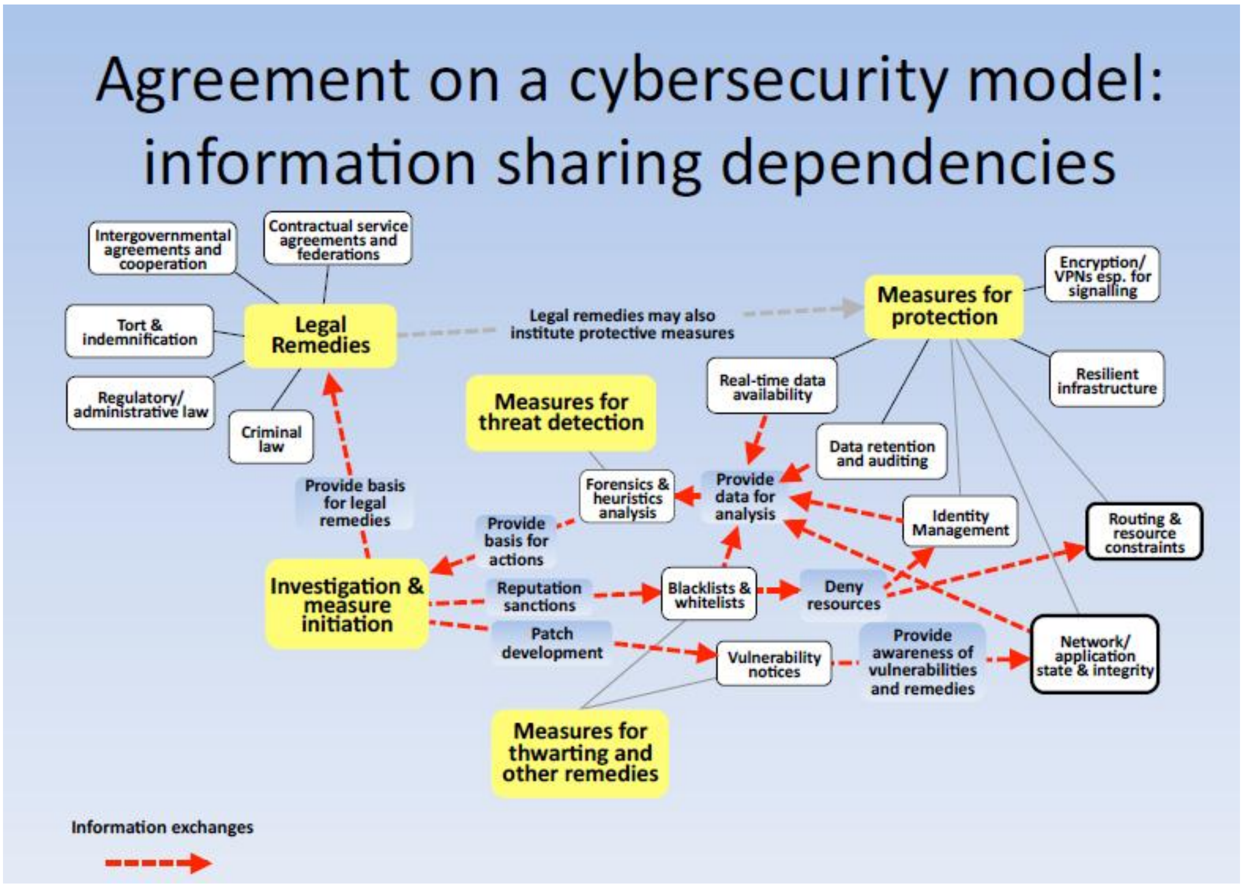
At the highest level, the first recorded cyber-assault on a country's entire infrastructure was in Estonia in April 2007 when websites of Parliament, ministries, newspapers, banks and others were brought to a standstill in distributed denial-of-service (DDOS) attacks. Even more insidious is the malicious use of web robots or 'bots'. They are very useful in search engines for tasks such as web spidering, but they can also be used to take remote control of websites without the owners knowing it, read the files and implant malicious code. Like the rogue computer Hal in the movie '2001' that takes control of the spaceship, this is a very power weapon in the wrong hands. Public utilities such as a telecoms and energy networks could be hijacked, traffic diverted, energy supplies cut off, causing untold economic loss and loss of life.

CERTS and CTBEX

Although it is not possible to assign precise levels of risk to cyber-security in terms of exact times and places, with sufficient data is it possible to assign degrees of risk to different areas of strategic importance and to possible timescales. Using past data on attacks and a strategic view of network vulnerabilities, some planning and preparation is possible, but success is entirely dependent upon good detection work based upon intelligence and information sharing between agencies. It is important, for example, that telecom operators and Internet service providers notify the regulator or cybercrime agencies of suspected or actual cyber-attacks.

It is equally important for these agencies to work in close collaboration and exchange of information, first at the national level, and second at the regional and international levels. To this end, the ITU has been involved in an initiative on cyber-security for telecom networks through the Cybersecurity Information Exchange Framework or CTBEX.[96] It consists of a set of protocols and standards and a general framework which integrates different security domains, such as measures for protection, detection, remedies and legal as illustrated in the Figure 3.13 below.

Figure 3.13



Agreement on a cybersecurity model: information sharing dependencies

Intergovernmental agreements and cooperation

Contractual service agreements and federations

Tort & indemnification

Legal Remedies

Regulatory/ administrative law

Criminal law

Legal remedies may also institute protective measures

Measures for protection

Encryption/ VPNs esp. for signalling

Resilient infrastructure

Measures for threat detection

Real-time data availability

Data retention and auditing

Provide basis for legal remedies

Forensics & heuristics analysis

Provide data for analysis

Identity Management

Routing & resource constraints

Provide basis for actions

Investigation & measure initiation

Reputation sanctions

Blacklists & whitelists

Deny resources

Patch development

Vulnerability notices

Provide awareness of vulnerabilities and remedies

Network/ application state & integrity

Measures for thwarting and other remedies

Information exchanges

Source: http://www.jnsa.org/isog-j/output/2010/1013/2_Rutkowski.pdf

Ministries and regulators need to be part of a national cyber strategy planning process. For example, the Ministry of Information and Communications in Mauritius with support from the African Development Bank has developed a holistic approach to cyber-security with a National Strategic Plan that was created for 2007-2011 and has been revised for 2011-2014.[97] This follows the creation of Police Cybercrime Unit in 2000 and a Computer Emergency Response Team (CERT-mu) in 2008. The Plan transparently identifies areas of

[96] http://www.itu.int/dms_pub/itu-t/oth/06/48/T06480000010006PDFE.pdf

[97] http://www.gov.mu/portal/goc/telecomit/file/ICTplan.pdf

cyber-security that need strengthening, which is the first step towards reducing risk. It also outlines the coordinating mechanisms required between agencies.

The creation of CERT-mu is an important step and follows best practice for many countries; for example, US-CERT is the 24x7 operational arm of the Department of Homeland Security.[98] In East Africa, the Cybersecurity Taskforce of the East African Communications Organizations (EACO) covering Burundi, Kenya, Rwanda, Tanzania and Uganda was formed in 2008. It tasked with setting up national CERTS in each member state. National expertise in cybercrime issues may reside in several different departments and law enforcement agencies and in private IT and telecom companies and it is therefore important that national strategic plans optimize on ways to share information on a timely basis. The following points can be used to assess how successful organizationally the setting up of cyber-crime agencies have been.

1. How many staff have been on cyber training
2. What outside expertise has been enlisted to grow the capacity of the agency
3. Has the agency developed its own training programme for use by other agencies
4. Has the agency developed a database coordinating details of known cyber-attacks from all other national sources
5. Has the agency developed plans to cover: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; support both from and for the ICT sector

Point 5 is from the EU Action Plan on CIIP.[99] Other countries have their variants, for example, Morocco's National Cybersecurity Management System has the following five domains: strategies and policies; implementation and organization; awareness and communication; compliance and coordination; monitoring and evaluation.[100] Telecom and information ministries and regulators clearly have a major input to make into each of these domains and expertise in cyber-security is something all ICT agencies need to add to their domain capacity.

