



The Top 10 Issues Facing the Telecom Sector

September 9, 2019 Judith Hellerstein CEO Hellerstein & Associates



Agenda



- Convergence
- Regulatory Frameworks
- Interconnection (Pricing and Costing)
- Licensing & Spectrum Issues
- Open Access
- Universal Access
- Trust
- Data Management
- Privacy
- Cybercrime/Cyber Security
- Internet of Things
- Encryption
- Platform Liability
- Internet Shutdown





Convergence



Copyright 2018 ©. The Institute for Public Private Partnerships, a Tetra Tech company PPP Solutions For a Complex World

Convergence: Definition



- Convergence is the coming together of two different entities. For Technology it 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





Regulatory Framework



Regulatory Frameworks



- There are three approaches taken by countries to address convergence:
 - a legislative approach;
 - a regulatory approach; and
 - a self-regulation approach.
- Although the first two are most commonly used among policy-makers, the self-regulation approach is gaining increasing popularity.



Legislative Approach



- The legislative approach develops legislation that responds to convergence.
 - Legislative solutions define new laws or create new regulatory frameworks to respond to convergence and guide future policy direction, either by developing and implementing a reform of the legal framework or by amendments to existing laws.
 - An advantage of the legislative approach is that it allows for the introduction of a new framework to deal with convergence, without the constraints imposed by other regulations or by the existing telecom, broadcasting, financial, or ICT law that may contain categories where converged services do not fit.
 - -A new law or an amendment of an existing law can eliminate contradictions and inconsistencies in regulatory classifications.



Regulatory Approach



- Under this approach, countries do not develop new legislation rather they modify existing regulations to address new technologies.
- This approach can be a practical way of addressing convergence provided that existing regulations can be modified or new ones introduced relatively quickly.
 - This approach must be carefully managed to minimize inconsistencies between new and existing rules as such it is often used by policymakers to complement a legislative approach.
 - This complementary mix allows governments to establish new legal frameworks while dealing with its specific effects through regulation. However, for this combined approach to work the legislation must be sufficiently flexible to allow periodic regulatory adjustments



Self Regulation



- The self-regulation process consists of developing and designing convergence policy through an ad hoc or existing consultative body or through a multi-stakeholder advisory group consisting of stakeholders from all sectors
 - The role and functions of these consultative bodies varies, but they generally issue recommendations to the government addressing the need for changes in convergence legislation and/or regulation.
 - The outcome is often self-regulation or industry guidelines.
 - These consultative bodies often address specific issues of convergence or undertake a more comprehensive analysis assessing the consequences of the legislative and regulatory environment
 - The self-regulation process has certain potential problems, e.g., the intervention of industry representatives may pose a risk in those jurisdictions where competition has not developed since the consultative body may be dominated by these operators and its conclusions could reflect narrow interests.



Regulatory Independence



- Effective regulation also requires that the Regulator adopt and implement procedures that are transparent and open to public participation and ensure accountability.
- Independence depends on:
 - Robust and transparent governmental and legal institutions
 - The number and quality of the regulatory staff.
 - The administrative structure of the regulator, including staffing processes,
 - -The legal status of the staff,
 - -Remuneration principles
 - -The ability to hire outside consultants provide key insights into the independence, depth of knowledge, and impartiality of the regulator, as well as its ability to attract and retain qualified personnel.



Stakeholder Consultations



- Consultations are an essential part of the decision-making process as they reinforce regulatory autonomy and accountability.
- Consultations can make the regulator more accountable without comprising its independence
 - Not only do consultations enhance the confidence the industry and the wholesale providers have in the regulator, but they also increase consensus and support for regulatory decisions, and provide a mechanism for input and feedback to the regulator from the stakeholders
 - It is critical that the Agency be willing to debate and answer questions openly and publicly.
- If the Regulator is seen as being weak or ineffective industry, consumers, and other stakeholders, will not trust him.
 - If these stakeholders lose trust in the Office of the Regulator or in the Regulator him/herself, foreign investors will pick up on this and be hesitant to invest in the country because of this uncertainty and trust in the market and in the Regulator's ability to ensure a level playing field.





