CELTIC Telecommunication Solutions

CELTIC Project Number:	**C2012/2-5**
Project Title:	SDN Concept in Generalized Mobile Network Architectures – SIGMONA
Confidentiality:	PU[1]

Document Identifier:	D5.2
Document Title:	**Analysis of direct impact of new network technologies on Regulation**
Main Author:	Jukka Salo
Contributors:	NOKIA, CWC, NEXTEL, TUC, AALTO
Work Package:	WP5
Version:	1.0
Date of last changes:	17.2.2015
File Name:	SIGMONA D5.2 – Analysis of direct impact of new network technologies on Regulation.doc

Abstract:

Keywords:

Disclaimer:

Document History:	
19.1.2015	Document created
17.2.2015	The first version 1.0 approved in the WP5 internal review

[1] Dissemination level:
PU = Public
RE = Distribution to a group specified by the consortium
CO = Confidential, only allowed for members of the consortium

Table of Contents

Authors

Partner name	Person name / Phone / email
NSN	**Jukka Salo**
	Phone: +358 40 546 1392
	e-mail: jukka.salo@nsn.com
University of Oulu / CWC	**Madhusanka Liyanage**
	Phone:
	e-mail: lliyanag@ee.oulu.fi
NEXTEL	**Oscar Lopez**
	Phone:
	e-mail: olopez@nextel.es
Technical University of Chemnitz	**Thomas Knoll**
	Phone:
	e-mail: knoll@etit.tu-chemnitz.de
AALTO University	**Nan Zhang**
	Phone:
	e-mail: nan.zhang@aalto.fi

Executive Summary

The new technologies under study in the SIGMONA project can become viable only if the economic advantage of their deployment becomes feasible. Besides the business aspects, the regulation aspects of the operated networks need to be taken into consideration in order to create a healthy market environment. The goals of the regulatory activity in the telecommunications industry can be described as to promote competition and to supply a country with sufficient and adequate services. The regulatory process is time consuming to administer and requires considerable expenditure of resources. It should focus only on those parts of the ICT sector where there is a clear need for regulation and should aim to establish or restore the conditions that support effective competition on a sustained basis.

Regulation is affected by the technological development in three different ways. First, there is a direct impact, where new technologies lead to the development of new services and modes of delivery unforeseen by the existing regulation. Second, new technologies affect the overall market structure and the level of competition by changing conditions for supply. Third, the new technological opportunities create a demand for new types of services, which again affect the overall market structure. **In this study the focus was on the direct impact** of new technologies on Regulation, especially from the perspectives of issues in **Interconnections** and **Security and Privacy**.

The **interconnection** scenarios discussed in this study have introduced new technical interfaces, new actors for running the business and new roles for the actors. For boosting the competition, the interoperability across the technical interfaces and the fair Service Level Agreements (SLAs) between the involved parties have to be ensured. Also, running business across countries and regions requires that the rules are harmonised between them. This, in turn, requires that the regulatory authorities in different countries and regions cooperate.

All identified interconnection issues seem to have high impact on the regulatory goals for I*nvestments*, C*ompetition* and *Market entry*. The issues related to the ‘Availability, Capacity and Quality of Interconnection’ and ‘Interconnection charges’ seem to be the most important issues which the regulators need to pay attention to when the new technologies are deployed. The terms for Interconnection are of particular importance for small operators and new entrants, which are dependent on the access to incumbent operators’ network facilities.

Several **Security and Privacy** issues related to the new network technologies were identified in this study both on the Service Provider side and on the customer side. The wide scale deployment of Cloud Computing, Network Function Virtualisation (NFV) and Software Defined Networking (SDN) can trigger a number of security and data protection risks stemming mainly from the new interfaces, shared environments, new actors with different views and objectives on Security and Privacy, and from the more complicated value networks. Also, different countries have different laws regarding which kind of data may be hosted and where: clarification of applicable law governing the flow, processing and protection of data is desirable, so that both the Service Providers and customers (private and corporate) have clear understanding about which rules apply, where and how.

In the proposed Network and Information Security (“NIS”) Directive of the EU, three policy options for ensuring NIS have been assessed. Option ‘Regulatory approach’ is the preferred one given that under this Option the protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably. The analysis made in this SIGMONA study supports the assessment of the NIS Directive: Government regulation would best promote the targets for Security and Privacy.

Glossary and abbreviations

Better regulation	An EU strategy aimed to make sure that regulation is used only when necessary, i.e. simplifying the existing legislation or improving new Commission proposals with the help of impact assessments and public consultations.
Body of European Regulators For Electronic Communications (BEREC)	The Body of European Regulators for Electronic Communications (BEREC) deals with questions of EU telecoms regulation. The authority replaces the European Regulators Group (ERG) which has existed since 2005. BEREC's main task is to support and advise the telecommunications regulatory authorities of the EU Member States, the European Commission and the European Parliament. This activity mainly takes the form of reports and statements.
Bottleneck	In the general economic terms, a ‘bottleneck’ is some kind of deficiency in the availability or functioning of an intermediate good or service. Bottlenecks create problems for producers and consumers by increasing the costs of resource supply and/or output distribution. (FUTURE BOTTLENECKS IN THE INFORMATION SOCIETY, Report to the European Parliament, Committee on Industry, External Trade, Research and Energy (ITRE), June 2001, EUR 19917)
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Dominance	An extreme form of Market Power. While the definition of market dominance varies with the laws of different countries, a finding of dominance usually requires proof of a relatively high market share and the existence of significant market barriers to entry into the markets in which a firm is dominant.
Essential facility	An essential facility is a facility that cannot be circumvented or replicated by any reasonable means. The concept of essential facilities is thus restricted to facilities (intermediate services), and indicates the strongest level of market dominance – i.e. there is no effective competition, and there are no viable alternatives. (FUTURE BOTTLENECKS IN THE INFORMATION SOCIETY, Report to the European Parliament, Committee on Industry, External Trade, Research and Energy (ITRE), June 2001, EUR 19917)
Ex ante regulation	The process of establishing specific rules and requirements to prevent anti-competitive or otherwise undesirable market activity by operators **before** it occurs.
Ex post regulation	It relies primarily on competition law, involves establishing few or no specific preventive rules in advance, but instead remedying and punishing market failure or anti-competitive behaviour **after** it has occurred.
Externality	In economics, an externality (or transaction spillover) is a cost or benefit, not transmitted through prices, incurred by a party who did not agree to the action causing the cost or benefit. A benefit in this case is called a positive externality or external benefit, while a cost is called a negative externality or external cost (Wikipedia)
Interface	The logical or physical connection between two networks, systems or devices; the point of interconnection of two components and the basis on which they exchange signals according to some hardware or software protocol.
License	A telecommunications license generally refers to the authorization to provide telecommunication services or operate telecommunications facilities. A telecommunications license usually defines the terms and conditions on which the license is authorized to operate and sets out its rights and obligations.
LTE	Long-term Evolution; 3GPP standard for wireless communication of high-speed data for mobile phones and data terminals

Market Failure	Market failure is a concept within economic theory wherein the allocation of goods and services by a free market is not efficient. That is, there exists another conceivable outcome where market participants' overall gains from that outcome would outweigh their losses (even if some participants lose under the new arrangement).
National Regulatory Authority	The regulatory agency or official at the central or federal government level that is charged with implementing and enforcing telecommunication rules and regulations. See Regulator below.
Net neutrality	Net neutrality (also network neutrality or Internet neutrality) is the principle that Internet service providers and governments should treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, and modes of communication (Wikipedia: http://en.wikipedia.org/wiki/Net_neutrality)
Network Function (NF)	A functional building block within an operator´s network infrastructure, which has well-defined external interfaces and a well-defined functional behavior. Note that the totality of all network functions constitutes the entire network and services infrastructure of an operator/service provider. In practical terms, a Network Function is today often a network node or physical appliance.
Network Function Virtualization Infrastructure (NFVI)	The Network Function Virtualization Infrastructure (NFVI) contains all the hardware and software components that constitute the environment in which VNFs of the MNO are deployed, managed and executed. The NFVI includes resources for computation, networking and storage.
Network virtualization	The process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network. Network virtualization involves platform virtualization, often combined with resource virtualization.
P-GW	Packet Data Network (PDN) Gateway
Rate of Return Regulation (RoR)	Is a rules-based form of price regulation designed to provide the regulated operator with relative certainty that it can meet its revenue requirements and that price will be adjusted, as required to meet that objective. Under this scheme, the regulated operator's revenue requirement is calculated and then service prices are adjusted so that it's overall service revenues cover such revenue requirement.
Regulation	A regulation is a form of secondary legislation which is used to implement a primary piece of legislation appropriately, or to take account of particular circumstances or factors emerging during the gradual implementation of, or during the period of, a primary piece of legislation
Regulator	This term is used to refer to government agency, institution or official responsible for regulation for all or part of the telecommunications sector in a country. In some countries it is a National Regulatory Authority (NRA), an independent regulatory authority, or a Ministry of Government. Sometimes, one entity is the regulator for some purposes and other entity for other purposes.
Software Defined Networking (SDN)	Software Defined Networking (SDN) is an emerging network architecture where network control is decoupled from forwarding, and is directly programmable (ONF White Paper: https://www.opennetworking.org/sdn-resources/sdn-library/whitepapers
S-GW	Serving Gateway
SP	Service Provider
Technology neutrality	States that any available technology (past, present or future) could be employed to provide certain service. In simple terms, regulators should let the market decide which technology should be used for a particular purpose. Together with service neutrality it forms the flexible approach to spectrum in the review.
Universal service	The practice of providing a basic set of telecommunications services to residents of a country at an affordable price.
Virtualization	Hardware virtualization or platform virtualization refers to the creation of a virtual machine (VM) that acts like a real computer with an operating system, but is separated from the underlying hardware resources. Technology allows servers

	and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.
Virtualised Network Function (VNF)	An implementation of an executable software program that constitutes the whole or a part of an NF that can be deployed on a virtualisation infrastructure.

API	Application Programming Interface
CAPEX	Capital Expenditure
CCIF	Cloud Comuting Interoperability Forum
CSP	Cloud Service Provider
eNB	Evolved Node B (eNodeB)
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
E2E	End-to-End
GTP	GPRS Tunneling Protocol
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
LTE	Long Term Evolution
MM	Mobility Management
MME	Mobility Management Entity
MNO	Mobile Network Operator
MVNE	Mobile Virtual Network Enabler
MVNO	Mobile Virtual Network Operator
NF	Network Function
NFV	Network Functions Virtualisation
NFVI	NFV Infrastructure
OPEX	Operating Expenses
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-GW	Packet Data Network (PDN) Gateway
PLMN	Public Land Mobile Network
QoE	Quality of Experience
QoS	Quality of Service
RAT	Radio Access Technology
SDM	Software Defined Monitoring
SDMN	Software Defined Mobile Network
SDN	Software Defined Networking
S-GW	Serving Gateway
TNO	Transport Network Operator
UCI	Unified Cloud Interface
UE	User Equipment
VM	Virtual Machine
VMNO	Virtual Mobile Network Operator
VNF	Virtualised Network Function
VPN	Virtual Private Network
WLAN	Wireless Local Area Networks

1. Introduction

The development path of any industry or economic sector is significantly affected by the opportunities provided by the available technologies, the particular characteristics of its markets and the directions and priorities of related government policies and regulations. These factors can be mutually supportive in stimulating growth and creating benefits, or they can conflict with one another, creating major blockages to development. Potential opportunities for development in a sector will arise from the interrelations among technologies, markets and policies. This has been, and will be, true also with respect to the telecommunication networks [10].