3.8.2 Cyber Crime

The level of cybercrime is difficult to gauge with any precision, but a study in 2012 for the UK Ministry of Defence by Anderson et al., collates estimates of various cybercrime categories at the global level, collecting global data where it is available and otherwise extrapolating from UK data on the basis that UK GDP is 5% of global GDP. Their findings are summarized in Table 3.2. For the sake of brevity the table presents sub-totals as a

[98] http://www.us-cert.gov/

[99] http://sta.jrc.ec.europa.eu/pdf/scni/ExperimentalPlatforms/1-CIIP_INFSO_WS%2020090619.pdf

[100] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/debbagh-morocco-cybersecurity-june-09.pdf

compromise with their caveat that "it is entirely misleading to provide totals lest they be quoted out of context, without all the caveats and cautions that we have provided."[101]

Table 3.2
Estimated Global Costs of Cybercrime, 2012

Cybercrime type	Global Estimate ($ millions)	Notes
Cost of genuine cybercrime, such as scams, phishing, etc.	**$2,457m** + $1,000m = $3,457m	For the years 2007, 2008-2010, 2011; mostly considered under-estimates
Cost of transitional cybercrime, such as online credit card fraud	**$7,360m** + $39,240m = $46,600m	For the years 2009-2011; some considered under-estimates
Cost of cyber infrastructure, such as antivirus costs, etc.	**$11,000m** + $13,840m + $24,840m	For the years 2010-2012; high degrees of uncertainty
Cost of traditional crimes becoming 'cyber', such as tax fraud	**$5,200m** + $145,000m = $150,200m	For the years 2010-2011; some uncertainty

Source: Anderson et al. (2012) 'Measuring the Costs of Cybercrime'; Notes: figures in **boldface** based upon available data, figures in non-boldface extrapolated from UK data based upon size of GDP; costs *may* include data on criminal revenues, direct losses, indirect losses and defence costs.

These figures, as the notes accompanying the original table make clear, under-estimate the real costs to society. What can be said with certainty is that the risks and the costs will increase over time as societies become more connected, and it will pay society to devote more resources to reducing the risks, which include public sector assets, private sector assets and personal assets, from crime on an industrial and global scale.

Since these criminal activities are carried over networks operated for the most part by telecom companies, there needs to be careful surveillance of suspicious traffic. But the reality is today that a lot of this activity is conducted from proxy servers and the origins of the criminals is unknown and could be from any country. The implication seems to be that detection is more likely of the crime than of the criminal, and although highly professional cyber detectives with access to cyber forensic laboratories can make progress these skills and facilities are not widely available in developing economies. This in turn implies that the focus of policy makers and regulators at the national level is best directed at limiting the damage through early detection, fast and efficient information sharing, and a focus on alerts and awareness. It is usually beyond the scope of regulators to track and trace the crimes to their origins, but regulators can play a vitally important role in creating the ecosystem of cyber-security.

[101] Anderson et al. (2012) 'Measuring the Costs of Cybercrime' p.25 http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Law Enforcement and the Proportionality Principle

When it comes to applying the law, regulators need to be cautious about the boundary between detection and law enforcement. The laws under which regulators work need to specify very clearly the limits of their responsibilities, such as the circumstances under which they can seek a search warrant for activities which are illegal under the telecoms laws. The enforcement of cyber laws is more likely to be the task of the police or customs and excise officials, and regulators need to avoid becoming embroiled in civil liberty issues.

A good guideline for any regulator or law enforcement agency is proportionality, a judgement regarding the seriousness of the infringement, whether, for example, it is a major crime with wide social implications or a minor infraction with little social impact. Because cyberspace is a relatively new area of governance, and because it crosses jurisdictions, countries have often been struggling to make laws that are appropriate. And it must be said that often the law making process is not as well informed as it should be. It is therefore important for law makers, policy makers and regulators to bear in mind some simple principles.

- In general, what is legal offline should be legal online, and what is a civil offence as opposed to a criminal offense offline should be treated similarly online.
- Extra-jurisdictional applications of national laws need to be very carefully vetted. Often what is legal in one country may not be legal in another. For example, an Internet posting may be considered fair comment and free speech in one jurisdiction but regarded as illegal in another, and yet the posting is available globally. Proportionality would suggest that criminalizing behaviour may not be either good justice or a good use of legal resources.
- Codes of practice – Intellectual property rights are becoming the subject of numerous bilateral and multilateral trade negotiations. The length and enforceability of copyright, for example, is often a controversial topic. With Internet hosting companies there is a question of who is liable for a posting that breaches copyright. The US Millennium Digital Copyright Act of 1998 provides one set of useful guidelines. It gives latitude to web hosts who abide by take-down notices in cases where someone unbeknownst to them has posted something that breaches copyright. The system is not perfect because identifying a particular posting on a site the size of Google or Yahoo! or Amazon or Twitter is not so easy, especially where it has gone viral, where others have shared it or added their own comments to it. Laws should be seen to be workable and proportionate and regulators should not be burdened with controversial applications of laws that are not well drafted. The regulator's job is better to ensure the greatest level of transparency on the part of

companies that operate under a licence, and to promote a sensible, that is to say *manageable*, code of practice which offers incentives, such as immunity from prosecution, for doing the right thing alongside obligations to avoid doing the wrong thing.

3.8.3 Cyber-Strategies

At the heart of cyber-security lies the issue of detection, that is detection of the event itself as well, ideally, detection of the offender. That can only come from sharing information, but there exists an asymmetry between private gains and social losses. As Tyler Moore has pointed out, by integrating part or all of their operations with the Internet in order to cut costs companies may substantially increase the risk of cyber-attacks but at the same time they may not choose to devote sufficient resources to the resulting insecurity.[102]

For policy makers and regulators the recommendations are to be prepared to mandate the sharing of critical cyber information but look for ways to incentivize organizations so it is in their own interests to share. To take an example from the financial services sector, in markets where EMV 'chip and pin' credit cards are available, banks and bank customers are offered insurance against card fraud when banks issue and customers use the EMV standard, but that cover is no longer available for traditional magnetic strip cards. Persuading organizations to come clean about cyber-attacks on their systems can be more difficult, but if by sharing information they also gain information and witness risk reduction the incentive is created. There are numerous other ways in which ministries and regulators can encourage organizations to cooperate, including inviting them to be part of the CERT expert groups.

A checklist might include the following:

- **Information sharing** – many parties to cyber-attack do not wish to publicize the fact which makes detection and identification of vulnerabilities more difficult. There may be a case for mandatory reporting, even if this involves confidentiality issues. A telecoms regulator, for example, should be informed immediately of such breaches in security and be appraised of remedial measures to safeguard the facility.
- **Awareness sharing** – many private companies, including vendors, have professional expertise in how to manage network security and also how to manage the managers. The weakest link may not be a piece of software coding, it may be the staff who open a malicious email or visit an entrapment website. Regulators may wish to set

[102] "For instance, companies operating critical infrastructures have integrated control systems with the Internet to reduce near-term, measurable costs while raising the risk of catastrophic failure, whose loses will be primarily borne by society." Tyler Moore (2010) 'Introducing the Principle of Cybersecurity; Principles and Policy Options' Harvard University: *Proceedings of a Workshop on Deterring CyberAttacks* http://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf

up their own unit to encourage education campaigns, and create expert groups to advise on new threats and new responses.

- **Strategic Coordination** – to be successful in anticipating and reducing the risk of cyber-attacks and cybercrimes national security agencies need to work closely on a multi-agency level with each other and with regulators from telecoms, from banking, and even from education ministries, etc., on permanent advisory and working group levels and with expert advice from the private sector.
- **Law enforcement** – regulators have their own areas of law enforcement under legislation. In many cases they can initiate a legal process, but in the case of cyber-crime the role of the regulator is more likely to coordinate with law enforcement agencies. The best approach of a telecoms regulator is to broker information sharing between licenced companies and cyber security experts.

