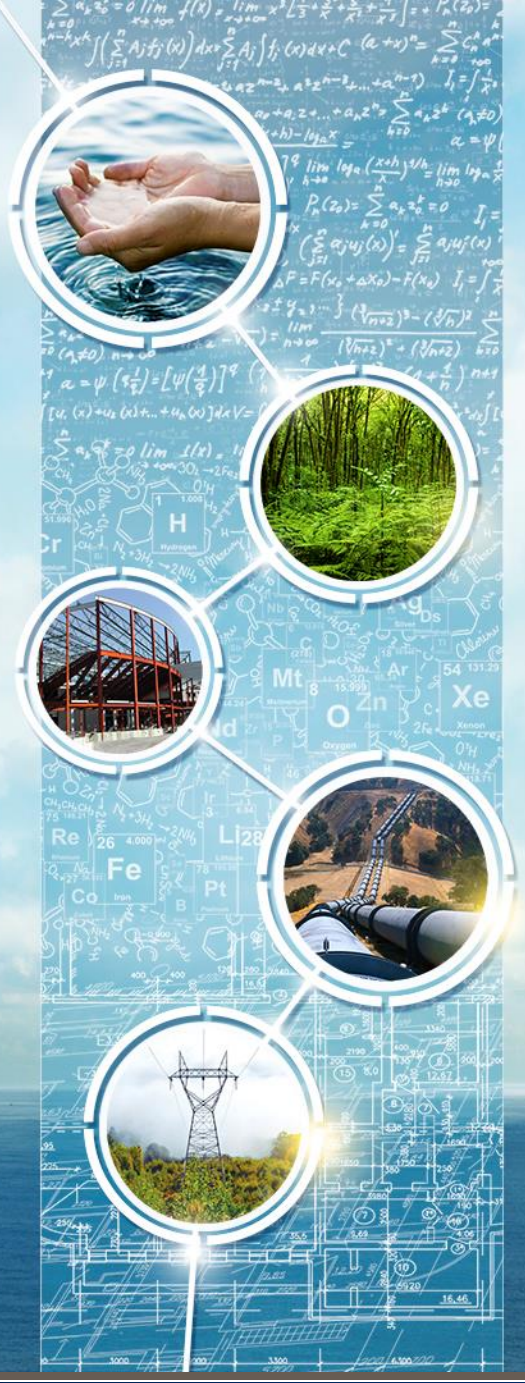

Convergence

July 31, 2018

Judith Hellerstein

CEO

Hellerstein & Associates

Agenda

- Convergence
- Regulatory Framework Checklist
- Institutional Design
- Broadcasting and Other Media
- Competition Authorities
- Postal
- Transport
- Finance
- Next Generation Networks
- Public Policy Issues and Implications
- Conclusion

Convergence: Definition

- Convergence is the coming together of two different entities, and in the context of computing and technology, is the integration of two or more different technologies in a single device or system.
  - It can also be defined as the ability of one or different networks to carry different services. Or the bringing together of industries in the communications area, which were previously viewed as separate and distinct in both the commercial and the technological sense.
  - The simple concept of convergence allows multiple tasks to be performed on a single device, which effectively conserves space and power
    - Examples are the provision of Internet access and TV to smart phones, carrying separate devices – like a cell phone, camera, TV and digital organizer, or the triple or quad play services offered by ISPs or Cable TV Operators.

Convergence Benefits

- Convergence creates possibilities for companies to develop and deliver services across technology platforms, increases economic growth, and allows for users to gain access to new kinds of communication and media services
  - Many different applications allow people to create multiple effects using simply their phone as the camera instead of carrying a separate device. There are even full length movies that have been created using only cell phones instead of a video camera
- Convergence promotes the expansion of competition, allowing the introduction of inter-modal competition where networks and technologies compete with each other with no technological or regulatory restrictions;
  - Mobile money is another kind of convergence. It allows your phone to be a bank account

Convergence: Benefits (continued)

- Technology convergence provides the possibility for new competitors to enter the markets.
  - Telephony can be offered by cable TV operators, TV to telephony providers. Amazon and Netflix have become the largest TV providers.
    - Their shows are not weekly but the entire season is released at one time allowing consumers to watch as they would like.
  - Time shifting allows programs to be saved and then watched whenever and wherever the consumer wants.
- Other benefits of Convergence are that it reduces costs of telecommunications services;
  - Fosters the development of more efficient technologies and services;
  - Opens the door for new ways for people to obtain Internet access

Impact on Regulatory Frameworks

- As convergence takes a firm hold in the communications industry, the process raises specific regulatory challenges given the merging of firms, and facilities.
- Adapting regulatory frameworks to convergence is not an easy task.
- Traditional frameworks were designed for an era when clear functional differences existed between services and infrastructure and were not designed for the this new environment of converged networks and services where functional differences no longer exist.
- Governments cannot and should not favor one technology, one network, or one service over another, nor should any operator restrict the use of any technology, network or service.
- Countries around the global have taken vastly different approaches to convergences starting with how they regulate Internet communications.