The combination of the new network technologies – i.e., Cloudification (Clouds), Network Function Virtualization (NFV) and Software Defined Networking (SDN) - will only become viable if the economic advantage of their deployment becomes visible. The structuring and modelling of the emerging business cases, which open up due to the introduction of these technologies, and the creation of detailed cost models of networking equipment (CAPEX and in particular OPEX model) are studied in Work Package 5 of the SIGMONA project. Besides the business aspects, the regulation aspects of the operated networks need to be taken into consideration in order to create a healthy market environment. The goals of regulatory activity in the telecommunications industry can be described as to promote competition and to supply a country with sufficient and adequate services.

Regulation is affected by the technological development in different ways. It is often difficult to draw a sharp distinction between different kinds of impact, because the same technology may affect the market structure and regulatory needs in several different ways simultaneously. In the SIGMONA project we have at first identified the potential regulatory issues, which may emerge when deploying new network technologies, and analysed their direct impact on Regulation. The focus areas in this work were Interconnections and Security and Privacy. The results of that work are reported in this document.

After the introduction given in this section, the document is structured as follows. In Section 2 the new technologies being studied in the SIGMONA project are briefly introduced. Section 3 introduces the current regulatory environment, including the goals and actors regulation, for instance. Section 4 includes an overall description to the regulation work in the SIGMONA project introducing the potential high-level approaches. The two focus areas of work, Interconnections and Security and Privacy, are discussed in Sections 5 and 6, respectively. Sections 7 and 8 provide the conclusions and the list of references. The Annexes have more detailed information on the business concepts in mobile virtual networks (A1), key concepts of Security and Privacy (A2), regulatory objectives in Cloud Computing (A3), guidelines for Security and Privacy proposed by National Institute of Standards and Technology (NIST) (A4), and on the arguments for impact assessment of Security and Privacy issues (A5).

2. Background – new technologies

There are several emerging technologies and enablers that could make new architectures feasible when implementing the future mobile networks. These technologies would allow, for instance, the virtual operator concepts, network sharing/slicing principles, and the separation of the control plane functionality from the user plane functionality and its cloudification.

Virtualization and Cloud Computing are evolving from the typical data center applications to the new areas. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. The general goal of Network Virtualization is to utilize a shared pool of configurable computing HW resources for the on-demand network access.

Software Defined Networking (SDN) is a term used for networks in which the control plane is decoupled from the data plane and made that control plane remotely accessible and remotely modifiable via third-parties' software clients. SDN requires some method for the control plane to communicate with the data plane. One such mechanism is the OpenFlow protocol.

Since the research on the techno-economic aspects related to the deployment of new technologies is ongoing in this project in parallel to this study, and the results from that research are not yet available when writing this report, short introductions on the generic deployment approaches of the new technologies are presented in the following sub-sections.

2.1 Cloud computing

Cloud computing is an expression used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time [47].

There are different deployment strategies for the Clouds technology [48]:

- **Private cloud** is a cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.
- A cloud is called a **Public cloud** when the services are rendered over a network that is open for public use. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services.
- **Community cloud** shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.
- **Hybrid cloud** is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

With the success of cloud technology in the enterprise realm, the telecom industry is now looking to the cloud to have the same benefits – economies of scale, cost effectiveness, scalability, lower CAPEX and OPEX. Operators want to exploit cloud technologies in their central offices and network functions to achieve these benefits.

In a Public cloud, organizations use Cloud Computing technologies through a **Cloud Service Provider (CSP)**. In a Private external cloud, Cloud Computing is still offered by a CSP. The difference between a Public cloud and Private external cloud is in the hardware: in a Public cloud the hardware is shared among different Cloud customers; in a Private external cloud, the hardware hosts the Cloud of only one customer. In a Private internal cloud, organizations use Cloud Computing technologies within the organization’s data centre.

2.2 Network Virtualisation, Network Functions Virtualisation

In today’s non-virtualised networks, Netwok Functions are implemented as a combination of vendor specific software and hardware, often referred to as network nodes or network elements. To launch a new network service often requires yet another network element, and finding the space and power to accommodate these boxes is becoming increasingly difficult, in additon to the complexity of integrating and deploying these elements in a network. Moreover, hardware-based network elements rapidly reach end of their reasonable lifetime: hardware lifecycles are becoming shorter as innovation accelerates, reducing the return on investment of deploying new services and constraining innovation in an increasingly network-centric worl.

Network Functions Virtualization (NFV) aims to address these problems by evolving standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage. It involves implementing network functions in software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required, without the need to install new equipment.

The operators and their may have the following benefits from exploiting the NFV [57]:

- Reduced operator CAPEX and OPEX through reduced equipment costs and reduced power consumption;

- Reduced time-to-market to deploy new network services;
- Improved return on investment from new services;
- Greater flexibility to scale up, scale down or evolve services;
- Openness to the virtual appliance market and pure software entrant;
- Opportunities to trial and deploy new innovative services at lower risk.

In addition to that NFV will change the ways how the existing operators run their network operations, it may also change the whole industry. It will enable [58]:

- decoupling supplier's HS and SW business models; new SW- only suppliers without Telco legacy;
- opening up new opportunities for SW integrators;
- step-changing for time-to-market of new functionalities;
- highly standardized and automated operation and management;
- re-engineer the Plan => Build => Run business process

From the operator's perspective, **NFV will enable more easy entries to market by Mobile Virtual Network Operators (MVNO)**. A more radical consequence from NFV could be that instead of building their own Virtualization Infrastructure, the operators could run their network in an Amazon cloud or become a Carrier's Infrastructure Provider [58].

The business concepts related to the Mobile Virtual Networks have been described further in Annex A1.

2.3 SDN

Software Defined Networking (SDN) is an emerging network architecture where network control is decoupled from forwarding and is directly programmable. This migration of control enables the underlying infrastructure to be abstracted for applications and network services. By centralizing network state in the control layer, SDN gives network managers the flexibility to configure, manage, secure, and optimize network resources for adapting to changing business needs. Moreover, they can write these programs themselves and not wait for features embedded in vendors' proprietary and closed software environments.

SDN is expected to deliver substantial benefits to both enterprises and carriers, including:

- Centralized management and control of networking devices from multiple vendors;
- Improved automation and management by using common APIs to abstract the underlying networking details from the orchestration and provisioning systems and applications;
- Rapid innovation through the ability to deliver new network capabilities and services without the need to configure individual devices or wait for vendor releases;
- Programmability by operators, enterprises, independent software vendors, and users (not just equipment manufacturers) using common programming environments, which gives all parties new opportunities to drive revenue and differentiation.

SDN provides a powerful complement to Network Funcations Virtualizations's (NFV) ability to maximum utilization of hardware resources. The concept of the Software Defined Mobile Network (SDMN) will change the network architecture of the current LTE (3GPP) networks. It will also open up new opportunities for the traffic, resource and mobility management, as well as impose new challenges on the network security. It is also foreseen that the investments on the networks and the operational costs would affected. Furthermore, **the value chains may change and new business models emerge**.

3. Regulatory environment

The development path of any industry or economic sector is significantly affected by the opportunities provided by the available technologies, the particular characteristics of its markets and the directions and priorities of related government policies and regulations [10]. These factors can be mutually supportive in stimulating growth and creating benefits, or they can conflict with one another, creating major blockages to development. Potential opportunities for development in the sector will arise from the interrelations among technologies, markets and policies. This has been, and will be, true also with respect to the telecommunication networks. Especially so, because they will play a ubiquitous and pervasive role in the daily life of people.

Policy, Governance and Regulation impact heavily on the values, norms and behaviour within a Value System, including rights and responsibilities of all actors (vendors, operators, users), competition models, profit sharing models, and IPR. They impact also into the structures inside and between Value Systems, including vertical and horizontal models.

Moreover, Policy, Governance and Regulation rules have a clear feedback loop towards the technology development and even value chain design on the business domain. Predictable and constant policies, governance and regulation are required to ensure that investment decisions and sensible planning can be done on this domain [63].

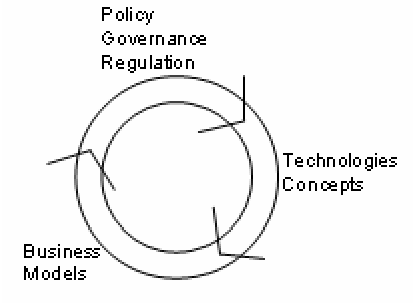

Figure 1: Feedback loop: Policy, Governance, Regulation – Technologies, Concepts – Business Models.

In the following sub-sections more details are presented on the regulatory goals and procedures, the relation between the competition law and Regulation, the specific regulatory issues, location of legal disputes, and actors and roles in Regulation.

3.1 Goals of Regulation

Today, the following targets for regulatory intervention are commonly accepted [1]:

- Increasing/ensuring **Consumer Welfare**. Consumer Welfare is ultimately determined by the structure and level of the retail prices paid by end consumers. The economic efficiency is a precondition to maximising consumer welfare.
- Ensuring rapid **innovation** and the introduction of new services through encouraging competition, where, it considers, competition will be effective and sustainable. Consumers can only enjoy superior services and products if the substantial investments to develop, create and produce these services are carried out.
- Promoting a favourable climate for **efficient and timely investment** and stimulating innovation, particularly by ensuring a consistent and transparent regulatory approach.

These regulatory targets can be understood also as the driving forces for regulatory actions related to the future mobile networks.

The generic regulatory objectives derived from the targets mentioned above are listed as follows [1][37][38][39] (key words bolded):

A) Encourage and attract stakeholders to **invest** in cost-efficient information infrastructure and technologies.

B) Ensure that through **competition** the telecom services are offered to customers in a cost-efficient way.

C) Ensure the availability of the essential requirements and mechanisms to facilitate **market entries** of new entrants in an adequate competitive environment, thus improving services and reducing charges.

D) Ensure that the right infrastructure is made available to customers in such a way that will continue to expand the scope and increase the value of telecommunication services offered to them (service and network **innovations**).

E) Support the operators to satisfy customers' needs and demands for affordable and high quality telecom services that enhance and improve customers' living and **efficiency** and productivity.

F) Since the future networks are critical infrastructures for the business and societal interactions, it is clear that ensuring **security, privacy and confidentiality** will be one of the key objectives when designing the new information sharing systems.

G) Encourage the operators to provide suitable and affordable telecom services to communities in non-profitable localities (**Universal Services/Universal Access**).

H) Ensure **justice** and efficiency for utilizing National Scarce Resources (e.g. Frequency Spectrum, Numbering).

I) Increase **national competitiveness** through use of ICTs.

Regulation has potentially also high costs. The regulatory process is inherently time consuming to administer and requires considerable expenditure of resources. In addition, regulation can have unintended consequences which may be detrimental to customers and the "public interest". No matter how capable and well intentioned regulators are, they will never be able to produce outcomes as efficient as a well-functioning market. Accordingly, Regulation should only focus on those parts of the ICT sector where there is a clear need for regulation (that is, where effective competition is not feasible) and should only be a temporary measure. Over time, regulators should aim to establish or restore the conditions that provide for effective competition on a sustained basis. This entails, for example, removing or reducing barriers to entry and exit. It also involves enabling the market itself to prevent the incumbent from abusing its market power, for example, through the entry of additional competitors [2].