3.8.4 Securing E-Commerce and a Public Key Infrastructure (PKI)

E-commerce is a vital part of the digital economy, not least for cross-border trade. To make it work, confidence is required that the person or company at the other end of the transaction is genuine, that the delivery of payment and of goods will take place in the way and time agreed, that the transaction cannot be repudiated once the contract is signed, and that the laws of the land will protect and safeguard rightful transactions.

Public Key Infrastructure

To meet this challenge the ITU-T (previously the CCITT) adopted the X.509 protocol proposed by the IEFT (Internet Engineering Task Force). X.509 is an authentication protocol consistent with IP/TCP and complements X.500, an earlier pre-Internet protocol of the ITU-T and the ISO (International Standards Organization) designed to allow access to directories of “distinguished names” meaning access to unique identifiers. The cryptology behind these standards is for an asymmetric exchange of keys (private and public keys) and symmetric opening of documents (the same document received as sent). The private key is used to lock a document and the public key, which is uniquely linked to the user’s private key, is used to unlock the document. In the public version both keys are issued by a trusted third party Certification Authority (CA) which provides certificates of authenticity of the link, of the signature and of the integrity of the document to show it has not been altered or tampered with in any way. The CA itself refers to a Registration Authority (RA) to validate the identity of the user and to a Validation Authority (VA) to validate the digital signature which is applied to the document by a hash key function.

Private keys can be issued to individuals or to corporate bodies or linked to an email address. A root certificate is issued to govern all subsequent certificates issued on behalf of a given user. The certificates will include a unique serial number and other information, for example the range of dates during which the certificate is valid or a ceiling value for a transaction.

The recipient of an encrypted document gets the sender's public key from the CA, and needs to check the certificate and also check a registry of revoked certificates. A list of the root certificates are stored on a user's computer for easy search using Online Certificate Status Protocol or OCSP by which the browser dynamically checks the CA's CRL (certificate revocation list) and updates the computer.

Private PKI

The most widely used private versions of PKI are "light" versions that have been developed by Internet companies, some of them based upon peering arrangements by-passing an independent CA. Netscape in the 1990s developed SSL (secure socket layer) protocol indicated by "https" whereby servers and clients exchange certificates for mutual authentication.[103] Most modern browsers embed copies of root certificates from CAs in their software and are members of the CA Browser Forum (CABForum) along with the independent commercial CAs themselves.

Applications of PKI

There are many industrial applications that use variants of the PKI system, for example, M2M meter-reading systems to ensure authenticity of the reading and of the client. However as the technologies advance, security concerns advance with them and the behind-the-scenes fixes become more complex.[104] Bogus companies managing to fool RAs and CAs into issuing of certificates is one such problem and it is the responsibility and liability of the user to browse certificates for reputable and genuine trading partners.

Consumer Security

At the consumer level, various security devices are available from banks, credit card companies and third party payment platforms to give confidence to making purchases online. None of them are perfect, especially over time as the technology advances which, when in the wrong hands can be used to decrypt encrypted documents, intercept text messages, hack into computers to steal passwords, etc. Despite efforts in some countries to promote PKI among the general public, for example the iGov Philippines project,[105] consumers in general have shown little interest as the alternatives have fewer overheads for the scale and frequency of the transactions they usually undertake.

A terminological issue is here worthy of note: e-government is an important way to serve the citizens of a country and *as citizens* people have to pay their taxes and claim their benefits, make appointments and applications, request personal health information, and generally have access to important public information. Citizens *as consumers* are engaged in

[103] Other PKI standards are listed at http://en.wikipedia.org/wiki/X.509#PKI_standards_for_X.509

[104] A useful review of complexity can be found at: http://resources.infosecinstitute.com/understanding-pki/

[105] http://i.gov.ph/services/?id=pki

strictly private activities and online businesses have developed their own security protocols which may or may not be compatible with PKI. Most governments also tend to follow these more consumer-friendly Internet compatible protocols but often add their own layer of security by requiring citizens to pre-register their identities.

PKI Complexity and Mutually Recognized Electronic Identification

Because public authorities have a responsibility to be transparent and protect taxpayers money they have been the ones to adopt a public key infrastructure. Private corporations often use other means to secure contracts and payments between themselves, but when they deal with public authorities they are often required to use PKI where large contracts are involved. The aims of a PKI system are to ensure at minimum:

- Electronic identification (ID)
- Authenticity of the ID link
- Authenticity of the electronic signature
- Integrity of the document
- Certification of validation of the above
- Legal acceptance of certificates for non-repudiation

To achieve these aims across borders is particularly challenging. For example, private companies and citizens of the EU stand to benefit if cross-border transactions can use the same standards PKI system. This is noted in the preamble to the Regulation of the European Parliament and Council on electronic ID.

> For example, giving the opportunity for a student to enroll electronically in a university abroad, to a citizen to submit tax declaration online to another Member State or to a patient to access his or her health data online. If there is no such mutually recognized electronic identification means, a doctor will not be able to access the patient medical data needed to treat him or her and the medical and laboratory tests that the patient has already undertaken will have to be repeated.[106]

Establishing a strong legal environment through a digital signatures act or e-commerce legislation is therefore of vital important for commercial confidence, especially for foreign trade. One of the biggest challenges is establishing in which jurisdiction authority resides and which sets of laws and arbitration principles will apply in cases of disputes. Other major challenges are to harmonize standards, which is especially difficult when new standards are being adopted at regular intervals, and making sure new standards are backwards

[106] http://ec.europa.eu/information_society/policy/esignature/docs/regulation/com_2012_2038_en.pdf p.4

compatible with older standards is a further challenge.[107] PKI is therefore always going to be work-in-progress.

[107] See for example issues with different revisions of X.509 http://www.ietf.org/rfc/rfc5280.txt

Module Three: Law and Regulation for a Broadband World

3.9 Privacy and Data Protection in an Interconnected Environment

The right to privacy has been a long established principle in many countries, enshrined in laws and often in the Constitution of a country. For example, of many in Latin America,[108] as *habeas data* or the right of a citizen to own their own data.

The challenges arise from four major sources. First, in the case of *habeas data*, the right can only be exercised *after* the event when the information has already been made public. Second, the capacity of the legal system to uphold the rights of the individual and enforce the law is not always adequate. Third, the laws are often specific to particular sectors, such as telecommunications, the media, health services, legal services, government agencies and they do not lay down what lawyers call the general 'principles of purpose' that can be applied across the board. In the absence of such a generic law, regulations governing consumer protection provide some safeguards. Fourth, laws and regulations enacted before the Internet era need revision and updating.

The question is how to apply personal data privacy principles to an interconnected digital world of the Internet. This is especially challenging when information can be gleaned from a whole range of digital sources such as social media, email servers, websites, blogs, online purchases, online inquiries, etc., by persons and companies who are often located outside the jurisdiction in which the citizen resides; when feeds to sites such as Facebook, Twitter and YouTube can go viral within minutes; when 'Big Data' and business analytics can be used to match and correlate people, ideas, actions, postings, etc., in both text form and in image. This means that laws prohibiting the identification of individuals may no longer work.

New laws, regulations and codes of practice must aim to balance the interests of individuals who have a right to privacy with the social benefits of a growing digital economy. In an interconnected world anything online can be located anywhere on the planet, and with the rise of cloud computing and PaaS (Platform as a Service), SaaS (Software as a Service) and IaaS (Infrastructure as a Service) anything online can, in principle, be transferred between countries. This is not a by-product of the rise of a digital economy, it *is* the digital economy.

3.9.1 Date Protection and the Principles of Purpose

A key principle of *habeas data* is the right to own or know and control what information is being gathered and stored about you and by whom and for what purpose. This right carries

[108] Argentina, Brazil, Columbia, Ecuador, Honduras, Panama, Paraguay and Peru all have *habeas data* as a constitutional right. See *International Law News*, (Fall, 2012) v.41.4 http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html

the implication of the right to demand corrections or possibly even to delete the information, which is also known as the 'right to be forgotten'. Personal information usually refers to information that can be used directly or indirectly to identify a 'natural' living person, although in a digital age there is very little that cannot be used to traced back to a living person. There is a further issue of who has the right of ownership, if anyone, over information of a deceased person. This means that the drafting of new laws or regulations or codes of practice needs to be flexible to changes in technologies and proportionate to the level of harm that can accrue from inaccurate information or lack of privacy.