Interconnection



Copyright 2018 ©. The Institute for Public Private Partnerships, a Tetra Tech company PPP Solutions For a Complex World

Interconnection



- While "interconnection" and "access" are related they are distinct.
 - Interconnection is a bridge between different networks to enable customers of each network to communicate with each other.
 - Access enables an operator to use the facilities and / or services of another operator
- Regulators also need to consider quality standards for interconnection.
 - Is the quality of service provided by an incumbent to an interconnecting entrant the same as to its own retail customers?
 - Is the overall level of quality consistent with that of increasing competition;
 - would some customers sacrifice quality for lower prices, sparking a "race to the bottom" for quality?



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.
- Interconnection between PSTN networks is relatively simple and well established, and does not raise interoperability issues, but IP Interconnection requires different kinds of access and different kinds of charges.
- Countries are addressing these needs by introducing: (i) both symmetrical & asymmetrical interconnection, (ii) new kinds of "access" through interconnection regulation and (iii) a technologyneutral interconnection charging system based on capacity, instead of time and distance



International Gateways



- An International Gateway is defined as any facility through which international telecommunications traffic is sent and received.
 - IGWs are potential bottlenecks in any nation's telecom market as they often restrict international traffic flows and maintain artificially high prices.
- A nation's ability to fully participate in the global Information Society may be impeded due to the high costs of Internet access or international communications.
- By liberalizing the IGWs and allowing a large number of operators, including those who operate domestic networks, to operate international gateways, incentives for illegal behavior, i.e., bypass, will disappear as the termination rate drops significantly.
- International calls will flow through legal channels, yielding taxes to the government and drying up the corrosive flow of black money.





Pricing and Costing of Services



Pricing



- It is important to be clear about what is meant by "prices".
 - A price for a given telecommunications service is more than just the charges for that service it consists of a description of the service, the terms and conditions of service provision and the applicable charges
- Prices are based on underlying cost using an acceptable methodology, LRIC, FDC
- Prices are non-discriminatory
- Prices are transparent



Cost Models



- What is a cost model?
 - A methodology for estimating a provider's cost of offering a service (or facility)
 - Motivated by the widely-accepted premise that service tariffs/prices should be cost-orientated
 - -Prices should relate to underlying costs
 - Measures the direct and indirect costs of providing interconnection
- Captures the volume sensitive & fixed costs that are directly identified with interconnection + a share of common overhead cost
 - Involve determination of many input variables
 - Typically implemented in spreadsheet program or similar software





Licensing & Spectrum Policy



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



Classes of Licenses

- There are five 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
 - Require the regulator to consider each license individually and conduct a competitive selection process or auction
- Class Licenses are less complex
 - Require only an approval process for a broad category of service.
 - Issued without competitive bidding and are available to all qualified applicants who meet certain eligibility criteria established by the Regulator
 - Set out the basic rights and obligations and regulatory provisions to the particular class of service being offered.
 - Allow for Service obligations to be applied to class licenses for extra comfort and protection of the Government



Classes of Licenses (continued)



- In recent years there has been a trend away from granting individual licenses to granting Class Licenses that authorize the provision of telecom services of the same type, regardless of who provides these services.
 - This is due to increased competition, increased flexibility in the type of licenses issued, the proliferation of service providers, and the convergence of the ICT sector and new innovative services and technologies coupled with telecom reform and deregulation.
- Registration requires the operator to formally register with the regulator before operation of the service, but do not require approval.
- 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.