3.2 Regulatory procedures

Regulation is a form of secondary legislation which is used to implement a primary piece of legislation appropriately, or to take account of particular circumstances or factors emerging during the gradual implementation of, or during the period of, a primary piece of legislation [10]. Regulators employ a variety of regulatory procedures. Depending on the legal framework, they may issue different types of regulatory instruments, such as regulations, decisions, orders, decrees, rules, policies, notices, resolutions. In general, the effect of these instruments is to make "decisions" that implement regulatory policies, resolve disputes, or deal with other matters within the regulators' mandate.

With the emergence of next generation networks, regulators are faced with the issue of deciding whether to implement an **ex post regulatory** model, or maintain **ex ante regulation**. Ex ante regulation refers to the process of establishing specific rules and requirements to prevent anti-competitive or otherwise undesirable market activity by operators before it occurs. The current regulatory framework for telecommunications was designed to transition former state-owned monopolies to a competitive environment. Therefore, the transition from ex ante regulation to ex post regulation is a natural continuation of the regulatory process. The next generation networks could require a new mind set and approach in regulation. Creating a framework for innovation and investment in infrastructure, in addition to securing the interconnection of networks, could possibly become a major issue for regulators in the future [64].

3.3 Competition law and Regulation

Market failures occur in many forms, and when they arise, it is necessary to consider whether the problem is likely to correct itself. If the market failures will not correct themselves, then there may be a need for additional tools to foster effective competition or to prevent socially undesirable outcomes.

The ICT Toolkit [2] introduces two broad approaches to promoting competition in the ICT sector, namely competition policy and regulation. Competition policy and regulation are not mutually exclusive.

Competition policy provides a set of tools to promote sustainable competition to preserve a market environment in which such competition can flourish. Competition policy may be implemented through general competition laws or through competition enhancing rules in specific sectors. In the ICT sector, such rules might include:

- General prohibitions on anti-competitive behaviour and mergers or acquisitions that would reduce competition, or
- Specific rules designed to encourage competition in the sectors, such as interconnection requirements or unbundling policies.

Competition laws (or "antitrust laws", as they are called in the US) aim to promote efficient competition by penalizing or undoing conduct that reduces competition in a market. Competition laws generally include provisions to:

- Prevent competing firms from banding together ("colluding") to increase prices or reduce quantities of goods and services, or to exclude other firms from a market,
- Prevent firms with a dominant position, or "significant market power", from using their market power to exclude competitors from the market, or otherwise reduce competition,
- Stop mergers or acquisitions that would reduce competition.

With the exception of provisions for mergers and acquisitions, competition laws are generally ex post regulation. They give the competition authority or the courts powers to respond to anti-competitive behaviour once it has occurred.

Regulation is useful where the market by itself would produce undesirable or socially unacceptable outcomes. Regulation attempts to prevent socially undesirable outcomes and to direct market activity toward desired outcomes. For example, ICT regulation is widely used to promote prices that reflect efficient costs and promote universal access to basic services.

3.4 Specific regulatory issues

In the following sub-sections a few, specific regulatory issues are presented. They are seen very relevant what comes to boosting of competition and new investments, and are discussed a lot in the in the Regulation related publications. They are (not in any order of importance) Bottlenecks; Barriers to entry and exit; Security and Privacy; Net neutrality; Interconnection; Non-discriminatory and equal access to systems and services; and Standardisation.

3.4.1 Bottlenecks

Bottlenecks refer to facility markets on which intermediate services such as networks and platforms are provided. Some facilities can be what are called **e*ssential facilities***. An essential facility is a facility that cannot be circumvented or replicated by any reasonable means. The concept of essential facilities is thus restricted to facilities (intermediate services), and indicates the strongest level of market dominance – i.e. there is no effective competition, and there are no viable alternatives [11].

Bottlenecks can be temporary, and in many cases market dynamics can generate acceptable solutions to many bottleneck problems. Bottlenecks requiring policy intervention generally arise because of asymmetries in the market that confer advantages on the suppliers of intermediate goods and services – such as monopoly or oligopoly structures. For policy purposes in an ICT, a 'bottleneck' can be said to exist where the availability and/or terms of access to a particular network facility or service environment fall below a benchmark or standard that has been deemed to be in the public interest. A significant dimension of access restriction concerns not just access by final users to a public infrastructure, but also access to the business environment of the public network by potential new market entrants [65].

3.4.2 Barriers to entry and exit

According to [2], a **barrier to entry** (typically in the long run) is a cost that a new entrant incurs, but that incumbent firms avoid. This cost asymmetry can prevent the potential entrant from competing with the incumbent even if its other costs are exactly the same as the incumbent's, and both face identical prices. Thus, barriers to entry may prevent entry by otherwise equally efficient competitors.

A **barrier to exit** is a cost (typically experienced only when exiting the market) that is so prohibitive that it can reduce, or destroy altogether, a firm's incentives to enter the market in the first place. Therefore, a barrier to exit may pose a barrier to entry as well.

3.4.3 Security and Privacy

The European Commission says in its press release[2] related to the Telecoms Council, Brussels, 31 March 2009, that 'ICT systems, services, networks and infrastructures form a vital part of European economy and society, either by providing essential goods and services or by constituting the underpinning platform of other critical infrastructures. They are often called Critical Information Infrastructures as their disruption or destruction would have a serious impact on vital societal functions'. This statement makes it clear that ensuring Security and Privacy (and confidentiality) will be key objectives when designing the new architectures of future telecommunication systems.

The key concepts of Security and Privacy are presented in Annex A.2.

3.4.4 Net neutrality

Net neutrality issues refer to the rights of subscribers to have the same level of connectivity when paying for the same level of service as well as to no limitations from the access operators and regulators. The U.S Federal Communications Commission has adopted three rules to preserve the openness of the network [66]. These rules include transparency of the network and no blocking of content. In addition, no unreasonable discrimination of content or applications is allowed.

Net neutrality deals directly with network access issues, thus the effect on universal access is high. For example, if regulation on network openness does not exist, some content will be discriminated against and access to that content is significantly lowered. In addition, if QoS requirements include privacy guarantees, it will improve the security and privacy of the service.

3.4.5 Interconnection

The purpose of an Interconnection regime is to benefit users by encouraging competition that will lower the price and improve the scope and quality of services. For competition to be successful at maximizing consumer benefits and innovation in telecommunications market, the telecommunication operators must have the opportunity to access all customers, even those customers connected to networks of their competitors.

The prices of Interconnection are in most countries regulated and cost-based. Cost-based prices can be determined in many different ways, and regulation can be either proactive or reactive. Reactive price regulation implies that the regulator assesses prices available on the market and intervenes only if prices are deemed to be above cost-based prices. Proactive price setting implies that the regulator announces price ceilings at regular time intervals.

3.4.6 Non-discriminatory and equal access to systems and services

Avoidance of discrimination is a central objective of most interconnection policies [1]. It should be noted that the interconnection arrangements may vary from one competitor to another without being 'unduly' or 'unjustly' discriminatory. Two competitors may have voluntarily agreed to different agreements, for example, to suit their different operating conditions. The real test, therefore, should not be "discrimination" in the sense of "differences" in Interconnection agreements. The test should be "unjust", "undue" or "unfair" discrimination, in the sense that an interconnecting competitor is placed at a significant disadvantage as a result of less favorable Interconnection agreement [1] (Module 3).

A specific type of discrimination, which can be fatal to the prospects of competition, involves providing insufficient network capacity to interconnecting operators as compared to an incumbent's own services.

[2] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/139&format=HTML&aged=0&language=EN&guiLanguage=en/

3.4.7 Standardisation

In the technology development phase, the standardisation of protocols and network equipments should be considered. However, if no common standards exist, the regulators should take command to ensure compatibility between networks and network equipments.

Standardization from one perspective is beneficial for most stakeholders because it guarantees system compatibility and thus universal access. Also from a financial perspective, standardization could be beneficial. For example, in the Blu-Ray vs. HD DVD war over the next generation DVD format, both camps invested a lot into the technology and both formats were sold in the market. When Sony's Blu-Ray format finally won, all the investments of Toshiba into HD DVD were for nothing and consumers were left with obsolete devices [67].

On the other hand, standardization reduces competition in the market in the short run as all will produce products with the same technology and the competing technology's supporters are forced to leave the market. In the long run, however, standardized technology lowers market entry barriers and thus increases competition when users can choose from any of the producers of a product or service.

When technology is standardized, it may decrease service innovation and network innovation in a market because no competition on the technology exists anymore. On the other hand, it may also increase innovation when actors cannot compete with the technology anymore and thus have to differentiate their product somehow.

3.5 Location of legal disputes

When a criminal offense has happened there is an issue which legislation should apply. There are, at least, three possible locations to choose from, that of the victim, that of the offender or that of the service provider [68].

The location of the victim seems a good way of protecting people's personal interest. That means that a provider must know what regulation applies to their customers. This might on the other hand make service provisioning overly complicated which might hamper the evolution of new services and markets.

Using the jurisdiction of the offender seems to be an obviously bad idea. This would provide an opportunity for 'scam havens' where remote stealing and fraud is legalized, similar to how tax havens have made business on providing an opportunity for people to avoid taxation.

The jurisdiction of the service provider might be a solution as that can provide sort of a neutral ground into which both the offender and the victim has to enter before contact can be made. The entering of the legal zone might be made either by explicit acceptance before connectivity can be established or it could be implicit as part of the service agreement with the service provider.

3.6 Actors and roles in Regulation

Some time ago in many countries a single Ministry or other government administrative unit performed the roles of telecommunications policy maker as well as owner and operator of the national telecommunications network. No need was perceived for a regulator in this environment. The same government officials were often involved in policy decisions, policy implementation, and operation of the telephone service. Privatization and market liberalization has led to a re-organization of the government institutions involved in the telecommunications sector. The most common institutional model used in the developed market economies around the world today is illustrated in Table 1 below [1].

Function	Responsible organization
Policy development	Government Ministry or Executive Branch
Regulation	Separate Regulatory Authority
Network Operation / Service Provision	PTOs (privately or commercially operated)

Table 1: Roles in policy settings and regulation.

This structure has the following features [1]:

- Government officials can set policies in the national interest, without conflicting concerns based on their role as owners, managers or employees of telecommunications operators. In particular, governments are more inclined to introduce significant competition in telecommunication markets if they do not also run the main operator.
- Separate regulatory authorities can implement government policy in an objective and impartial manner. Separation from state-owned telecommunications operators increases the ability of regulators to act impartially toward all market participants, for example in matters involving competition policy or interconnection. Market confidence in the impartiality of regulatory decisions generally increases with the degree of independence of regulators from both operators and governments.
- Privately owned operators can make rational economic decisions about the supply of telecommunications services, without conflicting concerns arising from government ownership.

Government awareness and support of telecommunications and ICT sector initiatives are essential, in order to mobilize resources necessary to define ICT policy and objectives, in particular.

Since the telecommunications infrastructure and markets are global by nature, global approaches are needed also in the area of policy, governance and regulation. However, the world from this perspective looks quite fragmented as shown in Figure 2 [69]: in 2014, there were 193 National Regulatory Authorities (NRA) worldwide, which are responsible for the economic regulation of the communications markets and for the supervision of the technical operability and safety of the communications networks in their countries (http://en.wikipedia.org/wiki/List_of_telecommunications_regulatory_bodies). In addition, there are a number of regional organisations, which are trying to harmonise the rules in a certain regional area. In Europe, for instance, the Body of European Regulators for Electronic Communications (BEREC) was established by Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009, as part of the Telecom Reform package [70][71][72]. It replaced the European Regulators Group for electronic communications networks and services which was established as an advisory group to the Commission in 2002.