By 2013, over 90 countries had some sort of Freedom of Information legislation,[109] the earliest dating back to 1766 in Sweden, but mostly these laws only apply to information held by the State, not the private sector. In that regard they do not fully enable the *Universal Declaration of Human Rights* adopted by the UN General Assembly in 1948 which states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

More recently many countries have introduced personal data privacy legalisation which extends to the private sector. These laws go beyond existing laws on consumer protection that provide the right of customers to fair contract conditions rather than unreasonable tie-in contracts, return of impaired goods, protection against price gouging, the right to itemized billing, and so forth. Consumer protection of this sort has been particularly prevalent in the telecommunications sector. Under new data protection laws, the data 'controller' of the information (the agent of the company collecting the information) as opposed to the data 'processor' (the sub-contractor who may store, transfer or manage the data) is required to seek the 'informed consent' of the individual, either through an opt-in or an opt-out procedure, and a statement on how the data may be used is necessary, with the understanding that it cannot be retained once the original purpose for its collection has been fulfilled. Web-based enterprises are required to state their policy towards 'cookies' and offer the user a way to agree to accept them or to disable them.

Balanced against these requirements to protect the individual are certain public safety requirements. For example, Internet access service providers such as Google and Yahoo! and social media companies may be required to retain email traffic and postings for up to two years or more to provide a trail of traceable evidence. Especially after the 9/11 attack on the World Trade Center in New York, law enforcement agencies have been much more concerned to have access to digital communications, but this will only be acceptable to the public if there are strong safeguards in place. This means the public must have faith in the quality and integrity of the legal process in their country. It also means that the

[109] For a list, see http://home.broadpark.no/~wkeim/foi-list.htm

enforcement of such policies has to cross jurisdictional boundaries and that raises questions of which laws are enforceable on, for example, a company that has multiple global locations. The most common legal wrangles tend to be over tax liabilities, but take-down notices, defamation suits, compliance orders and other legal tussles add up to the need for international cooperation even when the laws of different countries are not in harmony with each other. This becomes especially important in cases of national security and serious crimes such as child abuse and trafficking.

Data Protection Laws

By 2013, some 89 countries had adopted privacy or data protection laws. The European *Data Protection Directive* of 1995 was the first pan-European policy document in which the concepts of personal data protection in a digital world were embodied in legislation. It was followed by the *e-Privacy Directive* of 2005, revised 2009, which deals with digital communications and issues such as the integrity of data traffic, giving users ways to reject spam and to control cookies. Under the 1995 *Directive* companies may not move personal data, for example store data, to jurisdictions that do not have legislation that conforms to the standards set by Europe. This becomes important with the rise of cloud computing which technically allows data of any kind to be stored, processed and retrieved from any Internet location in the world.

A revised EU draft European Data Protection Regulation was proposed in 2012 which will extend applicability of the Directive to non-EU entities outside the EU when the data involved concerns EU citizens, will impose an ‘opt-in’ rather than an ‘opt-out’ requirement to ensure personal rights to data are fully protected, will allow for a ‘right of portability’ and a ‘right to be forgotten’ which will allow citizens to wipe out the history of their data, and strict conditions on notification of breaches in data protection and penalties for non-compliance. A further enhancement of citizen rights are anti-spam regulations, typically a Do-Not-Call (DNC) register which can also cover Do-Not-Send (DNS) in the case of phone text messaging, and a proposal in the US for a Do-Not-Track (DNT) web function as part of a wider package of consumer rights as proposed in the *Consumer Privacy Bill of Rights* brought before Congress in 2012.[110]

The US approach to data protection is generally less proscriptive. The Federal Trade Commission (FTC) has overall responsibility of supervising the enforcement of federal requirements on different sectors of the economy, such as the way information is collected and used about customers by telecom companies, confidentiality of health records, inland

[110] According to a Consumer Insights survey by Ovum “an average of 66% of the Internet population across 11 countries would select a “do not track” (DNT) feature if it was easily available…” ‘Little Data: big data’s new battleground’ http://ovum.com/2013/01/29/little-data-big-datas-new-battleground/

revenue data, etc., and to generally apply consumer protection regulations. But there is no prevention on the international transfer of data except tax records.

The threat of disrupting cross-border trade from a mismatch between the EU rules-based approach the more voluntary approach to the private sector in the US was averted in 2000 when the EU approved the US seven 'Safe Harbor Principles'[111] which allow for company self-certification:

- **Notice** - Individuals must be informed that their data is being collected and about how it will be used.
- **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security** - Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** - Data must be relevant and reliable for the purpose it was collected for.
- **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- **Enforcement** - There must be effective means of enforcing these rules.

However the emphasis in the US shifted significantly following the 9/11 terrorist attack towards greater state security and the need to assess and share information and the passing of the *Patriot Act* in 2001. This, together with some doubts about how effective self-certification really is, has kept the harmonization of approaches an open issue.

3.9.2 Cross-border data and cloud computing

One of the earliest set of policy recommendations on cross-border transfers of data arising from the computerization of business transactions was the OECD 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information.* [112] More recently, the rise of cloud computing has made it imperative that countries introduce updated personal data protection legislation that conforms to minimum safeguards, for example, to those enshrined in the EU *Directive*. For cloud computing to become a truly global means of data storage, retrieval, file sharing and data transfers under secure conditions there needs to be universally acceptable standards that at minimum allow for interoperability, otherwise the 'clouds' will remain constrained by economic and political boundaries. As a report from Cisco in 2009 pointed out "Special consideration must be given to using cloud computing to

[111] The Federal Trade Commission (FTC) is responsible for monitoring certificates under the SHPs

[112] http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

handle information that is vital to national security, to maintaining public trust and confidence in government, or to managing certain core government functions such as foreign relations, maintenance of property rights, law and order, and defense."[113]

There are two approaches to holding companies responsible for safeguarding confidentiality in cross-border data traffic. The EU approach is geographical, so data is allowed into countries that are deemed to meet the minimum standards set by the EU *Directive*. In reality, this has not stopped data crossing borders into some major economies such as China and Japan, despite the EU not having determined the adequacy of safeguards in either country. The alternative approach adopted by APEC and by Canada among others is based upon accountability. For example, Singapore's *Personal Data Protection Act* of 2012 places accountability on the shoulders of the 'data controller' which is the company that authorizes the collection of the data even when the actual collection or handling of the data and the storage and retrieval of the data is undertaken by a subcontracted 'data processor'. This can be seen as a more flexible approach that skirts around the country-profiling required by the EU and keeps the responsibility on the data controller wherever the data is transferred to and whoever handles it.[114] The ultimate market test will be whether international companies and their clients are willing to trust locating data in countries with the accountability approach.

Latin America

The need to update and add flexibility to data protection laws is driving the shift in most Latin American countries from a *habeas data* approach to a legislative approach, mostly based upon the EU Directive but largely without the EU rules on data retention which suggests less of a priority given to cyber-security issues.[115] Several factors may account for this, for example, a public wariness towards state surveillance, a lack of public awareness, a lack of cyber-crime experience by law enforcement agencies, and a slower pace of development of private cloud computing as much of the take-up has been e-government. But as the digital economy of Latin America grows with the spread of broadband access and traffic the need for more explicit data protection regulations and codes of practice will emerge. As of 2012, the only countries in Latin America not to have some form of over-riding personal data protection legislation were Bolivia, Cuba, Dominican Republic, El Salvador, Guatemala, Nicaragua and Venezuela. Progress towards such protection has being

[113] Russell Craig et al. (2009) *Cloud Computing in the Public Sector: Public Manager's Guide to Evaluating and Adopting Cloud Computing* http://www.cisco.com/web/about/ac79/docs/wp/ps/Cloud_Computing_112309_FINAL.pdf

[114] See ITU *Trends in Telecommunications Reform, 2013* chapter 7.