Regulatory Framework Checklist

- Regulators need to ask certain questions to make sure their frameworks are up-to-date.
- Does the regulatory framework facilitate the provision of different services over different platforms?
- Does the regulatory framework support full competition?
- Does the regulatory framework allow service providers to offer multiple services?
- What are the regulatory policies for these new technologies and services with regard to numbering, spectrum, universal service, emergency services and interconnection?
- Does the country's legal framework contain the necessary legislation to support an ICT environment (*e.g.*, intellectual property laws, computer crime, electronic transactions, data privacy and security)?

Effective Regulatory Framework

- Implement a well-defined and consistent regulatory framework for telecommunications, broadcasting, ICT, and other sectors such as Postal or Transport.
- Regulatory framework must give regulator the authority and means to effectively define and apply regulations in a market.
  - These characteristics are important, especially in markets where incumbent operators have extensive political and financial power.
  - Framework must provide for regulatory flexibility to adapt to the unanticipated needs and use of new technologies and services

Involve Stakeholders in the Regulatory Process

- Regulators need to involve all stakeholders in the regulatory process
- Consultation is an essential part of the decision-making process.
  - Enhances confidence in the regulator.
  - Increases consensus and support for regulatory decisions.
  - Provides a mechanism for input and feedback from stakeholders.
  - Reinforces regulatory autonomy and accountability

Neutrality Guidelines

- Need to create clear definitions for Technology, Service, and Network neutrality.
- Technology neutrality is basically the principle that rules should not discriminate in favor of any technology.
- Service neutrality is that rules should not discriminate in favor of any particular service.
- Network neutrality is the principle that Internet users should be in control of what content they view and what applications they use on the Internet.
  - It is about equal access to the Internet.
  - Broadband carriers should not be permitted to use their market power to discriminate against competing applications or content.

Challenges to the Existing Regulatory Framework

- Many Policymakers and regulators around the world are already responding to these challenges though with varying degrees of success, depending on the scope and depth of their changes, i.e, the EU, the US and Canada.
- They have done this by evaluating policy goals and regulations in the context of converged communications
- What type of regulation is needed
  - The role of the regulator is not to promote or 'accelerate' convergence, but to establish an environment for fair competition, i.e. a 'level playing field' so that if there is a demand for convergent services, such services can develop in the market and compete fairly with one another, bringing consumers the benefits of innovation, convenience and choice.

Problems with Regulatory Frameworks

- Often times, countries have adopted new regulatory frameworks that have attempted to take convergence into account, often create new regulations that could end up stifling competition and halting the spread of innovations and new uses of technology
  - As an example, the US Regulator recently gutted the Net Neutrality provisions which provided rules on technology, service, and net neutrality guidelines.
  - As an example, the European Regulatory Group (ERG) –made up of European member state regulators issued such a document. This document views a wide range of Internet communication as traditional "telephony service" and suggests applying the same traditional telephone regulation to the Internet – including services that link web sites to the PSTN

Regulatory Frameworks

- Internet-enabled communications, such as IP Voice, can increase competition, provide a platform for innovation, drive broadband deployment, and enable economic growth.
  - IP telephony is not a new kind of telephone service, but a whole new frontier in communications.
    - IP Telephony is much more than a substitute for traditional circuit switched telephone service.
    - It permits the integration of voice, data, and other IP applications enabling a host of breakthrough applications and services not possible with traditional circuit-switched networks
- Mobile money is similarly a innovative service that rides along the telecom network and requires the banking and telcom/ICT regulators to work together to come up with regulations.
- The same is true for any disruptive technology such as Blockchain

Regulatory Frameworks (Continued)

- The Regulator needs to work hard to bring all aspects of the telecommunications system into the new age.
- Emergency Communications are being upgraded as well allowing people to text or email photos and videos to the 911 Operator (the unit in charge of emergencies) or to the Police.
- Regulations have also been adopted to use the location services in smart phones, tablets or other electronic device to give Emergency services an address of where you are located in case of emergency

Updating Regulations

- Buttons or functions on gaming consoles or other similar products that add voice to the game were never conceived to be substitutes for telephony services nor would people assume or think that they would be and that they should be able to connect to emergency services.
- Similarly, Click to call buttons on website, blogs, Facebook messenger, Google, WhatsApp, Signal, Telegram, or other integrated communications services were never intended to be substitute for telephony service.
  - They were meant for communications and did not have emergency services in mind

Updating Regulations (continued)

- In several recent incidents, these mediums were used to notify others about emergencies but in all these cases a person picked up a phone (landine, mobile, fixed wireless) and called in the emergency.
- As such these services saved lives and without these services lives would be lost, but the point is that they were not the vehicle to call in the emergency
- Phones, however, were meant for calling despite their hundreds of other uses
  - This is why regulations were adopted to ensure that location services could easily tell where a person is located, an approximate address

Country Examples

- VOIP calls do not work in the following countries:
- Azerbaijan, Belize, China, Egypt, Iran, Jordan, Kuwait, Morocco, Oman, Pakistan, Paraguay, Saudi Arabia, United Arab Emirates
- However, Pre-recorded messages sent via these platforms do work
- Also various VPN systems can get through these blocks.
- Some blocks are not made by the country itself, but may be a result of a block by the ISP itself.