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 Spacetype rules and regulations

30

 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



Spectrum Policy



- To expand Connectivity, Regulators need to do 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 Policies



- Spectrum policies should address incentives for innovation, promote flexibility, establish spectrum users' rights and determine practical methods for compliance monitoring, interference management and dispute resolution.
- These factors apply whether spectrum is used in the spectrum commons or shared by some other means where implementation relies heavily on advanced radio technologies designed to facilitate spectrum sharing.
- Convergence of wireless technology with Internet technology is not a new topic. The challenges are to address the evolution of technology and growth in demand, ensuring that sufficient spectrum is available for current and future generations of services while protecting public safety and security



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 Sharing



- Spectrum sharing encompasses several techniques some administrative, technical and market-based.
- Spectrum can be shared in several dimensions; time, space and geography.
- Spectrum sharing typically involves more than one user sharing the same band of spectrum for different applications or using different technologies.
 - When a band already licensed to an operator is shared with others it is known as overlay spectrum sharing. For example a spectrum band used for TV distribution in one geographical area could be used for an application such as broadband wireless access in another area without any risk of interference, despite being allocated on a national basis
- Spectrum sharing can be achieved through technical means and through licensing arrangements.

Unlicensed Spectrum



- A spectrum commons is a part of the spectrum that is free from centralized control where anyone can transmit without a license.
- For this reason it is sometimes referred to as unlicensed spectrum.
- There are varying approaches by regulators for managing the unlicensed but regulated spectrum commons ranging from imposing license and permits constraints to few if any constraints at all beyond technical specifications.
- In some countries, a more liberalized approach towards spectrum management has evolved resulting in considerable innovative approaches in the use of Wi-Fi, WiMax, Ultrawideband (UWB), White Spaces bands.



White Spaces



- In telecommunications, white spaces refer to frequencies allocated to a broadcasting service but not used locally
- A white-spaces device" (WSD) is a device intended to use these available channels.
 - WSD are designed to detect the presence of existing but unused areas of airwaves, such as those reserved for analog television, and use these airwaves to send signals for Internet connectivity.
- On November 4, 2008, the FCC voted 5-0 to approve the unlicensed use of white space
- Singapore's Regulator is the second regulator in the world to have TV White Space regulated, ahead of UK and Canada.
 - The Singapore efforts were driven mainly by the Singapore White Spaces Pilot Group (SWSPG). The Institute for Infocomm Research subsequently spun off Whizpace to commercialize TV White Space radio using strong IPs that were developed in the institute since 2006.


White Spaces (Continued)



- Both Microsoft and Google have been using White Spaces to extend broadband access to rural areas, both in the US and elsewhere.
 - However, in the US these have only been done on a trial basis and only in limited bands for short range applications.
 - It is hoped that TV white space will be able to provide affordable broadband service to rural America
 - Extending the internet to rural areas through underground cables is expensive: It can cost \$30,000 per mile for fiber-optic cable and \$1 million to run cable under a river.
 - White Spaces can do this at a fraction of the cost
- White Spaces alone cannot be the magic bullet that solves the problem, but it is an integral piece of the puzzle just as Google's Project Loon is another piece of the puzzle



White Spaces Trials



- In June 2011 in the UK, Microsoft, using technology developed by Adaptrum & backed by a consortium of ISP's and tech companies, launched one of the largest commercial tests of white space Wi-Fi.
 - These applications were demonstrated under a highly challenging radio propagation environment with more than 120 dB link loss through buildings, foliage, walls, furniture, people etc. and with severe multipath effects.
- In 2017, Microsoft further expanded their research to show that small cell LTE eNodeB's could be used to provide cost effective broadband to affordable housing residents.
- Since then, Microsoft has been using white spaces to deliver Broadband access in rural areas of Kenya, Namibia, Argentina, and in rural areas of the US
- Google has been experimenting with white space in South Africa



- Spectrum Trading is a mechanism whereby rights and any associated obligations to use spectrum can be transferred from one party to another by way of a market-based exchange.
- With spectrum trading, the right to use the spectrum is transferred voluntarily by the present user, and a sum is paid by the new user of the spectrum which is retained, either in full or in part, by the present (transferring) user.