[115] As of 2012 only Argentina's approach has been recognized by the EU as meeting the minimum standards of the EU Directive, see *Cloud Times*, 'Data Protection of Privacy Issues in Latin America' 21 November 2012 http://cloudtimes.org/2012/11/21/data-protection-privacy-issues-latin-america/

going on for more than a decade promoted by the Ibero-American Network of Data Protection (RIPD), created in 2003, and now has over 20 member states.[116]

Asia Pacific

In countries of the Asia Pacific region the situation varies.[117] APEC's *Cross Border Privacy Enforcement Arrangement* [118] adopts the accountability approach rather than the geographical approach which perhaps reflects the emerging status of many of the economies involved and the need for a flexible regime of data protection to benefit from the rapid growth of cloud computing and data centre managed storage, retrieval, processing, security and transit business throughout the region.[119] In Asia Pacific countries, such as Australia and New Zealand, Hong Kong and Singapore, and the Philippines clear cut data protection laws are in place. In Japan the *Act on the Protection of Personal Information* (APPI) provides a degree of protection covering data on employees, while ministries such as health, education and labour have issued non-legally binding sets of guidelines based upon APPI. The central administrative authority is the Consumer Affairs Agency. South Korea enacted the *Personal Information Protection Act* (PIPA) in 2011 under the authority of the Minister of Public Administration and Security (MOPAS) but also has legislation governing particular sectors, such as financial sector and the *IT Network Act* administered by the Korea Communications Commission (KCC). Taiwan revised the *Computer Processed Personal Data Protection Law* (CPPL) to become the *Personal Data Protection Law* (PDLP) effective from 2012, but no separate national data privacy authority has yet been established. Indonesia brought together different references to data protection and privacy under a Government Regulation No. 82 of 2012 regarding *Provision of Electronic System and Transaction*, and also has sector legislation, for example governing telecoms. Beyond these cases, other countries of the region have yet to pass general personal data privacy laws or to set up privacy commissions, relying upon legacy legislation governing telecoms, finance, health and other sectors. But the Ministry of Industry and Information Technologies (MIIT) in China in 2013 for the first time issued a public consultation of a non-binding code of practice.

Africa and the Middle East

Throughout Africa and the Middle East there is no country that has an all-embracing data protection policy. In most cases in Africa privacy is a constitutional right and in Malawi, Namibia, Tanzania and Zambia this includes the right to privacy of communications, but only

[116] RIPD http://inicio.ifai.org.mx/English/6%20Background%20of%20the%20RIPD_English.pdf

[117] DLA Piper *Data Protection Laws of the World*, March 2013 http://www.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf

[118] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

[119] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Angola, Mauritius and Zimbabwe have enacted a separate data protection act and South Africa has one pending. In some cases, such as Mauritius, Namibia, South Africa and Zambia, privacy rights are included in their e-commerce legislation. Most countries in Africa do have a freedom of information act but none has an independent commission to oversee the privacy rights of individuals. In most cases there are regulations governing particular sectors, such as spamming provisions. An important aim of policy makers in Africa should be towards the harmonization of laws on data and personal privacy as a way of attracting investment in data centres and in cloud computing services by making it easier and safer to move data across borders. This was one of the objectives of the ITU's programme 'Harmonization of the ICT Policies in Sub-Sahara Africa' [120]

In the Middle East the situation is similar with few instances of separate personal data privacy laws. Two exceptions are laws governing the Dubai International Financial Centre and the Qatar Financial Centre which are modelled on the EU Directive. Qatar and Oman also have e-commerce laws including provisions for digital signatures based upon the UN's UNCITRAL Model Law on Electronic Signatures.[121] Historically, separate laws and regulations governing telecoms include provisions for the protection of customer data and prohibitions on the illegal interception of communications. Examples in the Middle East include Saudi Arabia, where the Telecommunications Act also covers Internet services, and Oman and the UAE where the telecom regulators have issued data privacy policy requirements including restrictions on unsolicited messaging. The electronic commerce law in Qatar does the same. But none of these countries have independent privacy commissions. Beyond the Gulf states, few other Middle Eastern countries have data protection laws. The privacy law in Lebanon, for example, covers individual persons but not the content of communications.[122] It has been pointed out that the concept of privacy in Middle-Eastern countries is often more a cultural than a legal concept, referring to the privacy of women and the household rather than to individuals and information, and often the policy emphasis is more upon blocking access to information, especially information over the Internet, rather than on protecting personal data privacy. It is difficult to see how such policies can be consistent with the growth of a digital economy and transformative technologies such as cloud computing.

3.9.3 Awareness and Alertness

As with cyber-security, so with personal data protection, in an interconnected world there are no guarantees of privacy. To reduce the risks of unauthorized leaks of personal data, or more seriously of identity theft, the number one and two issues are awareness and alertness. The former relies upon frequently available updated information about the

[120] http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/

[121] See UN Commission on International Trade Law http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

[122] http://isper.escwa.un.org/Portals/0/National%20Profiles/2011/English/Lebanon-11-E.pdf

dangers and risks involved and of the need for adequate protection, from laws and regulations (the 'rights') and from the practices used by data controllers (the potential for 'wrongs'). A good example comes from the frequent changes in the privacy rules of social media sites and user reactions to them, which is often to switch to other social media. Where there is a real choice in the market, customers have real market power. Therefore, one of the aims of an information campaign should be to give meaning to the term 'informed consent.'

Alertness calls for self-aware and sensible behaviour by users. Often this comes with experience as for example when a regular user of email has a sixth sense that an incoming email is malicious and should not be opened or replied to and a web-link should not be clicked on. On the other hand, fraud, sexual grooming, the release of passwords, all happen all too often on the Internet because users are not careful or not controlled enough. So both helpful information and education about sensible behaviour and etiquette on the Internet are topics that policy makers and regulators can be pro-active about, especially if they work closely with industry. Activities can include running safety and cyber-security workshops, seminars and competitions, school and college visits, webinars and websites, and recruitment of young volunteers to participate in peer-to-peer knowledge-sharing. Making 'Safer Internet Day' (SID) a big occasion will help.

Regulators should also take steps to update themselves and keep abreast of fast-moving software developments, such as Privacy-Enhancing Technologies (PETs). As well as advising users about these advances, regulators can review the adoption of security measures by data centres and cloud computing service providers. In some industries, such as telecoms and finance, reporting on their use could be part of a code of practice.

3.9.4 International Enforcement and Policy Cooperation

International cooperation and enforcement of privacy and data infringements can take place through various mechanisms, including bilateral and multilateral efforts, through more structured international organizations such as Interpol and through a mutual legal assistance treaty (MLAT) between countries for the purposes of exchanging data and information on legal and security issues.[123]

See the reference to MLAT above. Given the many different approaches and laws reviewed above, it has been suggested that using the EU Directive as a general guideline is a good way to ease data transfer issues, but even though this may bring recognition that cross-border data transfers are acceptable it will not solve all the problems. Law enforcement will still be necessary, especially when serious crime is involved.

[123] For a list of MLATs see http://www.legislation.gov.hk/table3ti.htm

There are several global and regional privacy and data protection organizations in addition to law enforcement cooperation agencies such as Interpol. The Global Privacy Enforcement Network [124] was started in 2010 following the adoption in 2007 by the OECD Council of the *Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy*[125] which provided that

> "[m]ember countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns."

By 2013, GPEN had 27 participating authorities, but none in Africa or the Middle East or Latin America, and only Australia, New Zealand and South Korea in the Asia Pacific. As with so many inter-government organizations, GPEN has a website that is restricted entry which rather misses the point that open access is the way to encourage participation in an interconnected world. However, countries who are members of the Asia Pacific Privacy Authorities (APPA) receive regular updates in GPEN activities,[126] and invitations to the annual International Conference of Data Protection and Privacy Commissioners.