Institutional Design

- Three primary institutional designs for Regulatory entities:
  - Single-sector regulator: sole function is to oversee the telecommunication sector.
  - "Converged" regulator: tend to have oversight for all aspects of the ICT sector
  - Multi-sector regulatory authority: usually encompasses various industry sectors considered to be public utilities, *e.g.*, telecom, water, electricity, and transportation.

Institutional Design (continued)

- Countries with converged regulators include Australia, Finland, Iraq, Italy, Japan, Kenya, Mali, Malaysia, South Africa, Singapore, Uganda, United States and United Kingdom
- Despite this trend, most OECD countries still have separate regulators for broadcasting and for telecommunications content regulation is typically addressed by a separate ministry or government authority (e.g., in India and Saudi Arabia) or by the broadcasting authority (e.g., in Botswana, Chile and Colombia).

MSRAs: Strengths

- Is the MSRA model the appropriate model for developing countries? In theory, the model seems to provide a solution to address many of the constraints faced by regulators in developing countries. But it is too early to assess the effectiveness of the model.
- MSRAs allow developing countries the potential to achieve greater efficiencies in regulation, by benefiting from shared knowledge and resources, including a common infrastructure, administrative set-ups, and specialized human resource skills, such as those of accountants, economists, engineers, and other professionals across sectors.
- Regulatory performance & efficiency is highly dependent on the regulator's ability to understand its priorities & follow a plan of action that is coherent within the context of the country & its sector's development goals.

MSRAs: Weaknesses

- The research on multi-sector regulation is mixed on whether the MSRA model indeed provides the expected gains, such as increased efficiency, effective regulation and eventually tangible contribution to network and economic development in a country.
- MSRAs may optimize scarce resources, such as human resources, public finances, and technical knowledge or expertise.
  - But when staff resources are limited, the need to operate in different and complex sectors simultaneously increases demands on qualified staff and may also compromise the ability to develop sector-specific knowledge at an adequate pace and contribute to delays in appropriate regulatory interventions

Broadcasting

- The ITU defines Broadcasting as a radio-communication service whose transmissions are intended for direct reception by the general public.
- Broadcasting often has substantial content regulation because it is perceived as playing a special role in the cultural life of a country and in developing a national identity.
  - As such, it was often regulated differently than telecom and sometimes even by a different regulatory entity
- Convergence has resulted in new technologies and services that often are not encompassed in existing service definitions and regulation. As such it requires changes to be made in broadcasting and Audio Visual regulations to ensure consistency in policy and regulation with telecom regulation

Postal Convergence

- In recent years with the growth of e-Commerce the postal offices in developing countries have been key parts of a broadband strategy as such an ICT regulator needs to take into account how postal regulations fit into its system.
- The Postal network has become an important partner in developing strategies for Broadband in many different countries
- As such Regulators must take into consideration how Postal regulations and protections integrate and protect consumers using “telecom” services within their offices

Financial Convergence

- A multitude of uncoordinated state and federal statutes, regulations, agency "guidance," and court decisions covers mobile payments providers and their products and services, which results in an incomplete and uncertain regulatory environment
- For example, in the US, although many laws are applicable to mobile payments and cover a variety of issues, the overall legal framework is neither comprehensive nor consistent.
  - The current laws are filled with gaps, ambiguities, and overlap that undermine important consumer protections.
- There is a need for the Telecom/ICT/Consumer protection regulator to sign Memorandum's of Understanding with the financial regulator to 1) establish procedures for coordinating their activities and 2) to ensure that consumers are protected against fraud, data misuse, and data protection or cyber intrusion.
- Additionally if another regulator is responsible for consumer protection than an MOU needs to be also signed with that agency as well.
  - In the US, the FTC is responsible for consumer protection and has signed an MOU with the CFPB.

Financial Convergence (continued)

- In the US, current state and federal laws have not kept pace with technological developments that have enabled new products and services
  - No law dictates whether a mobile device should be treated as legally equivalent to a credit card or, instead, as an “access device” (such as a debit card), which carry different consumer protections
  - Software licenses used by mobile apps are not explicitly included in banking regulations and laws.
    - Mobile users are not aware that key consumer protections are not available to them as they would be if they were using a more traditional form of banking.
  - Consumers have no guarantee that they will receive clear and noticeable disclosures for mobile payments terms and conditions.