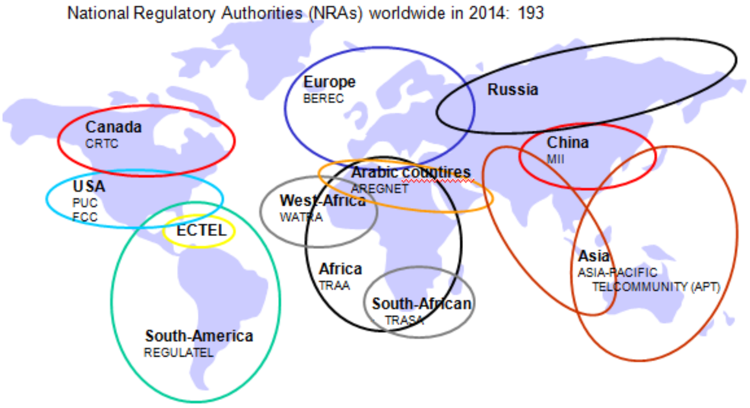

Figure 2: The International Regulator Landscape.

4. Overall approach to Regulation in SIGMONA

Regulation is affected by the technological development in three different ways (Figure 3) [2]. **First**, there is a direct impact: new technologies lead to the development of new services and modes of delivery unforeseen by the existing regulation. Use of the IP telephony, for instance, raises new issues with regard to the numbering and emergency services.

Second, new technologies affect the overall market structure and the level of competition by changing conditions for supply, which again affect the need for regulation. An example of this is the facility-based competition enabled through the use of cable broadcasting networks for the provision of Internet access.

Third, the new technological opportunities create a demand for new types of services, which again affect the overall market structure. The two most prominent examples are the introduction of mobile services and the introduction of the World Wide Web. The demand for mobile services created an entirely new market and enabled a number of new entrants providing their services in competition with the incumbent operators. In addition, as an example of the mobile services development, in Austria and Switzerland the mobile services superseded fixed line access, which at first led to a price reduction, but then showed a strong price increase after the almost completed fixed-to-mobile shift.

It is, however, often difficult to draw a sharp distinction between these three different kinds of impact, as the same technology may affect market structure and regulatory needs in several different ways simultaneously.

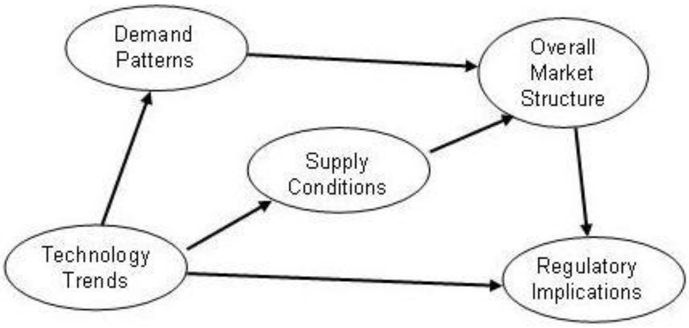

Figure 3: Direct and indirect regulatory implications.

In this study we have identified the potential regulatory issues, which may emerge when deploying the new Clouds, Network Virtualization and Software Defined Networking (SDN) technologies, and analysed their **direct impact** on Regulation. The impact analysis of the new business structures on regulation will be carried out in the next phase of the project work.

Because Interconnection (today it is more about Interoperability) and Securityand Privacy have been very much in the center of the regulatory work within the EU, and because they seem to be relevant also in the context of the new mobile network technologies, they were selected to be the focus areas in the regulation work of the SIGMONA project. In the following sections these two focus areas are discussed separately.

5. Interconnection regulation

The regulatory implications of the new cellular core network technologies on the Interconnection regulation are studied following the procedure, which is also illustrated in Figure 4 below:

1. At first, the concepts related to the virtual networks are clarified to better understand the different roles that the different actors may have in running the virtualized networks. This is already done in Section 2.
2. Secondly, the regulatory environment, concept of Interconnection, existing regulatory regimes, regulatory goals and generic issues in Interconnection are explained and discussed to better understand the regulatory environment with respect to Interconnection (Sections 3, 5.1, 5.2, 5.3, and 5.4) .
3. Then, the interconnection scenarios in the Mobile Virtual Networks are elaborated, starting with the typical interconnection scenarios without any reference to the new mobile core network technologies (Section 5.5).
4. The typical interconnection scenarios are then further elaborated taking into account the new business opportunities that the new technologies may enable. This work results in the potential issues which the regulators might need to pay attention to (Sections 5.6 and 5.8).

5. The impact of the new interconnection issues on the regulatory goals is then assessed; i.e., the direct impact of new technologies on Interconnection Regulation (Section 5.9). The regulatory goals have been derived from criteria of Economic Efficiency, i.e. the Best use of resources, Least-cost production, and Incentives for innovation (see Section 3.1).
6. In the final step, which is outside the scope of this document, the selected regulatory issues will be studied further in the next phase of the research, and actions will be proposed for Regulators to tackle those issues.

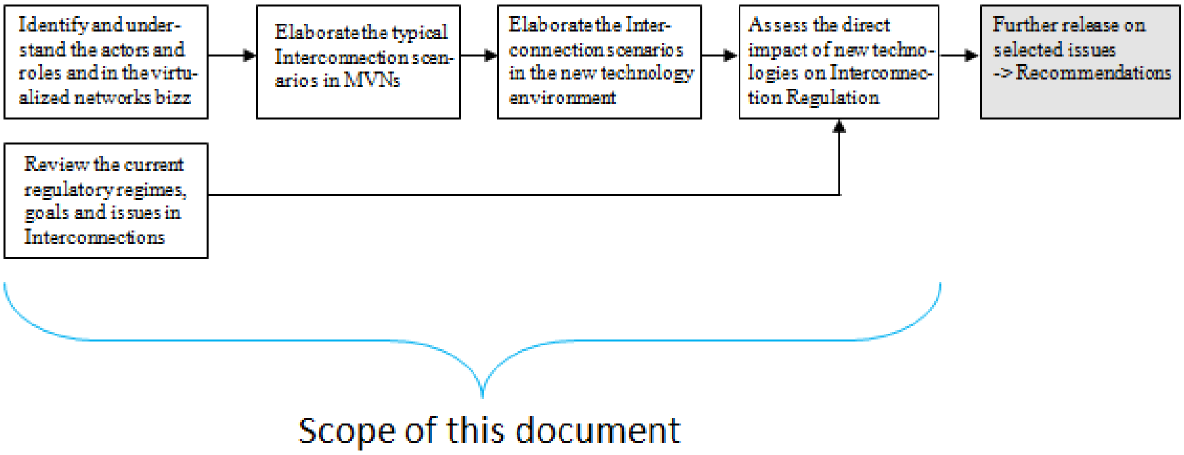
Identify and understand the actors and roles and in the virtualized networks bizz
Elaborate the typical Interconnection scenarios in MVNs
Elaborate the Interconnection scenarios in the new technology environment
Assess the direct impact of new technologies on Interconnection Regulation
Further release on selected issues -> Recommendations
Review the current regulatory regimes, goals and issues in Interconnections
Scope of this document

Figure 4. Approach to study the direct impact of new technologies on Interconnection regulation.

The focus of work in this study is on Interconnections of the Virtual Mobile Networks.

5.1 Concept of Interconnection

Interconnection is defined in different ways in the different regulatory and policy regimes that deal with it. A good definition is included in the 12 July 2000 proposed European Commission Directive on Access and Interconnection: *Interconnection means the physical and logical linking of public electronic communications networks used by the same or a different undertaking in order to allow the users of one undertaking to communicate with users of the same or another undertaking, or to access services provided by another undertaking. Services may be provided by the parties involved or other parties who have access to the network [51].*

The Cloud Computing Interoperability Forum (CCIF) was formed for the purposes of wider industry adoption of cloud-computing technology and related services. One output of this forum is a Unified Cloud Interface (UCI) requirement which is an attempt to create an open and standardized cloud interface for the unification of cloud API. The unified cloud interface (UCI) is focusing on inter-cloud interoperability [52].

As technology has changed, many forms of Interconnection have evolved. All of them involve the linking of networks to enable customers of one network to communicate with customers of another network, or to have access to services offered by another network operator.

5.2 Regulatory goals for Interconnections

According to ITU’s surveys [1], Interconnection related issues are ranked in many countries as the most important problem in the development of a competitive marketplace for telecommunications services. The purpose of an Interconnection regime is to benefit users by encouraging competition that will lower the price and improve the scope and quality of services. For competition to be successful at maximizing consumer benefits and innovation in telecommunications market, carriers must have the opportunity to access all customers, even those customers connected to networks of their competitors.

Interconnection is not a new issue, as it was necessary to interconnect the various national networks, each of them operated by national monopolies for enabling international communication. However, the liberalization of national telecom markets added a new dimension, as both supplementary and competitive networks now have to be interconnected.

Even though new technologies enable the creation of new alternative communication networks, the regulation of interconnection will still be an important tool for the facilitation of competition in both services and facilities.

Many regulators maintain that interconnection agreements are commercial agreements between the operators involved. It is therefore not the task of the regulator to draft the agreement, but only to ensure that agreements made are following the guidelines prepared by the regulator [2].

The goals of regulation are presented in Section 3.1. The same goals are relevant also for Interconnetions.

5.3 Interconnections and competition

Mobile telecommunication markets are shaped by network externalities. That means that as the number of subscribers of one MNO increases, the total benefit received by each individual for being a subscriber of that MNO also increases when all other variables which may have affects on welfare (e.g. price, quality) are held constant. The reason for such an increase is that the total number of subscribers of an MNO defines the number of people that each individual subscriber is able to communicate with. As every individual uses telecommunications service in order to be able to communicate with other people, it would not be wrong to claim that no one would want to be a part of a network, which only has few subscribers. No matter how high the quality of service is, or how low the prices are [53].[3]

As a result of network externalities, the first MNO that enters the market has a great competitive advantage over its future rivals. This is because the first mover of the market has potential to obtain a great number of subscribers before any other actor enters the market.

In the context of the transition from monopoly to competition, an incumbent telecommunications provider has a vastly superior market position and strategic interest to keep out or minimise competitors in its market area, which means that it has an incentive to limit Interconnection. If the incumbent, with the vast majority of customers, does not interconnect with new entrants, the new entrants will have little chance of attracting customers of their own. If promoting competition is an important goal, then the interconnection regimes need to be carefully designed to ease the way for firms to enter the telecommunications service industry [11] [4].

Interconnection between MNOs is mandated and highly regulated in many countries. The reason for this is that in many countries strong incumbent MNOs exist with a great deal of market power that refuses to interconnect with others on a voluntary basis. In these markets the interconnection regimes are defined by regulations in detail. In some countries, however, the MNOs decide to interconnect on a voluntary basis. In these markets the interconnection regimes are defined by the markets itself [53].

Many national regulators have found that their existing regulations cannot be applied to MVNOs without amendment. The general sentiment in EU is favorable to the business opportunity of new MVNOs [8].

5.4 Generic issues in Interconnections

According to Telecommunications Regulations Handbook [1], commercial, technical and operational arrangements must be made to facilitate Interconnection between network operators. A number of issues must be agreed upon by the operators, or determined by the regulator, in order to finalize these arrangements. Those issues can be divided into the following categories:

a) Framework and procedural issues

b) Commercial issues

c) Technical and operational issues

[3] Access to Internet (IP) makes many external (OTT) services available also to the subsciribers of a new entrant. Also, the usage of IP telephony very much circumvents the need for direct Interconnectionbetween the operator networks.