Even where privacy commissioners and national agencies for data protection have not yet been established, policy makers and regulators should consider establishing liaison points to support national initiatives in this direction and regular attendance at these security forums. In other words, policy makers and regulators should themselves practice awareness and alertness to become more effective as catalysts in society and industry for greater personal and public safety.

[124] https://www.privacyenforcement.net/public/activities

[125] http://www.oecd.org/internet/ieconomy/38770483.pdf

[126] http://www.appaforum.org/resources/communiques/38thforum.html

Module Three: Law and Regulation for a Broadband World

3.10 Content over Broadband

The delivery of content, mostly as video, over broadband is one of the key drivers of demand for broadband over fixed lines and by wireless. The days of FMS (fixed-mobile-substitution) are already history as content can now be delivered to multiple devices, from Internet high definition 'connected TVs' to handheld mobile devices of all kinds.

This is both a challenge and an opportunity for telecom companies who mostly own the networks. By caching content at vantage points within their networks they can become wholesale content distribution networks (CDNs) offering content service providers a guaranteed quality of service that may not be available over the Internet. Their billing relationship with customers and their knowledge of the local market are competitive advantages to them. They can also deliver their own content and applications, but content creation and applications innovation is not the traditional core competency of telecom companies.

Regulators on the other hand face more of a challenge than an opportunity, apart from an opportunity to get it right. It is to be expected that telecom companies baulk at the idea of content service providers, independent CDNs or Internet access providers by-passing their networks by going Over-The-Top (OTT). The only gain for the telecom company is that this drives the demand for broadband and for higher speeds, for which they can charge customers a fee. But against that they fear to lose revenues, especially from traditional voice and SMS services for which OTT provide substitutes. How should regulators react to the lobbying of telecom companies wanting to preserve their traditional core business? The net neutrality debate in part already addresses this question, with the consensus of non-carrier content providers being predictably against the right of telecom companies to block or throttle or degrade content services which are not their own. This is also likely the position favoured by most consumers.

The Challenge for Regulators

The challenge for policy makers and regulators is really twofold. How to ensure that there will be sufficient investment in networks to maintain a steady level of innovation and upgrade in broadband for society, and what laws and regulations to apply. The first challenge is best addressed through opening the market to new entrants who are willing to invest in networks. The fear that network owners will not be able to earn a sufficient rate of return on their investment is really a fear that they will not be sufficiently adept and flexible in the market to find new business models that work. Protection of incumbents is the guaranteed way to make this fear real as rent seeking replaces competition.

The second challenge is actually the greater one. Pre-dating the Internet was cable TV as an alternative to free-to-air (FTA) and Pay-TV broadcasting. The problem for regulators was that cable was a wired-based medium and not a radio-based medium like broadcasting, so it was close to being a carrier, and indeed could be adapted to carry telephony and when upgraded to digital to providing Internet access. It also became a competitor to IPTV provided by carriers. In different jurisdictions it was handled in different ways. In the US, where cable, like the Internet, really started, the Communications Act of 1934 applied to carriers and broadcasters under different parts of the law leaning heavily on the fixed line and radio distinction, so the powers of the regulator over cable became a question of legal interpretation for the courts. The courts decided that the law gave the regulator "ancillary" powers to protect broadcasting and so cable regulations were mostly derived from the impact cable would have on broadcasting, for example, threatening its advertising revenues.

In one case the court went further and upheld the FCC's requirement that cable operators should contribute to local content production through "mandatory origination" to achieve public service goals not being adequately fulfilled by the broadcasters. A change of stance by the FCC in 1976 repealed this requirement and replaced it by a new "access" requirement whereby cable operators had to provide equal access to public, educational and government services and to lease capacity to unaffiliated third parties. After some legal wrangling, these conditions were embodied in the 1984 Cable Act.[127]

Box 3.11

Star TV in Hong Kong, SAR (China)

As in the USA, protection of FTA broadcasters was the initial reaction of the regulator in Hong Kong to as independent new entrant to broadcasting.

In 1988 a company was formed to launch Star TV, a regional satellite TV broadcasting service out of Hong Kong. Viewers could receive the signals through a C-band dish attached to a cable distribution system. Before a broadcasting licence could be issued Star TV was challenged by the Broadcasting Authority (BA) to prove that it would not compete directly with local free-to-air broadcasters ATV and TVB and would not diminish their share of the market and their advertising revenues. Star TV had to reassure the BA that its target market was regional, not Hong Kong, and it would not be broadcasting in Cantonese, the local majority Chinese language of Hong Kong. On this basis Star TV was allowed to start regional operations in 1991.

The same line of reasoning was used in Hong Kong in the early 1990s as in the US with the regulation of cable TV. Government had licensed FTA broadcasters to provide programmes

[127] Michael Botein (2013) 'FCC Jurisdiction Over Internet and Broadband' New York Law School Legal Studies, Research Paper Series 12/13 #66 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2241621

for a mass public TV audience and regulations were designed to protect them. But technologies rapidly outdated this regulatory stance. First came a licence for Wharf Cable TV which, being a subscription service, was seen as less of a direct competitor to FTA. Then the incumbent carrier, Hong Kong Telecom (HKT) was permitted to launch a Video-on-Demand service again as a subscription service. This faltered, but was successfully resurrected in the 2000s as NOW TV, an IPTV service using DSL broadband. At the same time a new entrant Hong Kong Broadband was licensed to launch a web-based TV service. The 2000s then witnessed the rapid development of video content over broadband wireless access (BWA) using 3G and more recently 4G and WiFI to smartphones and tablets. The latest twist to the story is that with the shift to digital TV the FTA market is now being opened up, although not before an unsuccessful legal challenge by the larger of the two FTA broadcasters.

The telecom and broadcasting regulators have been merged into the Office of the Communications Authority (OFCA) and the cross-overs between OTA and over cable, over broadband, over BWA and over the Web to multiple receiving devices have transformed the market out of all recognition. In just two decades the challenge of regulating content over broadband makes the policies and regulations of the early 1990s seem like another era altogether.

As a consequence the Broadcasting Ordinance has been revised, with the distinctions between technology means of delivery fading into the background, the key distinctions now being whether the broadcast is free or subscription, and whether designed for a domestic or a non-domestic audience as these are the criteria that most closely reflect the impact of TV on Hong Kong society. Where the broadcast or the distribution originates in Hong Kong these services require a licence and the Ordinance tries to protect licensed services by outlawing a class of decoders designed to break the encryption of signals, but this is another area in which technologies make the law difficult to apply in a comprehensive manner. And with more OTT content becoming available, even decoders tend to become part of history.

Other forms of regulatory oversight include ownership restrictions on disqualified persons or parties, cross-ownership restrictions to maintain competition and diversity of programming and opinion, separations accounting between affiliated companies, and codes of practice to restrict undesirable content or content at inappropriate times of broadcast. Licencees are prohibited from broadcasting content that is likely to “(a) incite hatred against any group of persons, being a group defined by reference to colour, race, sex, religion, nationality or ethnic or national origins; (b) result in a general breakdown in law and order; or (c) gravely damage public health or morals.” [1] The Ordinance provides for an appeals process and the courts of law rather than the regulator to be the ultimate arbiter.

[1]. http://www.wipo.int/wipolex/en/details.jsp?id=6337

Broadband and the Internet now pose similar challenges to those thrown up by cable TV for the FCC. In the US the Internet had been treated by the FCC not as a carrier service but as an information service. However, in April 2010, in the case of Comcast Corp. v. FCC, the United States Court of Appeals for the District of Columbia decided that the FCC does not have ancillary jurisdiction over Comcast's Internet service under the language of the Communications Act of 1934, as amended. (See Module 3.7.1). The FCC has also traditionally defined other substitutes for carrier services, such as VoIP, as “enhanced” services and therefore not subject to the same regulations as “basic” services. But these definitions are really driven by their implications. A decision to encourage innovation and allow a new service to flourish is served when the service is treated as unregulated or regulated very lightly. The problem with defining according to traditional “basic” and “enhanced” or “value-added” is that all telecom services are “value-added” including voice, because without the transmission mechanism there would be no communication. And if it were not adding value then no one would pay for it. The shift in regulatory perspective in recent years has been away from these technologically-differentiated definitions, which really have no objective basis to them, and towards technology-neutral and economic regulation.