Intermodal Convergence

- With the acceleration of technological developments in network industries and, in particular, in infrastructures, there is a constant need to review the current regulatory regime.
- The growth of Smart Cities through out the world poses many questions to regulators in the transport, telecoms, water, transportation, and energy on how how to ensure all citizens are protected
- Just as in the financial section, there is a need for the Telecom/ICT/ Consumer Protection regulator to sign Memorandum's of Understanding with the Transportation Regulator, the Energy Regulator, the Water Regulator to 1) establish procedures for coordinating their activities and 2) to ensure that consumers are protected against data misuse, data protection or cyber intrusion.
  - Additional questions are: How should the sharing economy be regulated for regulators to invest in the infrastructure that supports it?
  - How should public goods and services including transportation, telecommunications, water and energy be managed and distributed?

Intermodal Convergence (Continued)

- While the possibilities are exciting and innovation continues to gain momentum at an accelerated pace, challenges are inevitable especially when it comes to infrastructure financing and the general management of smart cities
- Data is being gathered in virtually every mode of transportation.
  - That means data breaches and misuse happen—in transit systems, airlines, ride-hailing services, and even walking, biking and jogging.
  - The risks are perhaps especially great with “connected vehicle” technology.
- “Widespread concerns have been raised about the lack of security controls in many IoT devices,
- Gaining access to a car’s mechanical hardware, hackers could conceivably stop multiple vehicles in tandem, hold passengers for ransom, and manipulate vehicles to cause fatalities.
- All of this shows that Self Regulation is not the answer, but it is unclear what other type of regulation is needed and will it be effective

Next Generation Networks

- Next Generation Network is a broad term that describes key architectural evolutions in core and access IP based networks.
  - It refers to the future networks that support fixed, mobile and nomadic users and able to carry voice, data and multimedia services.
  - It is based on IPV6 and MPLS technologies and protocols.
- The Telecom network is evolving toward a future in which IP-based networks replace circuit-switched networks, both for fixed and mobile (3G, 4G, and 5G) services.
  - Legacy interconnection regulations will not disappear– indeed, the complex interconnection environment calls for greater oversight.
- Convergence has forced a reassessment of Interconnection policies
  - Effective interconnection arrangements are crucial in fostering the development of integrated ICT markets
- IP networks will coexist with older legacy networks, including 3G mobile and PSTN networks.

Next Generation Networks (continued)

- The technological innovations that have resulted in the convergence of telecom, information and broadcasting have raised numerous regulatory issues regarding interconnection.
- Effective interconnection arrangements are crucial in fostering the development of integrated ICT markets
- Convergence has forced a reassessment of this policy taking into account the interconnection of different types of networks and service providers (*e.g.*, cable television/content providers and IP networks/ISPs)

Interconnection in an IP World

- Traditional interconnection regulation was established for telecom operators with interconnection rates generally based on time (*i.e.*, per minute).
- Services based on IP protocol, however, do not fit within the traditional schemes of switched voice interconnection, e.g., IP interconnection separate out transport from service, while legacy networks combine them.
- Countries are addressing these needs by introducing: (i) both symmetrical & asymmetrical interconnection, (ii) new kinds of "access" through interconnection regulation and (iii) a technology-neutral interconnection charging system based on capacity, instead of time and distance

Public Policy Implications

- As convergence takes a firm hold in the communications industry, the process raises specific regulatory challenges
  - Public Policy Issues
  - Universal Service
  - Licensing and Authorization
  - Spectrum Management
  - Numbering and Portability
  - Interconnection
  - Network Reliability/Network Security
  - Law Enforcement
  - Media Ownership
  - Accessibility
  - Access to Emergency Services
  - Service & Content Regulation
  - Consumer Protection

Universal Service

- Universal Service: Convergence challenges the traditional way Universal Service/Access is delivered in several ways:
  - Funding of universal service is usually obtained through extra charges imposed on certain telecom services e.g. access charges or interconnection charges.
  - Many countries are beginning to include broadband in the definition of universal services?
    - Is this this best way of stimulating Internet penetration or should a wider range of access possibilities be offered.
- Should VOIP providers be required to offer services in all rural or high-cost areas
- Should there be different definitions for broadband access urban as opposed to rural areas of the country
- What is the best way of ensuring that all citizens have access to the Internet and to broadband?

Universal Service (continued)

- Should all Communications providers pay into the universal service fund or just the ones classified as phone providers
- Should cable companies pay into the fund?
- Should Internet companies pay into the fund?
- What other carriers or operators should pay into the fund?