Open Access



Copyright 2018 ©. The Institute for Public Private Partnerships, a Tetra Tech company PPP Solutions For a Complex World

Open Access



- Open Access to Infrastructure Sharing
 - Open Access is about creating competition in all layers of the network allowing a wide variety of physical networks and applications to interact in an open architecture.
 - Allows anyone to connect to anyone in a technology-neutral framework
 - Encouraging innovative and low-cost service delivery
 - Encourages market entry from smaller, local companies by lowering the entry barriers and reducing the likelihood of one entity becoming dominant.
- Requires trust in parties.
 - The service provider needs to feel that the infrastructure provider is going to tackle his/her needs with same degree of attention as if the organization was doing it itself.
 - That pricing and access terms will be transparent and nondiscriminatory.
 - That the Incumbent's transport services will be separate from its access services to build this essential trust.
 - That Governance structures with oversight powers will be set up to monitor the operators





Universal Service or Access



Copyright 2018 ©. The Institute for Public Private Partnerships, a Tetra Tech company PPP Solutions For a Complex World

Universal Service



- First Generation Definition of Universal Access (Service)
 - Universal Service refers to all households in a country having a telephone, so that all individuals can make a telephone call from home.
 - Universal Access as all individuals having reasonable access to a telephone that they can use within a reasonable distance and at a reasonable cost. This could either be in their own home, at a business, or some public facility. It is seen as an interim step.
- Universal Service and Universal Access measure different things, and require different policy measures.
 - Absolute Universal Access is achieved when 100% of the population has access to a given service.
 - Absolute Universal service is achieved when a given telecom service is affordable to 100% of individuals or households



New Definition of Universal Service



- Need to modify the definition of what is UA and what is US
 - Is it voice, dial-up Internet access, or Broadband
 - Do we need to have different definitions for Urban as opposed to Rural?
 - What about Voice and Internet?
 - Is there a need to create a new term, such as UAS that covers all three of these issues?
- Need to move away from defining Universal Access by technology and move to defining it by its usability.
- New definition: Universal Access --as the ability for a government to make it possible for someone to use technology to its full potential.
 - In this definition, Universal Access empowers people in rural and underserved areas by providing them with the ability to harness the power of the Internet.
 - This definition moves us away from a numerical counting of technology to ensuring that those having these technologies know how to use it effectively to make a difference in their day-to-day lives.



Universal Access Concepts



Issues	Basic Meaning	Differentiation
Availability	Coverage of inhabited geographic territory	Region/Area Locality/Size
Accessibility	All people can use	Gender, Race, tribe, religion Ability /disability
Affordability	Ability to Pay	Access device (Handset, PC, subscription costs) • Cost of calls & services • Minimum "basket" below a certain national limit (e.g., 3% of family income)



Universal Access Measurement



- Need to find better ways of measuring success of UA programs moving away from coverage to usage and quality of service
- The question then becomes are people able to use the access they have? Or is climbing a tree the only way they can get service? And does this count towards meeting UAS goals?
- Is Broadband defined differently in urban areas as opposed to rural areas?
 - What are the allowed contention ratios?
- UAS goals will continue to rise with technology & service development – towards e-Inclusion
- Focus shifts away from simple access to:
 - Bandwidth/speed, ICT capacity/ability, Applications/services





Trust



Trust



- Trust is a key ingredient for a sustainable, evolving and global Internet.
 - It is the cornerstone for all successful connectivity strategies
 - An 'open and trusted Internet' is a globally interoperable Internet that cultivates innovation and creates opportunities for all.
 - Its foundation lies in user trust, technologies for trust, trusted networks and trustworthy ecosystem.
- Without trust, users feel vulnerable and marginalized and are reluctant to take advantage of the many legitimate benefits that the Internet offers.
- Privacy is one of the biggest challenges regarding identity on the Internet.



Building User Trust



- User trust is important to the future success of the Internet because if users do not trust the Internet, they will restrict their use, and may even cease using it for certain activities.
 - This could have a serious impact on the evolution of the Internet, its use and growth.
 - Building user trust does not just mean simply reassuring people and hoping for a positive outcome.
 - Building user trust means putting in place the right infrastructure (trusted networks), empowering users to protect their activities (technologies for trust), setting the right policies, and providing a responsive environment that properly addresses users' well-founded concerns (trustworthy ecosystem).