[4] See note 3.

Some key Interconnection issues in each category of the list above have been listed in the following:

a) Framework and procedural issues:
   - Adequacy of regulatory guidance for Interconnection negotiations
   - Independent and timely dispute resolution
   - Availability of Interconnection with incumbent operators for various types of services
   - Access to standard Interconnection terms with an incumbent operator
   - Non-discriminatory access to Interconnection facilities and services

b) Commercial issues:
   - Level and structure of Interconnection charges; basis for calculation (i.e. type of costs used to calculate charges, revenue sharing, bill and keep, etc.)
   - Unbundling of Interconnection charges for different network components and related services
   - Payment for network modifications to facilitate Interconnection
   - Confidential treatment of competitive and customer information

c) Technical and operational issues:
   - Open network standards and technical compatibility
   - Location of Points of Interconnection (POI)
   - Equal ease of customer access to competitive networks (e.g. customer dialing parity)
   - Quality of Interconnection, including availability of sufficient Interconnection capacity to avoid congesting, and to ensure the timely provisioning of Interconnection services and facilities
   - Access to numbers and implementation of number portability

5.5 Interconnections in Mobile Virtual Networks – typical scenarios

Mobile Virtual Network Operator’s (MVNO) outgoing and terminating traffic can take place in two alternative ways [59]:

- Traffic through its own Point of Interconnection, or
- Traffic through the Point of Interconnection of its hosting Mobile Network Operator (MNO).

The above listed ways apply also to traffic between the MVNO and its hosting MNO. In case of an own Point of Interconnection, the MVNO normally has its own switching facilities.

In the following subsections, different Interconnection scenarios between the Mobile Virtual Networks and other networks are presented. The notation presented in Figure 5, which is used to illustrate Interconnections and relationships between the actors, is based on the Casey et al´s industry architecture notation [9] with some slight modifications. In the modified version the Role and Technical component have been combined for simplicity.

In this study the focus is on the MVNOs (i.e. Full-MVNO, see Appendix A.1), where the Mobile Network Operator (MNO) just provides the access network infrastructure and, sometimes, a part of the core network, while the new actor provides the rest of the elements of the value chain.

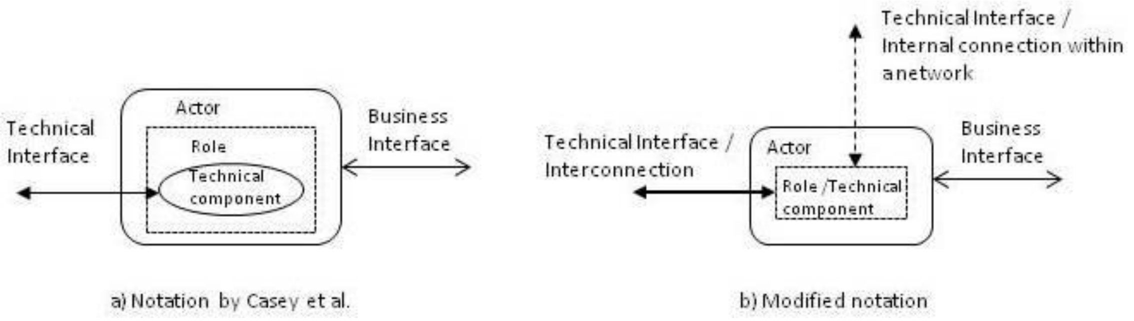
Technical Interface
Actor
Role
Technical component
Business Interface
a) Notation by Casey et al.
Technical Interface / Internal connection within a network
Technical Interface / Interconnection
Actor
Role /Technical component
Business Interface
b) Modified notation

Figure 5. Notation for illustrating Interconnection scenarios.

5.5.1 Typical scenario 1

In this scenario, illustrated in Figure 6, the hosting MNO-1 operates the access network and a major part of the core network. MVNO-A has leased a slice of the core network capacity from MNO-1 and operates it through the management interface. It is also possible that MVNO-A has purchased a part of the core network, and owns it.

MVNO-A provides its services as a network operator having its own interconnection links and interconnection agreements with other network operators.The interconnection link capacity has probably been leased from the hosting operator or from the Interconnection Provider.

Traffic between MVNO-A and its hosting MNO-1 may be routed via the specific Point of Interconnection, or such specific Point of Interconnections does not exist.

The calls between the MNO-1 and MNO-2 are routed through their own interconnection links as defined in their interconnection agreements.

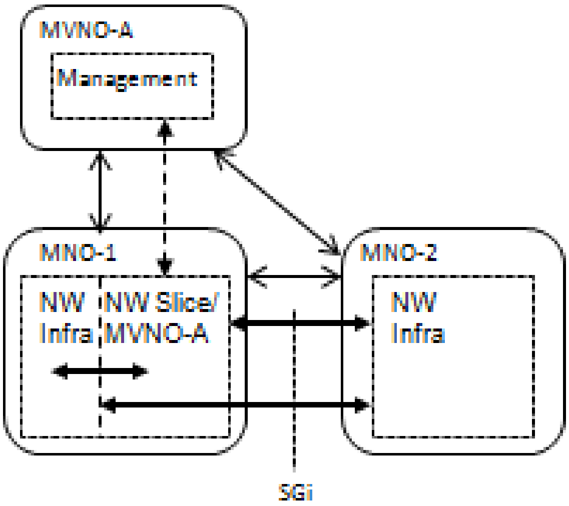

Figure 6. Typical scenario 1.

5.5.2 Typical scenario 2

In this scenario, illustrated in Figure 7, MVNO-A has made the leasing contracts with two (or several) MNOs, i.e. MNO-1 and MNO-2. The coverage of its network is the combined coverage of its contracted networks.

The hosting MNO-1 and MNO-2 operate their access networks and the major parts of their core networks. MVNO-A has leased the slices of the core network capacity from both MNOs and operates them through the management interface. MVNO-A provides its services as a network operator having its own interconnection links and interconnection agreements with other network operators (MNO-1, 2 and 3), and possibly with the Interconnection Provider.

Internal traffic between the MVNO-A subnetworks can take place via the internal connections, e.g. the leased lines, which are not considered here as Interconnections between operators. Traffic between the subnetworks may also be routed via the Point of Interconnection between MNOs (Note * in Figure 7).

Traffic between MVNO-A and its hosting MNO (MNO-1 and MNO-2) is routed via the Point of Interconnection, or such specific point does not exist.

Traffic between the MNO-1 and MNO-2 are routed through their own interconnection links as defined in their interconnection agreement.

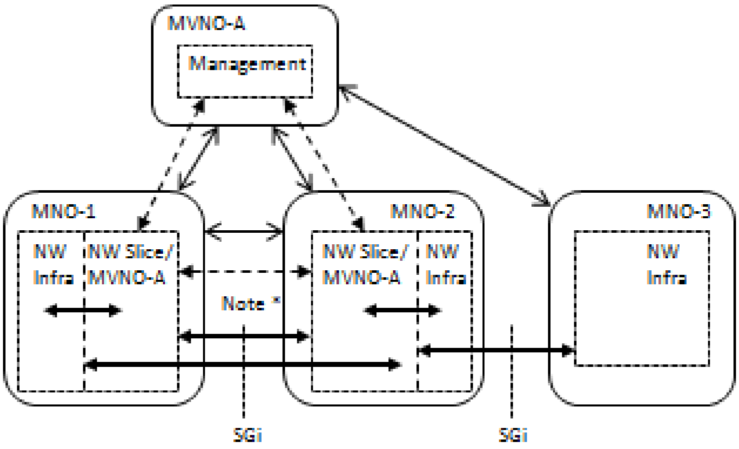

Figure 7. Typical scenario 2.

5.5.3 Typical scenario 3

In this scenario, illustrated in Figure 8, MVNO-A has made the leasing contract with MNO-1, and MVNO-B with MNO-2. MVNO-A and MVNO-B operate their network slices through the management interfaces.

The hosting MNO-1 and MNO-2 operate their access networks and major parts of their core networks.

Both MVNO-A and MVNO-B provide their services as network operators having their own interconnection links and interconnection agreements with other network operators (with the hosts, for example, as shown in Figure 8).

MVNO-A and MVNO-B have also the interconnection agreement and link between themselves.

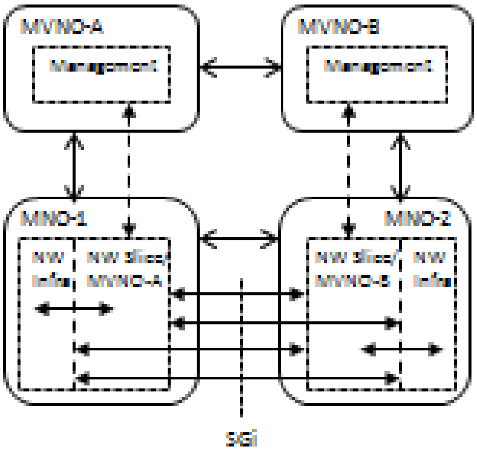

Figure 8. Typical Ssenario 3.

5.6 Interconnections in the context of the new mobile network technologies (SDN, Clouds, Network Virtualization)

In this section, the different interconnection scenarios, as presented in the previous section, are presented in the environment where the new technologies (SDN, Clouds, Network Virtualization) have been deployed by the Mobile Network Operators. The focus is on the MVNOs and their Interconnections. It is assumed that the Clouds technology is used for the scalability reasons.

5.6.1 Typical scenario 1 and new network technologies – version a

This scenario, illustrated in Figure 9, corresponds to ‘Typical scenario 1’ in the previous Section 5.5.1, where the hosting MNO-1 operates their access network and a major part of the core network. The Control Plane functions have been implemented with SW in the Telco Cloud, but they are not shown in the illustration for simplicity. The Telco Cloud is operated by MNO-1.

MVNO-A has leased a slice of core network capacity from MNO-1 and operates it through the management interface. It is also possible that MVNO-A has purchased a part of core network equipment for implementing that network slice. For simplicity, Figure 9 does not illustrate MNO-1’s part of the network capacity.

The User Plane functions have been implemented on both HW and SW [56]. It depends on the service, whether the “fast path” (P-GW-HW) or “slow path” (P-GW-SW) is used for routing the user traffic.

MVNO-A has the interconnection agreements with MNO-1 and MNO-2, and possibly with the Interconnection Provider. Interconnection between MVNO-A and MNO-2 (and Interconnection Provider) is via the SGi interface (irrespective of whether the slow path or fast path has been used).

In this scenario, the new network technologies do not bring such new aspects to Interconnection, which a Regulator should pay attention to: the actors and interfaces are the same as they are in the old network implementation architectures.

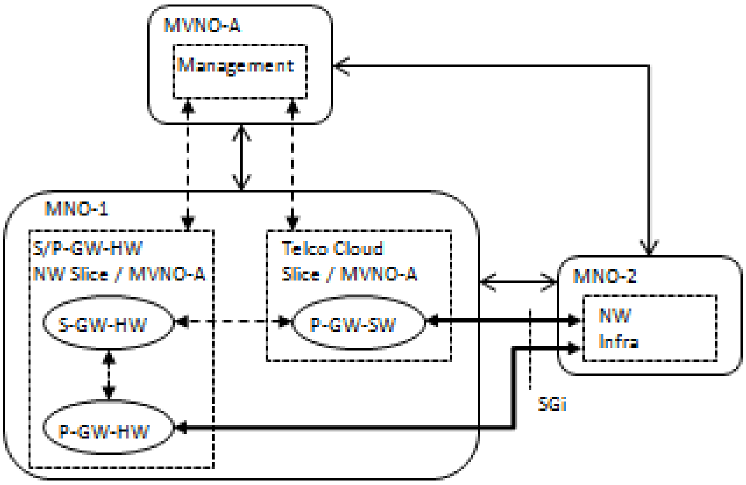

Figure 9. Typical scenario 1 with new technologies – version a.