Authorizations and Licenses

- Traditional licenses & authorizations were designed for a circuit switched technology era when clear functional differences existed between services and infrastructure
- Goal of licensing is the allocation of scarce resources, establishing regulatory certainty and a framework for privatization and competition, universal access, etc
- Traditionally the number of licensed voice telephony or broadcasting operators has been limited.
- Authorization and licensing of service providers were based on the type of service (voice, data, and video) or technology (cellular, fixed telephony, terrestrial broadcasting).
- However, in a converged setting, it is difficult to maintain these boundaries because of overlaps, broadcasters are offering telecom services (Internet, voice), while telecom service providers (e.g. phone companies) are offering broadcasting services (IPTV). Further, cellular operators are providing mobile television services

Licensing

- Traditionally, the number of licensed voice telephony or broadcasting operators has been limited.
- Previously, authorization and licensing of service providers was based on the type of service (voice, data, and video) or technology (cellular, fixed telephony, terrestrial broadcasting).
- However, in a converged setting, it is difficult to maintain these boundaries because of overlaps, broadcasters are offering telecom services (Internet, voice), while telecom service providers (e.g. phone companies) are offering broadcasting services (IPTV).
- Further, cellular operators are providing mobile television services
- Other providers are offering shows only available on the Internet.

Licensing (continued)

- Many regulators and policymakers have already modified their licensing regimes from the traditional one-service or technology license to a technology neutral, simplified set of licensing categories, and in some cases, a unified (single) license or market entry procedure for all technologies and services.
- Many countries are combining this simplification with the introduction of flexible licenses that use a technology and service neutral approach to determine the rights and obligations granted by the licenses.
- These update the obligations for Interconnection, numbering, universal service and consumer protection rules to the new environment of convergence
- Along with a new licensing structure, it is also necessary to simplify market entry procedures as well as to simplify the administrative requirements for all telecom operators.
- This involves modifying general authorization to allow more services to be provided

Types of Licenses

- There are seven classes of licenses
  - Individual
  - Class
  - Registrations
  - Notifications
  - Open Entry
- Additionally there are several other types of licenses
  - Social Purpose
  - Experimental

Classes of Licenses

- Individual Licenses are the most complex and require the regulator to consider each license individually.
- Class Licenses are less complex since they require only an approval process for a broad category of service, are Issued without competitive bidding and are available to allqualified applicants who meet certain eligibility criteria established by the Regulator
- Registration requires the operator to formally register with the regulator before operation of the service.
- Notification requires the operator simply to notify the regulator of the service, but no regulatory approval is necessary.
- Lastly, open entry is the most flexible and requires neither notification nor registration.

Unified Authorizations

- Unified Authorizations
  - Technology and service neutral
  - Allow licensees to provide all forms of services under the umbrella of a single authorization, using any type of communications infrastructure & technology capable of delivering the desired service.
  - In most countries, unified authorizations are issued as individual licenses.
  - However, in some countries, the process for issuing the unified authorization blends aspects of general authorization processes and competitive licensing regimes.
    - These hybrid processes can best be described as noncompetitive individual licensing processes: while applicants do not compete for a limited number of authorizations, they must meet a variety of criteria to qualify for a license and their applications are subject to close regulatory scrutiny.

Multi-service authorizations

- Multi-service authorizations
  - Allow service providers to offer multiple services under the umbrella of a single authorization, using any type of communications infrastructure & technology capable of delivering the services in question
  - Technology neutral -- like unified authorizations
  - More limited than unified authorizations -- licensees are permitted to provide any of a designated set of services, but not all services
  - Issued as general authorizations or as individual licenses.
  - Not uncommon to have both general authorization & individual license regimes for multi-service authorizations

Social Purpose Licensing

- One example of innovative licensing is a “social purpose” license. This is a license granted in rural unserved or underserved areas to non-traditional network operators, such as community network operators.
- By setting aside spectrum for non-traditional operators, regulators can remove the competitive barriers to spectrum access and prioritize spectrum for social-use purposes.
- Social purpose licensing has proven to be tremendously successful in launching community networks.
- Mexico is at the forefront of innovative, social purpose licensing.
  - In 2015, the Mexican communications regulator, Instituto Federal de Telecomunicaciones (IFT), amended its frequency plan to set aside 2 x 5 megahertz of spectrum in the 800 MHz band for “social” use.
  - To qualify for a social-use license, applicants must demonstrate that the spectrum would be used to service communities of 2,500 people or less, or communities located in a designated indigenous region or priority zone.

Experimental Licenses

- Experimental licenses are another way to provide communities direct access to spectrum.
- Experimental licenses authorize the licensee to test and develop new technologies and services, while protecting incumbent services against harmful interference.
- India has also issued experimental licenses for community network projects.
  - In 2016, for example, the Indian government issued eight experimental licenses in the 470-582 MHz band to carry out experiments of Television White Space-type rules and regulations
- Experimental licenses are generally temporary. Many community networks find that experimental licenses help them establish their operations, but they also run the risk of the experimental license taking considerable time to be transformed into a more permanent license

Licensing

- As with licensing regimes, new advanced technologies and converged services that use spectrum are demanding more flexible and service/technology neutral frameworks
- Need to keep in mind that spectrum management is about addressing the problems of potential interference between different licensed users, which is why regulators have created different classes of licenses.
- Consideration should also be given to whether there should be flexibility in spectrum allocation to take full advantage of new services and new technologies for existing services that may evolve with time.
  - A technology- or service-neutral approach to spectrum use might be another good option to consider.