As with cable TV, Internet-based services cut across the technological separations of carriers and broadcasters, including the fixed-wireless divide. But there is another separation that has become increasingly blurred, the one between apps and content. The spread of P2P communications using web-based applications, such as ‘torrents’, means for example, it is possible to download different parts of a movie or video from many different servers over a period of hours, or within minutes with fast enough broadband. Downloading a health check app similarly provides the user with health care content, or an education app allows a user to access education content and so on.

Most of these apps and the content they provide access to are provided by third parties. They can be delivered by third parties. They are part of a vibrant digital economy. But they can represent a challenge to the social norms and culture of a society and sometimes a security risk. For example, in May 2013 an Internet posting in the USA provided a video of a gun made from plastic by a 3D printer which was rendered legal under the *Undetectable Firearms Act of 1988* by having a piece of steel inserted into the body of the gun to make it evident to a metal detector.[128] The State Department demanded temporary take-down due to a possible breach of the *International Traffic in Arms Regulations*, but this may not apply to the Internet if it is judged by the courts to be a “library” of information.

[128] http://www.guardian.co.uk/world/2013/may/06/3-handgun-fired-cody-wilson

What Lessons?

Whatever the outcome of this particular case it is a good illustration of the many new challenges to policy and regulation that content via the Internet throws up. So what lessons can be drawn? The first is that in an interconnected world in which content can go viral within minutes, and in which proxy servers can be used to by-pass national restrictions, the law may not be a very effective means to control content. The second is that, rather like the war on drugs, the most effective interventions are likely to be at the user end. At the benign end of the scale are awareness and alertness campaigns and the use of Internet filtering apps by parents and guardians to protect children.

At the other end of the scale is the use of the law. For example, it may be impossible to prevent the uploading of child pornography somewhere in the world but cyber-detection and law enforcement can identify users and break-up the crime rings that supply them. However when the law is being used, the principle of proportionality is important and this is mostly to be judged in terms of two factors: whether the intent itself was criminal or not and the social impact of the infringements weighed against the rights of the individual of freedom of access to the Internet.

3.10.1 Freedom of Opinions and Expression

In 2012 the United Nations General Assembly accepted a report from its Human Rights Council that, among other things,

> *Affirms* that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights; [129]

The Universal Declaration of Human Rights is a statement of human design. Societies make choices, and the recognition of a 'human right' as a universal principle is an inherent part of a democratic tradition whatever form it takes. The idea of a 'human right' hinges on the fact that people will naturally demand it when they have the opportunity. While it cannot be said that everyone in the world agrees on democracy and human rights, what can be asserted with good reason is that global forces for change such as interconnected broadband and the Internet, which can do so much to alleviate poverty, illiteracy, poor

[129] UN Human Rights Council (2012) 'The promotion, protection and enjoyment of human rights on the Internet' http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

health and other social ills and so much to improve the overall wellbeing of society, are not compatible with too many restrictions on the freedom of expression, and not at all with the efforts to restrict the freedom of thought.

It is important to stress these points as a guideline, because the challenges are very real. Getting the balance right between freedom of expression and freedom to access and to use the Internet on the one hand, and protecting society from serious problems is never going to be an easy one to achieve, nor if achieved will it remain in balance forever. What the UN Declaration of Human Rights provides is a good reality check on proportionality, on what that balance should look like.

No society can be absolutely safe, no society can be absolutely free, but every society can be resilient if the great majority of people are convinced of the goals. Different societies have different priorities, different needs, enjoy different cultural traditions, and the resilience of every society will be determined by how far they can adjust to these global changes. The role of the Internet in giving ordinary people a voice cannot be over-estimated and regulators have an important role to play one way or the other. Social media in particular represents a genuine opportunity for user-generated news and analysis and is having repercussions throughout the world.

But there are clouds on the horizon as every action causes a reaction. At the highest levels there are serious debates about Internet governance and what should be the respective roles of governments and civil society. This has become a controversial issue among member states of the ITU for example, where some members argue a need for greater state involvement and others see this as a dangerous way to rein-in freedoms on the Internet. There are also pressures on social media organizations to exercise some degree of editorial control over what appears on their sites. In some cases this is really about content that may be considered extreme and harmful to society, such as the spreading of race or religious hatred or homophobia or gratuitous violence. In other cases it may be about clamping down on freedoms of expression and information. For example, at times in during the Arab Spring in some countries the regulator closed down mobile networks and occasionally the Internet also became unavailable. In emergencies such extreme actions might reduce the immediate likelihood of violence, or they might be an act in a political conflict that only exacerbates tension. The cost of such actions is to reduce transparency and the free flow of information.

Policy makers and regulators should therefore bear two things in mind. First, what are the social consequences and implications of taking or not taking action and is this better left up to the courts of law. Second, are the actions being proposed designed to strengthen and safeguard social freedoms, or simply to serve and protect vested interests.

3.10.2 Regulating Specific Forms of Content

As the case of Hong Kong illustrates, the old distinctions between content and content channels is breaking down. Under the traditional approach, regulators would rightly see FTA broadcasting as having the greatest social impact and therefore the regulation of content considered inappropriate was more strictly applied. Subscription channels reached smaller audiences of self-selected viewers, and in the early days of the Internet receiving content online was limited to highly specialised users. Those distinctions are rapidly losing their validity. People of all ages can access virtually any content over the Internet, some of it highly disturbing, using a mobile phone.

In a sense, all channels are equal, it's just that some are more equal than others. Most families have TVs, and most individuals have mobile devices. In some countries broadband is widely available, in others not, but it is only a question of time and the availability of high speed broadband is the driver of these content channels. The supply of content is also becoming diversified as never before, from the big movie makers and the TV in-house productions, to the professional and the amateur videos on You Tube, to local content providers trying to become a business, to content on social media networks, to downloaded P2P content. There are no all-embracing standards for rating this cornucopia of content. Some regulators, for example in Singapore, are suggesting a code of practice by which content providers such as Internet access providers like Yahoo! will not only commit to making local content but will rate it appropriately for audience guidance.

This does inevitably raise the issue of a more libertarian approach to regulation. Exposure to family shows on TV which openly discuss issues of sexuality, mortality, and similar 'adult' themes has been a factor in changing social attitudes, and it may not be the attitudes of the young that are changing because their attitudes are already conditioned by the technologies and the social discourse of their peers around them. It is rather the attitudes of older generations that are being challenged to change with the times, the generations to which most policy makers and regulators themselves belong, and seeing things through futuristic eyes is not always easy. The point here is that it may become impossible, despite regulations, to shield society from exposure to all sorts of challenging content. Society itself has to adjust to this by becoming more resilient to these challenges, and more self-confident is meeting them. This starts with home and family and school and college environments, and regulators will perhaps need to shift their perspectives from trying to regulate what cannot be regulated to engaging more closely with all stakeholders, from providers to users, to support society in managing these challenges.

Child Safety

Of particular concern to all stakeholders of the Internet is the safety of children: in particular safety from inappropriate content, from child abuse and the dangers of sexual predators and from trafficking. There are two aspects that should be noted with particular care: online behaviour and dangerous websites. In 2010 the ITU also launched a Child Online Protection (COP) initiative, including the allocation of number 116111 for help lines,[130] and issued a *Guideline for Policy Makers for Child Online Protection*.[131] The reality is that infants below the age of five can now readily use the Internet and laws and regulations will not prevent predators, nor prevent children being able to access unsuitable material,[132] which means that at a large part of the focus must be on helping parents and guardians how to educate the children in their care to conduct and protect themselves online. Regulators also need to be aware, as ICANN has pointed out, of unscrupulous 'fast flux hosting' whereby "operators automate domain name service updates to hide the location of web sites where illegal activities – IP Piracy (music, videos, games), hosting of child pornography, hosting of phishing systems, sales of illegal pharmaceuticals, and execution of identity theft and fraud – are performed."[133] Children can very innocently find them themselves in a completely wrong environment.