5.6.2 Typical scenario 1 with new technologies – version b

This scenario, illustrated in Figure 10, corresponds to ‘Typical scenario 1’ in Section 5.5.1, where the hosting MNO-1 operates the access network and a part of the core network. MVNE is providing virtualization services to MVNOs (i.e., MVNE facilitates the entries of new MVNOs) and for that purpose it has leased the access network and core network capacity from MNO-1, and potentially also from other MNOs. MVNE has potentially, but not necessarily, also leased capacity from a Cloud Service Provider (CSP) for running a part of the core network functions and management functions in the Cloud. MVNE has further allocated slices of its leased capacity to MVNO-A.

In this scenario, the Control Plane functions have been implemented with SW in the Telco Cloud or in the Public Cloud, but they are not shown in the illustration.

The User Plane functions have been implemented on HW (S-GW-HW) in MNO-1's network and on SW (P-GW-SW) in the Cloud. MVNO-A has direct business relationships with the end-users and, thus, might have an incentive to take over the management of S/P-GWs. The Management functions may also be located in the Cloud.

Also in this scenario Interconnections take place via the SGi interface. The new implementation technologies bring new aspects to it, however. There are two new actors in the value chain: Mobile Virtual Network Enabler (MVNE) and Cloud Service Provider (CSP). A question arises on who is responsible to negotiate the interconnection agreement with MNO-2:

1) It could be the task of MNO-1, who will anyway negotiate such an agreement for its own interconnections and if the physical connection (SGi interface) is implemented via their core network (Note 1*).
2) In the first place it may not be the task of CSP, because they provide the platform for running SW, and that platform may be located where-ever, at least in theory (Note 2*).
3) It could be the task of MVNE, who would so facilitate the easy entry to the market by a new MVNO (Note 3*).
4) In the case that MVNO is already a big, well-branded actor, who is now making an entry to a new market area and may have a lot of negotiation power, they would probably take the task to negotiate the interconnection agreement themselves (Note 4*).

It is in the interest of all those actors that the interconnection agreement can be negotiated and agreed upon, however.

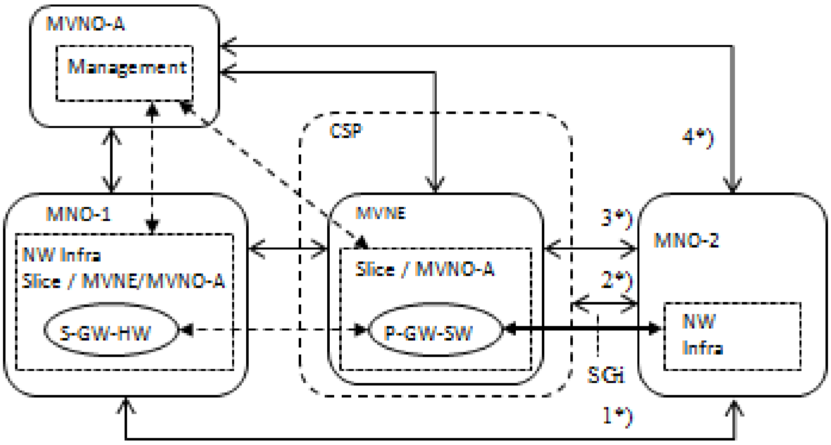

Figure 10. Typical scenario 1with new technologies – version b.

5.6.3 Typical scenario 2 with new technologies

The scenario, illustrated in Figure 11, corresponds to 'Typical scenario 2' in Section 5.5.2, where MVNO-A has made the leasing contracts with two MNOs, i.e. MNO-1 and MNO-2. The coverage of its network is the combined coverage of its contracted networks.

Irrespective of whether only one or both of the two MNOs have implemented a part their core networks functions in the Telco Cloud (owned by the MNO in question), it does not bring such new aspects to Interconnection, which a Regulator should pay attention to: the actors and interfaces are the same as they are in the old network implementation architectures. Except potentially an MVNE and a CSP, which scenario has already been discussed in the previous scenario.

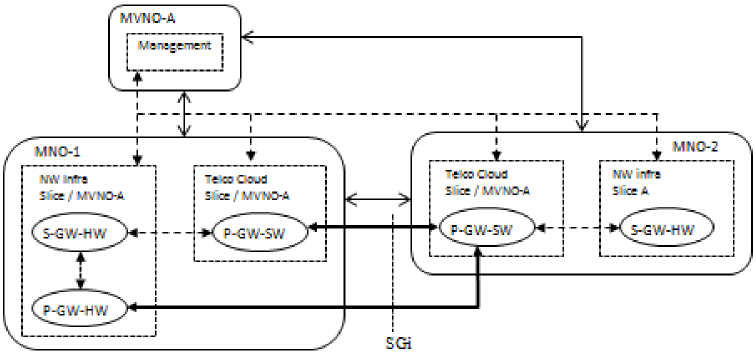

Figure 11. Typical scenario 2 with new technologies.

5.6.4 Typical scenario 3 with new technologies

This scenario, illustrated in Figure 12, corresponds to 'Typical scenario 3' in Section 5.5.3. Now MVNE-1 and MVNE-2 are providing the virtualization services to MVNO-A and MVNO-B, respectively. MVNO-A and MVNO-B have the direct business relationships with the end-users. MVNEs lease access network and core network capacity from MNOs. MVNEs have also leased capacity from CSPs for running a part of the core network functions and management functions in the Cloud. The Clouds are interconnected.

The Control Plane functions are expected to have been implemented with SW, but they are not shown in the illustration.

The User Plane functions have been implemented both with HW (S-GW-HW) in MNO-1's and MNO-2's networks, and with SW (P-GW-SW) in the Clouds.

The Management functions may also be located in the Cloud.

In this scenario, the new implementation technologies bring also new aspects to Interconnections. There are new actors in the value chain, i.e. MVNEs and CSPs, and the negotiations on the interconnection agreements may be more complicated:

1) It could be the task of MNO-1 and MNO-2, who will anyway negotiate such agreements for their own interconnections. And especially so if the physical connection (SGi interface) is implemented via their core networks (Note 1*).

2) It could be the task of MVNEs to negotiate on Interconnections, because it is their mission to facilitate the easy entries to markets by new MVNOs (Note 2*). MVNEs may have leased Interconnection capcity which they then allocate to MVNOs.

3) If an MVNO is already a big and well-known actor (e.g. MVNO-B in Figure) in one market and is now making an entry to a new market area, it may itself take care of the task to negotiate on the interconnection agreements with other actors (like with MVNE-1 in Figure) (Note 3*).

4) The big MVNOs would probably take care of the task to negotiate the interconnection agreement between themselves (Note 4*).

5) As in Scenario 1 – version b above, it may not be the responsibility of CSPs to negotiate on Interconnections, because their main task is to provide the SW platforms for the network functions. At least so in the first place. The Clouds have to be interconnected, however.

It is in the interest of all actors that the interconnection agreements can be negotiated and agreed.

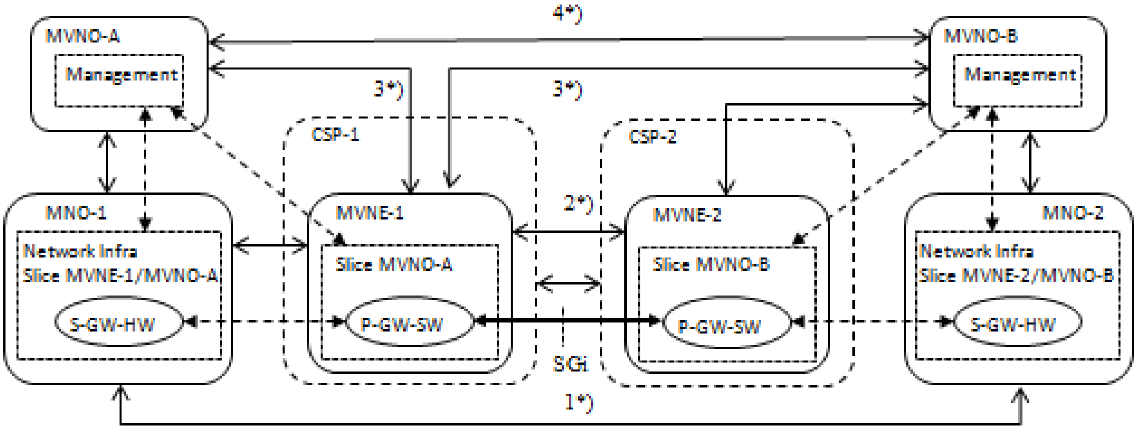

Figure 12. Typical scenario 3 with new technologies.

5.7 Summary of Interconnection issues in the context of new technologies

The interconnection scenarios discussed in the previous sections have introduced new technical interfaces, new actors for running the business (a part of a value chain) and new roles for the actors. A key prerequisite for the deployment of the new technologies, and for running the business, is that the interoperability across the technical interfaces and the fair Service Level Agreements (SLAs) between the involved parties are ensured. However, this may not happen without any guidance from the regulatory authorities. Also, running the business across countries and regions requires that the rules are harmonised between them. This, in turn, requires that the regulatory authorities in different countries and regions cooperate.

In some scenarios (‘Typical scenario 1 with new technologies -version a’, and ‘Typical scenario 2 with new technologies’), the new network technologies do not bring such new aspects to Interconnection, which the Regulator should pay attention to. This is mainly because the deployment of the new technologies does not imply the entries of new actors to the market place and the interfaces are the same as they are in the old network architectures. So, the market structures remain the same as they are currently when the existing network technologies are used (see Typical scenarios 1 and 2).

In the other scenarios (‘Typical scenario 1 with new technologies – version b’, and ‘Typical scenario 3 with new technologies’), new actors are entering to the market, and a prerequisite for that is that Interconnections and interoperability are allowed by the incumbent operators. In these scenarios, the new network technologies bring also new aspects to Interconnection. There are new actors or new roles in the value chain: Mobile Virtual Network Enabler (MVNE) and Cloud Service Provider (CSP) may implement P-GWs with software, and possibly in a Cloud. The responsibilities to negotiate on the Interconnection agreements depend on the roles that the different actors have in the value chain and on their position in the competitive environment.

Interconnection issues

The generic Interconnection issues were listed in Section 5.4. They were classified as the a) Framework and procedural issues, b) Commercial issues, and c) Technical and operational issues. The main Interconnection related issues from deploying the new network technologies and potential new business models are here summarized to be the following:

- Availability, capacity and quality of Interconnection between the system entities;
- The level and structure of Interconnection charges; basis of calculation;
- Non-discriminatory and equal access to Interconnection facilities and services;
- Interoperability and availability of open standards for interoperability across technical interfaces;
- Need for global (regional in minimum) rules for interconnecting systems across countries and regions.