Spectrum Management

- All services require spectrum to operate making spectrum management a more daunting and crucial task than ever before.
- The problem here is how to reconcile the entry of the license holder into new service areas.
- Unencumbered frequency bands used for communications services were once widely available; now they are a relatively scarce commodity in an increasingly spectrum-dependent world.
- As new spectrum technologies unfold and proliferate, spectrum managers and regulators have to adapt and evolve to continue to manage the increasing crowded spectrum resource in a responsible, fair, and technology-neutral manner.
- Current regulatory regimes based on national and international frequency allocations, providing for exclusive use of frequencies will need to be continuously reviewed.

Spectrum Policy

- Regulators need to certain key things:
  - Ensure that spectrum remains open, transparent, fairly allocated and that the licensing mechanism is technology and service neutral.
  - Ensure that there is a harmonization of spectrum to global standards
- Regulators should also create a flexible spectrum policy that allows for innovative usage through unlicensed spectrum and also allows easy ways for people to reuse spectrum that is not being used within rules that avoid harmful interference.
- Making more spectrum available:
  - Spectrum is the lifeblood of wireless Internet access.
  - Spectrum solutions that take advantage of innovative approaches can advance connectivity and help countries roll out broadband to more people in the country

Spectrum Innovation: Increasing Access To Broadband

- Other ways to expand connectivity within the country are:
  - Encouraging the development of license exempt technologies, for example, White spaces, Delay Tolerant Networking, Mesh networks, CubeSats, WiFi, WiMAX and other wireless technologies.
  - Reviewing spectrum use policies that are related to license free spectrum especially for rural applications to facilitate the deployment of technologies that use these frequencies for universal access or other projects.
  - Increasing and encouraging the deployment of and experimentation with local access networks using new wireless and wireline technologies, such as, but not limited to, White Spaces, Mesh Networks, WiFi, WiMAX, SCPC DAMA and PLC
  - Facilitating the use of unlicensed spectrum to reach rural and remote areas and also for deploying applications
  - Creating specific national local access licenses for remote and rural applications to advance connectivity for the un connected, using USF fees

Spectrum Management (Continued

- The current trend is to develop new spectrum-efficient technologies that allow new users of spectrum to be accommodated while at the same time reducing the cost per user per hertz by increasing the number of users that can access a given portion of spectrum.
- New technologies are evolving that allow for the sharing of spectrum more efficiently, the leasing of unused spectrum to other companies, and the auctioning of white spaces between spectrum licenses that previously were thought to not be usable.
- New and emerging technologies will spur an increase in demand for spectrum-dependent wireless services, challenging regulators and users alike.

Spectrum Roadmap

- Regulators will need to create a roadmap for how to proceed.
  - Define a clear roadmap for access to spectrum to support current and next generation services on a technology neutral basis;
  - Embrace and define new capabilities and technological change into the management of the radio spectrum;
  - Adapt and modify the telecom regulatory framework to accommodate the flexibility of the new technology in providing telecom goods and services;
  - Enable the introduction of new and different services over existing infrastructure by ensuring a level playing field to all current and future operators; and
  - Enable and encourage deployment of broadband wireless access

Interconnection

- Traditionally interconnection regulation was established for switched voice services, where rates were generally based on a per minute charge
- Converged Services, most notably those based on the IP protocol, require interconnection rights and new interconnection schemes with different types of access and charges to ensure that everyone can interconnect regardless of the type of network they are using.
- Newer interconnection pricing involved symmetrical interconnection costs, where any operator, regardless of network type, is obliged to interconnect with any other operator.

Interconnection (continued)

- Interconnection pricing is based on access to parts of the infrastructure (e.g., the local loop or directory services databases), or to allow the provision of wholesale services (e.g., wholesale Internet access service or mobile roaming).
- Some have even adopted a technology neutral interconnection charging system based on capacity, instead of the traditional metrics of time and distance.
  - Here operators may request a specific capacity for interconnection and pay a flat-rate charge that reflects the fixed-cost nature of the interconnection capacity

Network & Data Security

- The increasing use and reliance of Big Data and its integration within innovative and new technologies throughout the world is another reason why it is important to have strong data protection and privacy laws.
- Innovative companies starting out need to put much energy and cash into ways of making their site safe for consumers.
- These new innovations are based on data and technology and network and data security need to be a primary focus of all creators and operators.
- The rapid increase of new devices that can be connected to each other and the lack of attention being paid to the network security of these devices, software or other components sold in the marketplace potentially can cause great harm to consumers.
- Regulation needs to be in place to protect consumer's and their data from hacking, intrusion, or ransomware.