Technologies of Trust



- Technologies for trust are the technical building blocks for establishing and maintaining trusted networks, applications and services.
 - They are the technical foundation for a trusted Internet
 - These Technologies are used to secure the networks, applications and services that we use everyday.
 - Without encryption, governments, companies and individuals would not be able to keep their communications confidential and their information secure.
- As threats continue to emerge and grow, we must ensure we all have the necessary tools for privacy, security, and, ultimately, economic and social opportunities.
- We need policies that support rather than hinder the development, availability and use of trust technologies.





Data Protection and Privacy



Data Protection



- Data Protection Laws are legislation enacted to protect personal, commercial, and governmental data from unauthorized access, alteration (corruption), destruction, or use.
- Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data.
 - It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

52

 Data protection is also known as data privacy or information privacy.



Data Protection Definition



- Data protection deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.
 - The context of data protection varies and the methods and extent also vary for each;
 - Use of techniques such as file locking and record locking, database shadowing, disk mirroring, to ensure the availability and integrity of the data.



GDPR



- The General Data Protection Regulation is a rule passed by the European Union in 2016, it replaced the previous 1995 Data Protection Law
 - This current law sets new rules for how companies manage and share personal data.
 - In theory, the GDPR only applies to EU citizens' data, but the global nature of the Internet means that nearly every online service is affected, and the regulation has already resulted in significant changes for US users as companies scramble to adapt.

-The Rules went into effect on May 25, 2018

- Much of the GDPR builds on rules set by earlier EU privacy measures like the Privacy Shield and Data Protection Directive, but it expands on those measures in two crucial ways.
 - First, the GDPR sets a higher bar for obtaining personal data
 - Under GDPR, any time a company collects personal data on an EU citizen, it will need explicit and informed consent from that person.
 - Users can request all the data a company has from them as a way to verify that consent or they can revoke their consent.

GDPR (Continued)



- The GDPR sets rules for how companies share data after it has been collected
 - This means companies have to rethink how they approach analytics, logins, and, above all, advertising.
- It adds complex new requirements for any company that gets user data secondhand, requiring a lot more transparency on what a company is doing with your data
- It alters how businesses and public sector organizations can handle the information of their customers.
 - It also boosts the rights of individuals and gives them more control over their information.
- Under GDPR, the "destruction, loss, alteration, unauthorized disclosure of, or access to" people's data has to be reported to the data protection regulator.



GDPR (Continued)



- Additionally, companies that have "regular and systematic monitoring" of individuals or process a lot of sensitive personal data have to employ a data protection officer (DPO).
- There is also a requirement for businesses to obtain consent to process data.
- The regulation also gives individuals the power to get their personal data erased in some circumstances.
- One of the biggest, and most talked about, elements of the GDPR has been the ability for regulators to fine businesses that do not comply with it.
 - If an organization does not process an individual's data in the correct way, it can be fined.
 - If it does not have a data protection officer, it can be fined. If there is a security breach, it can be fined.



Privacy



- Data privacy and data protection are very closely interconnected, so much so that users often think of them as synonymous.
- But the distinctions between data privacy vs. data protection are fundamental to understanding how one complements the other.
- Privacy concerns arise wherever personally identifiable information is collected, stored, or used
- Data protection is about securing data against unauthorized access.
- Data privacy is about who is authorized to have access to this information.
- Another way to look at it is: data protection is a technical issue, while data privacy is a legal one.



Privacy-Definition



- Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion.
 - The right to be free from surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed.
- Information privacy is the right to have some control over how your personal information is collected and used.
- As the technology gets more sophisticated, so do the uses of data. And that leaves people facing an incredibly complex risk matrix for ensuring that personal information is protected.
- As a result, privacy has fast-emerged as perhaps the most significant consumer protection issue today—in the global information economy.