5.8 Importance assessment of interconnection issues

It has been pointed out in several studies and white papers that the deployment of new network technologies being studied in the SIGMONA project would increase the cost-efficiency of the networks. This in turn would contribute to the consumer welfare with the lower end-user prices. Lack of Interconnection and interoperability between the technical entities, and across the administrative domains, would be a key obstacle to prevent the deployment of new concepts to the maximum extent.

The main Interconnection related issues from deploying the new network technologies and potential new business models were listed in the previous section. Their importance from the regulatory perspective has been assessed in this section using the regulatory goals (Section 3.1) as the main criteria for assessment. The aim of the assessment is to understand what would happen to the regulatory goals, if the Interconnection related issues of the new network technologies would not be addressed by the regulators. The results of this assessment are summarized in the following and in Table 2.

Availability, capacity and quality of Interconnection between the systems

The new network technologies will improve the service delivery in many ways. For the competition to be successful, the new Service Providers must have the capability to provide access to all services irrespective of their location. Without any obligation to provide Interconnection by the incumbent Service Providers, there would be less competition from new entrants and less investment on the new and more efficient systems. Support on the availability, capacity and quality of Interconnection between new systems would have high impact on the regulatory goals A) – E) and G), medium impact on goal I), and low impact on goals F) and H).

Level and structure of Interconnection charges, basis of calculation

Interconnection charges are payments between service providers to compensate each other for the traffic deliveries in their networks.

According to Telecommunicaion Regulation Handbook [1], there are various reasons for specifying that the interconnection charges should approximate costs. Serious problems can result from a dominant firm charging competitors such interconnection prices that are significantly above cost. It would deter the market entry and the customers of the new entrants would ultimately have to pay for these excessive charges. Also, the excessive prices can provide revenues that the dominant firm could use to subsidize losses. Such losses could be a result of predatory pricing action taken by the dominant firm to drive competitors out of a market.

Regulation on the level and structure of Interconnection charges would have high impact on the regulatory goals A) - E), medium impact on goal G) and low impact on goals F), H) and I).

Non-discriminatory and equal access to systems and services

Avoidance of discrimination is a central objective of most interconnection policies. It should be noted that the interconnection arrangements may vary from one competitor to another without being ‘unduly’ or ‘unjustly’ discriminatory. Two competitors may have voluntarily agreed to different agreements, for example, to suit their different operating conditions. A specific type of discrimination, which can be fatal to the prospects of competition, involves providing insufficient network capacity to interconnecting operators as compared to an incumbent’s own services.

Regulation on the non-discriminatory and equal access to systems and services would have high impact on the regulatory goals A) - C) and G), medium impact on goals D), E) and H), and low impact on goals F) and I).

Availability of open standards for interoperability across technical interfaces

The new networks will comprise many new actors partly being rivals in business, partly cooperating in their offer to the customer. This implies the widely accepted standards for interfaces and rules for interoperability.

In the new network technologies, the protocols have to be specified between the different system components for enabling the interoperability within an administrative domain, or between the domains. Regulation on the availability of open standards would have high impact on the regulatory goals A) – C) and G), medium impact on goals F)[5], H) and I), and low impact on goals D) – E).

Need for global rules for interconnecting systems across countries and regions

Since the administrative domains may span across country and regional borders, global approaches will be needed in the regulation. Regulators who impose uniquely local regulatory burdens, or more costly requirements than other regulators do, can handicap actors in their national markets. The world from this perspective, however, is very fragmented: we have more than 190 national regulatory agencies world-wide, and we have a number of regional organisations, which are trying to harmonise the rules on that certain regional area. This means that it will be very challenging to agree on the joint, global approaches on the regulatory issues.

With respect to the new network technologies, the global approaches would take the following regulatory goals forward: high impact on the regulatory goals A) - B), medium impact on goal D) and E) and low impact on goals F) – I).

Table 2. Importance assessment of Interconnection on regulatory goals

Issue Criteria (goals)	Availability, capacity and quality of IC	IC charges	Non-discr. and equal access	Open Standards for IC	Global rules for IC
A) Investments	high	high	high	high	high
B) Competition	high	high	high	high	high
C) Market entry	high	high	high	high	high
D) Innovation	high	high	medium	low	medium
E) Efficiency	high	high	medium	low	medium
F) Security	low	low	low	medium	low
G) Universal access	high	medium	high	high	low
H) Justice w.r.t. Scarce Resources	low	low	medium	medium	low
I) National competitiveness	medium	low	low	medium	low

5.9 Impact of new technologies on Interconnection regulation

The following conclusions can be made from the analysis reported in the previous section:

- All Interconnection issues have high impact on the regulatory goals for I*nvestments*, C*ompetition* and and *Market entry*.
- The issues related to the 'Availability, Capacity and Quality of Interconnection' and 'Interconnection charges' have high impact also on the regulatory goals for *Innovation*

[5] Different Service Providers cannot interconnect and provide integrated security services unless they use common standards.

and *Efficiency*. As the issue of ‘Availability, Capacity and Quality of Interconnection’ has high impact also on the regulatory goal for *Universal access*, the above mentioned two issues seem to be the most important issues which the Regulators need to pay attention to when the new technologies are deployed.

- According to the results from the analysis, the issue of ‘Global rules for Interconnection’ seems to have less impact on the regulatory goals than the other listed issues.
- All Interconnection issues, except ‘Open Standards for Interconnection’, seem to have low impact on the regulatory goal for *Security*. Different Service providers need open and common standards to be able interoperate in order to provide sufficient level of security for service users.

Interconnection is important both as a consumer issue and for securing fair competition. The terms for interconnection are of particular importance for small operators and new entrants, which are dependant on the access to incumbent operators’ network facilities.

The direct impact of new technologies (Clouds, NFV, SDN) on Interconnection regulation can be summarized as follows (in a random order):

- There will be needs for new types of Interconnections between the new and old types of platforms implementing the EPC functionality, and the Regulator has to ensure their availability between the different actors of the value chain.
- Interoperability between the virtualised network functions has to be ensured irrespective of who has delivered them. This may need that the interfaces between the SW components (at some level) have to be standardized.
- Interoperability has to be ensured also between the services, which may be implemented in a different way than when using old technologies. Also to be noted here is that the regulator should apply the same rules on a service irrespective of how that service has been implemented (e.g. WhatsApp and SMS/MMS).
- The new technologies create opportunities for new market entries and structures, which would create competition and innovation, and, hence, should be promoted by the Regulators.
- Whether prices of Interconnection, especially in case of new types of Interconnection, shall still be based on costs may need to be reconsidered. A reason for change might be that an incumbent operator with the old implementation technologies has much higher CAPEX and OPEX burden to carry than a new entrant may have.
- It has to be clarified whether new Interconnections will cause new imbalances in payments between the value chain actors.
- The differences in the nature of networks and new types of Interconnections recall Regulators to review the regulation principles and to evaluate how to migrate to the new market/technology environment with minimum distortions for the performance of the market, while at the same time preventing any disruptions to competition.

6. Securityand Privacy regulation

The future networks are a part of the critical information infrastructure, and it has to be ensured that they meet the requirements set for such infrastructures. It is clear that Security and Privacy will be of utmost importance for the critical infrastructures, and certainly they are among the key aspects to pay attention to when designing the new mobile network concepts and exploiting the related new technologies.

The European Commission says in its press release[6] related to the Telecoms Council, Brussels, 31 March 2009, that ‘*ICT systems, services, networks and infrastructures form a vital part of European economy and society, either by providing essential goods and services or by*

[6] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/139&format=HTML&aged=0&language=EN&guiLanguage=en/

constituting the underpinning platform of other critical infrastructures. They are often called Critical Information Infrastructures as their disruption or destruction would have a serious impact on vital societal functions'.

The above-mentioned statement is one of the reasons that Security and Privacy is a key discussion topic also in the regulation related research of the SIGMONA project.

The implications of the new cellular core network technologies on the Security and Privacy regulation will be studied following the procedure which is also illustrated in Figure 13:

1. At first, the existing regulatory environment, and regulatory goals and regimes in Security and Privacy are presented to better understand the environment, where these topics are discussed today (Sections 3, 6.1 and 6.2).
2. Then, the potential Security and Privacy issues in the context of new technologies will be identified (Sections 6.3.1 - 6.3.4).
3. Thirdly, the relevance assessment of the identified Security and Privacy issues from the perspectives of regulatory goals will be made (Sections 6.3.5 - 6.3.6).
4. Then, the analysis of the potential regulatory approaches for solving the Security and Privacy issues will be made using the regulatory goals as the criteria (Sections 6.1 and 6.4).
5. In the final step, the direct impact of the new technologies on the Security and Privacy Regulation is assessed (Section 6.5).

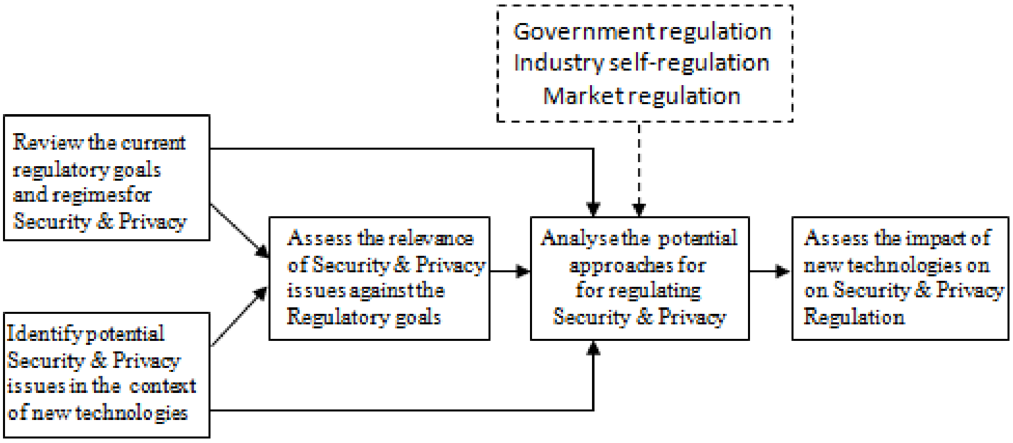
Government regulation
Industry self-regulation
Market regulation
Review the current regulatory goals and regimes for Security & Privacy
Identify potential Security & Privacy issues in the context of new technologies
Assess the relevance of Security & Privacy issues against the Regulatory goals
Analyse the potential approaches for for regulating Security & Privacy
Assess the impact of new technologies on on Security & Privacy Regulation

Figure 13. Approach to study the direct impact of new technologies on Security and Privacy Regulation.

6.1 Regulatory goals for Security and Privacy

It is clear that ensuring Security and Privacy will be one of the key objectives when designing the new information sharing concepts of the future networks. To which level the new network concepts supports Security and Privacy is an issue that can be determined by the regulators when setting the policies for operations.