Cyber Security Definition

- Cyber security is the practice of defending computers and servers, mobile devices, electronic systems, networks and data from malicious attacks.
  - It is also known as information technology security or electronic information security.
  - The term is broad-ranging and applies to everything from computer security to disaster recovery and end-user education.
- Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.
- Cyber security relies on cryptographic protocols used to encrypt emails, files and other critical data.
  - This not only protects information that is transmitted but also guards against loss or theft.
  - End user security software scans computers for pieces of malicious code, quarantines this code and then removes it from the machine.

Network Security

- Network Security
  - Governments consider that providers of publicly available communications services should take appropriate measures to safeguard both the security of their services and the Private and personal data they have collected of their users .
    - For VOIP services, this could include measures to protect against viruses. Phising, denial-of-service attacks, Intrusion, and ransomware.
- Law Enforcement
  - The ability for law enforcement authorities to access communications networks (often referred to as Lawful Intercept) is an issue of great concern to governments, especially as terrorism threats grow and multiply.
  - Governments have adopted different regulations to enable them to have access to all types of networks, mobile, Internet, and Cable TV.

Cybersecurity

- Electronic security protocols also focus on malware detection — ideally in real time.
  - Many use what's known as "heuristic analysis" to evaluate the behavior of a program in addition to its code, helping to defend against viruses or Trojans that can change their shape with each execution.
- The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves.
- Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known threats.
- Today, this approach is no longer sufficient, as the threats advance and change more quickly than organizations can keep up with.
  - As a result, advisory organizations promote more proactive and adaptive approaches to cyber security.

Internet Privacy

- Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums.
  - If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.
- Internet privacy risks include:
  - Phishing: An Internet hacking activity used to steal secure user data, including username, password, bank account number, security PIN or credit card number.
  - Pharming: An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.
  - Spyware: An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.
  - Malware: An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

CyberCrime

- Cybercrime is any criminal activity that involves a computer, networked device or a network.
  - While most cybercrimes are carried out to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials.
  - Some cybercrimes do both -- i.e., target computers to infect them with viruses, which are then spread to other machines and, sometimes, entire networks.
- Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information.
- Cybercriminals may target private personal information, as well as corporate data for theft and resale.

Cyber Crime Definition

- The U.S. Department of Justice divides cybercrime into three categories:
  - crimes in which the computing device is the target, for example, to gain network access;
  - crimes in which the computer is used as a weapon, for example, to launch a denial-of-service (DoS) attack; and
  - crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally obtained data.
- The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, defines cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements.
  - Other forms of cybercrime include illegal gambling, the sale of illegal items, like weapons, drugs or counterfeit goods, as well as the solicitation, production, possession or distribution of child pornography.

Cyber crime/Security

- Cybercrime/Cyber security often extends across national boundaries as Illegal content is stored outside a country or viruses are transmitted through a number of countries from sender to recipient.
  - For people to enjoy the many benefits of an interconnected world, they must feel confident in the security of the networks, services and applications they use.
- Policymakers must therefore seek to protect legitimate activities against four broad categories of cybercrime/Cybersecurity:
  - offenses against data privacy and the integrity of computer systems
  - computer-related crimes or offenses
  - digital piracy and copyright violations; and
  - content-related offenses, which may include Child pornography, illicit content, online gambling, libel and cyber bullying

Types of CyberCrime

- There are many different types of cybercrime; most cybercrimes are carried out with the expectation of financial gain by the attackers.
  - Cyberextortion, is crime involving an attack or threat of attack coupled with a demand for money to stop the attack, for example--Ransomware
  - Cryptojacking, uses scripts to mine cryptocurrencies within browsers without the user's consent
  - identify theft, occurs when an attacker accesses a computer to glean a user's personal information that they can then use to steal that person's identity or access bank or other accounts.
  - credit card fraud, occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet
  - ransom wear--a form of cyberextortion in which the victim device is infected with malware that prevents the owner from using the device or the data stored on it. To regain access to the device or data, the victim has to pay the hacker a ransom.
  - Cyberespionage--occurs when a cybercriminal hacks into systems or networks to gain access to confidential information held by a government or other organization

Cybercrime (Continued)

- Cybercrimes may have public health and national security implications, making computer crime one of the Department of Justice's top priorities.
- In the US, Cybercrime is the responsibility of the Computer Crime and Intellectual Property Section (CCIPS) within the US Department of Justice.
  - It is responsible for implementing national strategies to combat computer and intellectual property crimes worldwide.
  - CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.
  - Section attorneys work to improve the domestic and international infrastructure-legal, technological, and operational-to pursue network criminals most effectively.

Enforcement

- The Secret Service's Electronic Crimes Task Force (ECTF) investigates cases that involve electronic crimes, particularly attacks on the nation's financial and critical infrastructures.
  - The Secret Service also runs the National Computer Forensics Institute (NCFI), which provides state and local law enforcement, judges and prosecutors with training in computer forensics.
  - The Internet Crime Complaint Center (IC3), a partnership between the FBI, the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA).
  - This group accepts online complaints from victims of internet crimes or interested third parties.