Data Privacy Definitions



- Data privacy is focused on the use and governance of personal data—things like putting policies in place to ensure that consumers' personal information is being collected, shared and used in appropriate ways.
- Security focuses more on protecting data from malicious attacks and the exploitation of stolen data for profit.
 - While security is necessary for protecting data, it's not sufficient for addressing privacy.
- When comparing data privacy vs. data protection is that data privacy can only be ensured through a technology approach.
 - If someone can steal your personal data, than that the privacy of your data is not guaranteed, which puts you at risk for identity theft and other personal security breaches.
 - But the opposite relationship is not necessarily true: personal data can be protected while still not being reliably private.



Privacy (Continued)



- The point is technology alone cannot ensure the privacy of personal data.
- Most privacy protection protocols are still vulnerable to authorized individuals who might access the data.
- Technology is still implicated in data privacy, precisely because the authorized users of technology have a responsibility to the privacy law.
 - In short, no number of technological safeguards can eliminate the central role of trust in ensuring data privacy.
- The only mode of protection that personal data in transit can rely on is encryption, so that an unauthorized third party may see the data but not read or collect it.
 - With end-to-end encryption, however, the only "authorized users" (you and the recipient) with known IP addresses can get through the privacy shield and gain access to the data.





Encryption



Copyright 2018 ©. The Institute for Public Private Partnerships, a Tetra Tech company PPP Solutions For a Complex World



- Encryption technologies enable Internet users to protect the confidentiality of their data and communications from unwanted observation and intrusion.
- Electronic encryption is the process of scrambling or enciphering data so it can be read only by the person who has the key to unscramble it.
- Modern encryption scrambles data using a secret value or key known only by the recipient and the sender. For stored data, the secret value typically is known only by the data owner.





- There are four types of Encryption Techniques:
 - Symmetric encryption uses an identical key to encrypt and decrypt the message. Both the sender and the receiver have access to the same key
 - Asymmetric encryption, also known as public-key encryption, is a oneway form of encryption. Keys come in pairs, and information encrypted with the public key can only be decrypted with the corresponding private key. The recipient publicly publishes a key for the sender to encrypt their data. The recipient then uses a private key to decrypt the data.
 - End-to-end encryption is any form of encryption in which only the sender and intended recipient can read the message.
 - Data-at-rest encryption is any form of encryption that protects data physically stored in a digital form



Encryption Challenges



- The security-privacy conundrum. Policy debates about encryption present the issue as security versus privacy, a matter of balancing the responsibility of governments to protect their citizens versus the rights of citizens to protect their privacy from government, commercial, or criminal intrusions.
 - But this is not really accurate as encryption is the technical foundation for trust on the Internet. Without trust there is no freedom and much less growth of ecommerce.
- Encryption backdoors. This is the concept that a tool can help an authorized third party. i.e., the Government, gain access to and decrypt encrypted data without access to keys.
 - The technical consensus is that introducing backdoors puts legitimate users at risk and is unlikely to prevent criminals from communicating clandestinely. Bad actors will likely find alternative means of communicating, while average users may not have the same tools.



Encryption Challenges (continued)



- Tamper-resistant technology. This technology is designed to make it difficult for attackers to modify technology, and to make any tampering evident.
 - Used in conjunction with encryption, antitampering measures can help prevent (1) entry to a device after repeated login attempts; and (2) the installation of encryption backdoors, rootkits (malicious code designed to access different areas of a computer without authorization), and other malicious software.



Encryption Recommendations



- Encryption should be the norm for all Internet traffic. This is why a group of technical organizations have joined together to enable all consumers to benefit from encryption.
 - Let's Encrypt is a free, automated, and open certificate authority (CA), run for the public's benefit. They provide people with the digital certificates they need to enable HTTPS (SSL/TLS) for websites, for free,
- Designers and developers of digital products and services are strongly encouraged to ensure that users' data, whether stored or communicated, are encrypted by default.
- End-to-end encryption solutions should be made available to all wherever possible.
- Network and service operators are encouraged to deploy encryption and firewall policy administrators are urged to allow encrypted traffic.

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.