3.10.3 Intellectual Property Rights

Intellectual property (IP), copyright in particular, is always an issue for Internet companies, especially in an era of user-generated content and content going viral. For example, take-down notices are difficult to enforce. The World Intellectual Property Organization (WIPO) has put in place rules addressing interoperability, a key principle behind Internet neutrality, through the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The guidelines are, however, only related and limited to the prohibition of the circumvention of certain technological measures to gain access to protected digital works.[134] Regulators and Internet companies are grappling with appropriate and effective codes of practice with regard to safe use, copyright infringements, hate content, child pornography, libel, and so on. The only effective way forward is if there is industry agreement, but often the debate becomes infused with political, social, religious and cultural deliberations which can result in unrealistic solutions.

IP issues always put policy-makers and regulators under pressure from lobby groups, and there exists a panoply of trade agreements that commit signatory countries to protect patents, trademarks, copyright, designs and geographical indicators for country of origin,

[130] http://www.itu.int/osg/csd/cybersecurity/gca/cop/

[131] http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/Draft/POLICY%20MAKERS.pdf

[132] See http://www.missingkids.com/KeyFacts for some data

[133] http://www.icann.org/en/groups/ssac/projects

[134] WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty http://www.wipo.int/export/sites/www/copyright/en/activities/wct_wppt/pdf/wct_wppt.pdf

ranging from the World Trade Agreement (WTO) which administers the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) under the auspices of the World Intellectual Property Organization (WIPO) to multilateral (MTAs) and bilateral treaty agreements (BTAs) and Free Trade Agreements (FTAs).[135] These agreements need to take into account the very different stages of economic development and administrative capacity of the countries involved. For example, the context of the 2008 Economic Partnership Agreement between the CARIFORUM Latin American states and the European Community, given in Article 131 includes the sentence:

> [The Parties] recognize that the protection and enforcement of intellectual property plays a key role in fostering creativity, innovation and competitiveness, and are determined to ensure increasing levels of protection appropriate to their levels of development.[136]

The reference to "appropriate to their levels of development" is telling for a number of reasons. Take software piracy as an example. Although more and more countries are developing a capability in software development, the economies of scale that are required to make operating systems and utility programmes commercially valid act as a brake on less developed countries. Because the price of imported software can be high relative to personal incomes in these countries the incentive for many users is to use pirated copies. Although officially frowned upon it is nevertheless widely recognized that it can be a way to kick-start an ICT market in low-income country. It is interesting to note that as China has reached an advanced stage in writing software coding, Chinese developers are among the strongest advocates of IPRs within China.[137] The same pattern of development can be expected in other countries and in other economic sectors.

Policy makers and regulators are undoubtedly under pressure to enter trade agreements to gain access to major markets, and as further rounds of WTO negotiations have faltered in recent years an increasing number of FTAs and BTAs have emerged, including the Trans-Pacific Partnership (TPP) initiative led by the USA.[138] Many contain IPR provisions which are controversial because the countries owning most IP are the wealthier nations, and economists are divided on how far IPR issues should be part of trade negotiations. These are, by definition, issues of political economy. The business of trade negotiators and policy makers is to find mutually-beneficial workable compromises, but it is important in market-oriented economies that regulators remain as far as possible neutral and honest brokers for the ICT industries under their authority.

[135] For BTAs/FTAs entered into by the EU see http://ec.europa.eu/trade/policy/countries-and-regions/agreements/ and by the US http://www.ustr.gov/trade-agreements/free-trade-agreements

[136] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:289:0003:1955:EN:PDF

[137] John Ure (2007) *China Standards and IPRs (Working Paper for the EU-China Trade Project, April 2007)* http://trpc.biz/wp-content/uploads/2007-04_TRP_ChinaStandardsIPRs_workingpaper.pdf.pdf

[138] For a list of FTAs to 1H 2013 see http://en.wikipedia.org/wiki/List_of_free_trade_agreements

Regulation and IPRs

In the ICT sector, as in other industries such as pharmaceuticals, IPRs have become a battle ground for companies in fierce competition with each other over issues such as ownership of algorithms to trade-mark designs. Whereas disputes between companies are usually civil law cases, under Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) signatory countries are required to establish criminal laws to cover cases of "willful trademark counterfeiting or copyright piracy on a commercial scale". However, often individuals can get caught up in criminal cases, and once again it is important for the sake of equity and practicality to exercise proportionality when applying the law.

One approach to online copyright violations has been the "three strikes" approach whereby the regulator issues two warnings and then applies a penalty, such as broadband disconnection, a fine or referral to a law court. France introduced a "three strikes" law in 2010 and by September 2012 the *High Authority for the Distribution of Works and Protection of Rights on the Internet* (HADOPI) had issued over 1.1 million first warnings, of which 9% were followed by second warnings of which 0.3% (14 cases) were taken to court.[139] In the first case to be heard the court imposed a fine. But critics see a danger of over-reaction to downloading when it is technologically difficult to stop, and complain that by making it a criminal rather than a civil offence public resources are used to protect private, mostly corporate, property rights. The counter-arguments include the economic impact copyright theft can have upon local content, such as a local movie industry, and theft is theft even though digital theft unlike physical theft may not deprive the owner of the original asset. As always, the arguments will be influenced by the questions of intent and proportionality and effectiveness.[140]

Other innovate approaches have been tried. For example, Google decided to offer copyright holders who could prove their content had been illegally posted on You Tube one of three options: to take down, to keep up with acknowledgement, to keep up and share in advertising revenue associated with visitors viewing the content. Needless to say, this last option has proved popular and in some cases profitable. Regulators might consider encouraging other win-win approaches.

Regulation and Openness

[139] http://www.techhive.com/article/262285/french_court_levies_first_fine_under_threestrikes_law_on_illegal_downloads.html

[140] Stealing an apple from a tree leaves behind other apples and the tree, whereas stealing a marrow that wins a prize for its size deprives the owner of a valuable asset and causes hurt. Both are theft, but the consequences differ. The law may determine liability for the action and determine punishment for the consequences.

The basis of accountability is transparency. This is true of government and of the private sector. One of many initiatives to improve the level of transparency and openness is the OECD-backed Global Privacy Enforcement Network ("GPEN"), a global network of privacy enforcement authorities working together to protect the privacy rights of individuals. In May 2013, for example, GPEB organized an Internet Privacy Sweep ("the Sweep") by 19 participating authorities. The capacity of regulators to carry out industry and market research of this nature is often limited in developing countries, but to develop such capacity is a move in the right direction as it can only lead to better informed public policy.

Another good example of openness is the decision of UNESCO to make its digital publications free for anyone to download under a worldwide open license.[141] UNESCO was the first member of the United Nations to adopt such an Open Access policy for its publications. In 2010 The World Bank announced it will offer free access to more than 2,000 financial, business, health, economic and human development statistics that had mostly been available only to paying subscribers.[142] This sets an important principle that publically-funded data collection, research and publication should be made freely-available, subject only to certain confidentiality rules. In lower income countries policy-makers and regulators will certainly benefit from having this added source available to make more informed decisions, and it follows an important trend in education by some of the world's leading universities to place their course materials online free of charge.[143] The World Bank is also supporting local open data Initiatives to make government data more open and online, for example the LGU Research Project in the Philippines.[144]

Regulators would do well to examine their own websites and databases to judge how transparent they are to their own public. A better informed public will be able to provide regulators with better informed feedback which in turn will make regulation more responsive and more effective.

[141] http://www.unesco.org/new/en/media-services/single-view/news/unesco_to_make_its_publications_available_free_of_charge_as_part_of_a_new_open_access_policy/

[142] http://unstats.un.org/unsd/accsub/2010docs-CDQIO/Ses1-WorldBank.pdf

[143] http://www.unesco.org/new/en/communication-and-information/access-to-knowledge/open-educational-resources/

[144] http://www.lguopendata.ph/. See also http://www.developmentgateway.org/