Enforcement of Cyber Crime

- A cyber criminal can force law enforcement agencies into a virtual chase around the world by using any number of techniques that mask the identity of the cyber criminal and make tracing communications difficult
  - It is why it is imperative for other countries to join the Council of Europe Convention on Cybercrime.
  - The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.
  - Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.
  - It does this by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.
  - It also contains a series of powers and procedures such as the search of computer networks and interception.
  - More than 70 countries have signed the Budapest Convention

Budapest Connvention

- The Budapest Convention sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data.
- Additionally, the Convention contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties.
- The Convention requires the provision for adequate protection of human rights and liberties.

Accessibility in a Converged World

- Accessibility
  - In a converged environment, where some sectors are no longer regulated, e.g., VOIP or IPTV services, are not subject to obligations such as, closed captioning or other services for people with disabilities and specific needs, how do you ensure that everyone can equivalent access to these services?
  - Regulations need to be adapted so that these same services delivered over another platform are also accessible to people with disabilities and specific needs
  - In a sharing economy, how do you create regulations that push for universal design so that citizens can benefit equally?
  - Standards such as those proposed by the World-wide Web Consortium, W3C, on both layout and content need to be adopted by all?

Emergency Services

- Regulators world-wide need to decide how to ensure that IP telephones that are replacements or complete substitutes for voice telephony will work to connect these networks to emergency service operators and display the correct location of the caller.
- Also that these services can accept submissions by text, email, or voice.
  - As discussed earlier, many countries have adopted rules that ensure that all IP phone providers can connect to emergency services.
  - The key here is to identify which IP telephony services are substitutes for telephony and thus subject to regulation, and which are additional new services that people would never consider ever needing to call emergency services

Quality of Service Regulation in a Converged Environment

- Regulatory frameworks need to be modified so as to take full advantage of these new converged services and still maintain a certain level of QoS
  - In the traditional regulatory framework ensuring certain QoS standards has been a main function of the regulator. However in a converged environment, new technologies have blurred the boundaries between the broadcasting and telecommunications sectors.
- Quality of Service Standards
  - New QoS standards must be created for converged services since each of the services has very different QoS requirements. Telecom has more stringent QoS standards because it has to be always available, but broadcasting because it was one to many and not one to one had very different requirements. Traditionally broadcasters have not allocated resources dynamically. Instead, broadcasting towers, satellite networks, serve customers in a static fashion since signal transmission is independent of the usage.

Regulatory Framework: Service & Content

- The main trend in this area has been to split the regulation of the transmission network and technology from the regulation of the content.
  - Success will only occur if regulators and policymakers observe the key principles of service and technology neutrality as well as establishing and insisting upon transparency, and enforce the appropriate licensing rights and obligations.

Consumer Protection

- As mentioned in the section on Intermodal Competition there is a need for the Telecom/ICT/ Consumer Protection regulator to sign Memorandum's of Understanding with the Transportation Regulator, the Energy Regulator, the Water Regulator to 1) establish procedures for coordinating their activities and 2) to ensure that consumers are protected against data misuse, data protection or cyber intrusion.
  - Additional questions are: How should the sharing economy be regulated for regulators to invest in the infrastructure that supports it?
  - How should public goods and services including transportation, telecommunications, water and energy be managed and distributed?

Consumer Protection (Continued)

- Other questions are more basic? How can Consumers be protected against fraudulent or bankrupt communications providers or operators. This is an important new function of today's regulator.
  - How do you provide protection to consumers in an area where neither the services nor the technology are regulated.
  - Consumer protection or Competition Regulator does not protect access to phone service or phone numbers, just a consumer's personal identifiable number

Conclusion

- Governments and regulators play a key role in stimulating demand for ICT services and applications, in the framework of broader strategic goals, such as connecting public institutions, businesses and residential users with broadband, promoting economic development, digital inclusion, social cohesion and equality of opportunity.
- Regulators need to be attentive to the challenges stemming from convergence to pave the way for the establishing a regulatory environment that is transparent, conducive to investment and growth, fosters fair and greater competition and innovation, stimulates the deployment of infrastructure, promotes the development of new services, protects consumers, and is security conscious.
- Regulators should adopt appropriate regulation on interconnection and access, including pricing, taking into account the relevant technological market developments including the roll-out of Next Generation Networks in the core and in the access layer.

Conclusion (continued)

- Governments need to build an adaptive regulatory framework by adopting a technology neutral approach, and a simplified and flexible licensing regime that provides for easy market entry of new players, such as through general authorizations and multiservice/unified licenses.
- Foster competition in converged services over wireless networks through efficient and integrated spectrum management
- Establish appropriate policy goals and refrain from imposing regulatory restrictions except when strictly necessary to promote competition and consumer protection, and that are proportionate to the established policy goals.

Thanks

Questions, Comments, Suggestions

Judith Hellerstein

Hellerstein & Associates

Judith@jhellerstein.com

www.jhellerstein.com