Cybercrime (Continued)



- Cybercriminal activity may be carried out by individuals or small groups with relatively little technical skill or by highly organized global criminal groups that may include skilled developers and others with relevant expertise.
- Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for executing most types of cybercrime.
- Phishing email is an important component to many types of cybercrime, but especially so for targeted attacks, like business email compromise (BEC), in which the attacker attempts to impersonate, via email, a business owner to convince employees to pay out bogus invoices.



Cyber Crime and 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.
- Typical Cyber Crimes 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.

70

 Malware: An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.



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.





- 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.


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.



Cybersecurity (continued)



- Electronic security protocols also focus on malware detection ideally in real time.
- 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.



Cybersecurity (continued)



- The US's National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.
- In the US, the Department of Homeland Security (DHS) is the agency responsible for Cybersecurity and for strengthening the security and resilience of cyberspace
- The international community has been trying to develop cybernorms for international behavior for over a decade.
 - This has been happening through UN processes, through the Global Commission on Cyberspace (GCCS), through international law discourse, and other fora.



The GCSC



- The Global Commission on the Stability of Cyberspace (GCSC) (a multistakeholder commission of experts) sets out to bring perspective by developing 'proposals
- The GCSC is charged with developing proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace
 - One of the outcomes of the 2015 GCCS meeting in The Hague was the establishment of 'the Global Forum on Cyber Expertise'.
 - Their declaration not only sets out an agenda around five themes (Cyber Security Policy and Strategy, Cyber Incident Management and Critical Infrastructure Protection, Cybercrime, Cyber Security Culture and Skill, and Cyber Security Standards), it also clearly defines its guiding principles for reaching these goals.





Internet of Things



Copyright 2018 ©. The Institute for Public Private Partnerships, a Tetra Tech company PPP Solutions For a Complex World

Internet of Things



- The term "Internet of Things" refers to "scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention.
 - IoT includes consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and more.
 - It presents a new way for users to interact with the network, using devices that are not limited to traditional computers, smartphones, and laptops.
 - Compromised IoT devices, such as webcams or even lightbulbs, can be used to form "botnets", networks of Internet-connected externally controlled devices.



IoT Security



- Poorly secured IoT devices and services can serve as entry points for cyber attacks, compromising sensitive data and threatening the safety of individual users.
- Attacks on infrastructure and other users, fueled by networks of poorly secured IoT devices, can not only affect the delivery of essential services such as healthcare and basic utilities, but also it puts the security and privacy of others at risk, and threatens the resilience of the Internet globally.
- Understanding the growing impact that IoT security has on the Internet and its users is critical for safeguarding the future of the Internet





Internet Shutdowns



Copyright 2018 ©. The Institute for Public Private Partnerships, a Tetra Tech company PPP Solutions For a Complex World

www.ip3.org

Internet Shutdowns



- An Internet shutdown can be defined as an "intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location often to exert control over the flow of information.
- An internet shutdown happens when someone (usually a government) intentionally disrupts the Internet or mobile apps to control what people say, see or do.
- A shutdown can take two forms:
 - A total shutdown or blackout where all services on the Internet are blocked off, targeting mobile Internet access and/or fixed lines, such that users in a country or region are not able to access the Internet.
 - A partial shutdown, where content blocking techniques are applied to restrict access to websites or applications, very often to block people from communicating or sharing information amongst them.

Impacts of Internet Shutdowns



- Internet shutdowns have far-reaching rights, economic, and technical impacts.
 - They undermine users' trust in the Internet, setting in motion a whole range of consequences for the local economy, the reliability of critical online government services and even for the reputation of the country itself.
 Policymakers need to consider these costs alongside security imperatives.
- Internet shutdowns affect economies in numerous ways, disturbing productivity and generating monetary losses in time-sensitive transactions.
 - Studies have shown that there is a real impact of shutdowns on countries' GDP. Brookings, in their study showed that Internet shutdowns cost countries about USD 2.4 billion between July 1, 2015 and June 30, 2016, with maximum losses incurred by India (USD 968 million).
 - Deloitte estimated that even countries with low levels of Internet access can suffer an average estimated GDP impact amount of USD 6.6 million per day

Impacts of Internet Shutdowns



- Beyond macro-economic impacts, shutdowns also affect businesses and SMEs, in Cameroon, local entrepreneurs lost contracts and could not conduct important transactions, leading to loss of money, business closures and firing of employees
 - Businesses that are heavily dependent on electronic transactions are particularly exposed to very serious consequences such as bankruptcy.
 - In Kashmir, pharmacies cannot get supplies since these can only be ordered electronically and paid for electronically
- Besides the financial impacts, the secondary economic impacts resulting from shutdowns can potentially discourage foreign investors and spillover on a wide range of sectors, including the tourism industry



Internet Shutdowns in Context



Internet Shutdowns in Context

Insights from the Shutdown Tracker Optimization Project (STOP)



Challenges of Internet Shutdowns



- Governments do have legitimate concerns and duties to safeguard public order and national security for their citizens, but there are other ways of going about this. They could target the specific people causing these security issues and not the entire country.
 - Any measure that restricts free expression or association to advance these objectives must remain exceptional, be grounded in law and be strictly necessary and proportional to achieve a legitimate aim.
- Shutdowns undermine commitments to the UN Sustainable Development Development Goals that all nations have agreed to. SD9 states that governments commit to ensuring universal and affordable Internet access by 2020.

85

Internet shutdowns are in conflict with this commitment



Internet Shutdowns



- There is currently no evidence of the effectiveness of shutdowns to restore public order. On the contrary, there are multiple accounts of severe economic damage and other collateral damages provoked by these measures.
- The only way to solve these issue is through a sustained dialogue between governments, private sector players, the technical community, academia, and civil society.
- Governments should be cognizant that shutdowns affect many sectors of society and it is imperative to engage in an open exchange to seek alternative ways of addressing legitimate issues, rather than turning to shutdowns as a policy tool.
- Governments should instead think twice about the economic and social impact shutdowns cost to their country
 - Network disruptions hinder productivity, adversely impacts business confidence, and are often detrimental to short and long-term investments.



Platform Liability



- Digital platforms play a central role in the economy and our everyday lives. Each platform has distinct characteristics, but in recent years specific concerns have grown around their dominance in the marketplace and impact on key parts of daily life.
- Public demands for Internet platforms to intervene more aggressively in online content are steadily mounting.
- First we must define the term "digital platforms"
 - A service accessed via the internet;
 - the service is two-sided or multisided, with at least one side open to the public and allows members of the public to produce content, buy and sell goods or services, or otherwise interact in ways that enable them to be more than simply passive consumers of goods and services; and,

87

The service enjoys Reed- or Metcalf-type network effects



Defining What is a Digital Platform



- The question of defining "digital platforms" is not simply important for market definitions in any antitrust analysis.
- It also relates to what constitutes appropriate standards of conduct and consumer protection.
- The bulk of regulation designed to promote competition generally applies only to dominant firms.
- Traditionally, in Antitrust policy, we have divided activities into lines of business and determine what sort of behaviors harmed consumers, but with digital platforms they potentially perform multiple diverse functions in diverse markets simultaneously.
 So the traditional way of dividing markets and declaring dominance does not work.



Digital Platforms: Is Regulation the Answer



- Public demands for Internet platforms to intervene more aggressively in online content are steadily mounting.
- Calls for companies like Google, Apple, YouTube, Facebook, Amazon, Twitter and Microsoft to fight problems ranging from "fake news" to online radicalization seem to make daily headlines all over the world.
- Efforts to impose some sort of regulation or taxes on these providers are heard often in the halls of parliaments all over the world
- Experience and economics tell us that digital platforms have a strong, perhaps overwhelming, tendency to concentration. But it also tells us that trying to impose regulations that do not make sense will cause economic harm to all
- We need to work with all partners in this digital world to create regulation that will work.
 - This might include creating one agency that has ongoing oversight of the sector and also creating a new regulatory toolkit for competition.







Thanks Questions, Comments, **Suggestions** Judith Hellerstein Hellerstein & Associates Judith@jhellerstein.com www.jhellerstein.com Whats App-+12023336517