To fulfil the regulatory requirements it will not be enough to tackle it only with the technical security mechanisms; there will also be a need for laws that prohibit certain actions that would be impossible to find technical solutions to enforce. In her speech in March 2014, Commissar Neelie Kroes said the following [40]: *Businesses working across the single market must sign 28 different telecoms contracts with 28 separate suppliers.The new services they use have to cope with all those different systems. No guarantee of quality, security, service. Not much good if you're considering a multi-million-euro investment in the cloud. Meanwhile networks and systems are insecure and unprotected. Deutsche Telekom reports 800,000 attacks every day – and that is just one company. Countries and companies that keep threats to themselves make the whole chain vulnerable. Companies who think this isn't happening to them are very naïve, or lying.*

In the following, the list of regulatory goals for Security and Privacy is presented. That list is based on the generic regulatory goals presented in Section 3.1 and on the regulatory objectives for Cloud Computing (presented in Annex A.3). They are seen to be common for all new technologies under the scope of the SIGMONA project. These goals are:

1) **Promote the Digital Single Market** to encourage efficient cross border services. The harmonised implementation of all relevant Directives and legislative instruments are needed in the EU and in the global context.
2) **Balance of interests** in protecting privacy and in fostering the EU-wide and global use of services. Europe to fully realise the benefits of new technologies. Note: the current laws may discourage non-European users from using EU-based cloud computing providers or making use of European data centres, for instance.
3) Security and **Privacy legislation** has to be looked at in a **global context** and its compatibility with new technologies has to be ensured; For instance, Cloud Computing has to be facilitated in Europe and at a global level. Different jurisdictions / regions shall cooperate to develop interoperable requirements that facilitated information flows with appropriate Security and Privacy protection.
4) **Foster interoperability and data portability**; Endorse technology neutrality and promote competition. Avoid mandated standards or preferences that could frustrate, rather than promote, on-going interoperability efforts of the industry at large and among the vendors providing services and solutions.
5) **The applicable law must be easy to define**. A single set of rules on data protection, valid across EU, shall be set up. A legal framework is needed that can be applied across borders, which gives users the means to exercise their rights across borders, which is based on the concept of accountability and draws on technological controls and self-regulatory codes and mechanisms as supported by Articles 17 and 27 of the Directive 95/46/EC.
6) **The right to be forgotten**, i.e., the right for the individual to request the deletion of his/her personal data.
7) **Increased responsibility and accountability** for those processing personal data.

6.2 Legal framework for Security and Privacy

In the following sub-sections the details of the legal framework for Security and Privacy, the Security and Privacy issues in the context of new network technologies, and their relevance assessment against the specific regulatory objectives are presented.

6.2.1 General legal framework for Security and Privacy

The networks today are in general more open than in the past and one weak link affects the integrity of the whole system. The growth of spam, viruses, spyware and other forms of malware, which is undermining users' confidence in electronic communications, is partly due to that openness. To ensure the security of these critical infrastructures and to protect the citizens' privacy, the European Union has taken several measures for ensuring the security of these critical infrastructures and to protect the privacy of its citizens.

In the EU's 1) Privacy Directive (EC Directive 2002/58/EC) [24] and 2) Data Protection Directive (Directive 95/46/EC) [13], Privacy in the processing of personal data and the confidentiality of communications are recognised as fundamental rights that should be protected.

1) The Privacy Directive requires the Member States to harmonise and ensure an equivalent level of protection of the right to privacy with respect to personal data in the electronic communication sector. Regarding the confidentiality of communications, the Privacy Directive says that EU member states shall ensure the confidentiality of communications and the related data traffic through the national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds

of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned.[7][8]

2) The Data Protection Directive prohibits the transfer of personal information to any country that does not have adequate privacy laws. As a result, EU member states have implemented legislation that prohibits the transfer of personal information from the EU to third countries unless such countries have adequate privacy protection in their laws [25].

On 25 January 2012, the European Commission proposed a comprehensive reform of the EU data protection rules. The draft European Data Protection Regulation is meant to supersede the EU Data Protection Directive from 1995. According to the EC, the new rules will strengthen online privacy rights and boost Europe's digital economy. The reform of the outdated privacy rules reflects that technological progress and globalization have profoundly changed the way data are collected, accessed and used [21].

The European Parliament, having already voted in favor of the General Data Protection Regulation ("GDPR") [45], voted on March 14, 2014, on the proposed Network and Information Security ("NIS") Directive [44]. In line with previous committee reports, the Parliament vote ensures that the Proposed Network and Information Security Directive focuses on protecting critical infrastructure in the energy, transport, financial services and health sectors. These sectors are seen to be very dependent on the correctly functioning network and information systems. The Commission draft also applies to "enablers of key internet services", such as providers of cloud computing services, app stores, e-commerce platforms, internet payment gateways, search engines and social networks. The EU legislative bodies will now enter into negotiations to agree a final text [43].

The policy options for ensuring NIS have been assessed in the Impact Assessment of the NIS Directive [46]. Three policy options have been named as

- Option 1 – Business as usual
- Option 2 – Regulatory approach
- Option 3 – Mixed approach

The assessment covers, in addition to the level of security, the economic and social impacts of three options.

For comparison, the United States does not provide adequate privacy protection from the European point of view [22]. To address this problem, the European Commission and the United States Department of Commerce negotiated the Safe Harbor agreement, which is only applicable to transfers between the United States and the European Union. Organizations outside the United States that have business operations within the European Union have to rely on different mechanisms to adhere to the Transborder Transfer principle from Directive 95/46/EC. This principle requires that personal identifiable information can only be transferred to those countries that are deemed to provide adequate security.

6.2.2 Legal framework for Security and Privacy in Cloud Computing

In Europe, the processing of personal data is mainly regulated by the Data Protection Directive 95/46/EC [13], which is currently under revision. The Directive imposes quite stringent duties and obligations on the actors of such processing, mainly on the '**Controller**'[9] but also on the

[7] QEG: There is still some discussion on who owns and who can access data e.g. about user's mobile phone location. E.g. can a customer request to erase all data about himself including phone tracking data, etc.

[8] QEG: It's not very clear if the future networks are ready to embrace true e2e secure communication such as provided with Telegram IM application or still would require broken model with opportunities for legal interception?

[9] *Controller* means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. *Processing of personal data* (*Processing*) means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

'**Processor**'[10]. The facts that personal data can be rapidly transferred by the Cloud Service Providers (CSPs) from one data-centre to another and that the customer usually has no control or knowledge over the exact location of the provided resources (the 'location independence' concept described in the article *Cloud Computing Legal Issues: An Overview (Part 1/2)*), stimulate customers' concerns on data protection and data security compliance [18].

Article 4 of the Data Protection Directive requires the Member States to apply the data protection rules to controllers who process personal data in the 'context of the activities' of their EEA (European Economic Area) 'establishment', or who are not 'established' in the EEA but, for purposes of processing personal data, 'makes use of' equipment (or 'means') situated in the EEA [14]. However, the **application of article 4 to Cloud Computing is complicated** by the fact that many cloud computing service providers don't own the data centres or equipment they use, and may well use the resources of other clouds. Those other Cloud Service Providers in turn may ultimately use data centres and servers rented by third parties. This means that the cloud users don't necessarily know in which data centres, or even countries, their data are stored or where their processing operations are run.

In addition, the data protection laws may differ between EU member states. There are also practical issues relating to whether the Directive can be enforced in non-EU countries. Clarification is therefore needed in the updated Directive on which country's security requirements and other rules apply to a Cloud Computing user or provider [16].

The **Governance models** and processes need also to take into account the specific issues arising from the inherently global nature of the Clouds. Data is subject to specific legislative requirements that may depend on the location where they are hosted, and for what purposes they are processed. Different countries have different laws regarding which kind of data may be hosted where and how it is to be protected. Within the Cloud, data/code may be hosted anywhere within the distributed infrastructure, i.e. potentially anywhere in the world [15].

Clarification of applicable law governing the flow, processing and protection of data are desirable, so that both Cloud customers and Cloud Service Providers have a clear understanding about which rules apply where and how. While there is no question that the Privacy Directive, like other EU Directives, applies to Cloud services, questions do arise as to how and to what extent they apply (geographic and potential subject-matter limits), as well as how they *should* apply to maximise the potential benefits of those services, while still providing the appropriate level of personal data protection [15].

6.2.3 Legal framework for Security and Privacy in Network FunctionsVirtualization (NFV)

The legal framework for Security and Privacy, as defined in Section 6.2.1, is assumed to be applied also for Network Functions Virtualization. Also, the rules and policies which are being specified for Security and Privacy in Clouds are assumed to be applied for Network Functions Virtualization because of the strong interrelation of those two technologies.

6.2.4 Legal framework for Security and Privacy in Software Defined Networking (SDN)

The legal framework for Security and Privacy in the context of Network Functions Virtualization is assumed to be relevant also in the context of Software Defined Networking, see Section 6.2.3.

6.3 Security and Privacy issues in new technologies

Secure networks are critical to all businesses, especially with their increased migration to the Clouds and Software Defined Networking (SDN). The following sub-sections deal with different Security and Privacy issues in the scope of SIGMONA project, i.e., Cloud Computing,

[10] *Processor* means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Network Functions Virtualisation (NFV), and Software Defined Networking (SDN). The key concepts of Security and Privacy are presented in Annex A.2, which are good to be kept in mind when discussing the related issues.

6.3.1 Security and Privacy issues in Cloud Computing

ITU focus group on Cloud Computing[11] has identified the Security and Privacy issues separately for the Cloud Service Users and Cloud Service Providers [17]. The following issues following have been identified for the Cloud Service Users:

- **Responsibility ambiguity**. The lack of a clear definition of responsibility among Cloud Service Users and Service Providers may evoke conceptual conflicts. Also, the problem of which entity is the data controller stays open at an international scale.
- **Loss of governance**. For an enterprise, migrating a part of its own IT system to a cloud infrastructure implies to partially give control to the Cloud Service Providers.
- **Loss of trust**. It is sometimes difficult for a Cloud Service User to recognize his Service Provider’s trust level due to the black-box feature of the cloud service. There is no measure how to get and share the Service Provider’s security level in a formalized manner. Furthermore, the cloud service users have no abilities to evaluate security implementation level achieved by the Service Provider.
- **Service Provider lock-in**. A consequence of the loss of governance could be the lack of freedom regarding how to replace a Cloud Service Provider with another.
- **Non-secure cloud service user access**. As most of the resource deliveries are through a remote connection, i.e. non-protected APIs, services are one of the easiest attack vectors. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results.
- **Lack of information/asset management**. When applying to use cloud computing services, the Cloud Service User will have serious concerns on lack of information/asset management by Cloud Service Providers, such as the location of sensitive asset/information, the lack of physical control for data storage, and the reliability of data backup.
- **Data loss and leakage**. The loss of encryption key or privileged access code will bring serious problems to the cloud service users.

With respect to the **Cloud Service Providers (CSP),** the following issues were identified by the Focus Group [17] :

- **Ambiguity in responsibility**. Different user roles, such as Cloud Service Provider, Cloud Service User, client IT admin and data owner, may be defined and used in a cloud system. Ambiguity of such user roles and the responsibilities definition related to the data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention.
- **Protection inconsistency**. Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistent among distributed security modules.
- **Bylaw conflict**. Depending on the bylaws of the hosting country, data may be protected by different applicable jurisdictions. For instance, the USA Patriot Act may authorize such seizures. The EU protects cloud service user's private data, which should not be processed in countries that do not provide a sufficient level of guaranteed protection. An international Cloud Service Provider may conflict with the bylaws of its local data centres, which is a legal threat to be taken into account.

[11] ITU-T Focus Group on Cloud Computing (FG Cloud) was established further to ITU-T TSAG agreement at its meeting in Geneva, 8-11 February 2010 followed by ITU-T study groups and membership consultation. It was successfully concluded in December 2011.

- **Business discontinuity**. The "as a service" feature of cloud computing allocates resources and delivers them as a service. The whole cloud infrastructure, together with its business workflows, thus relies on a large set of services, ranging from hardware to application. However, the discontinuity of service delivery, such as a black-out or delay, may have a severe impact on the availability.
- **Shared environment**. Cloud resources are virtualized and different Cloud Service Users (possibly competitors) share the same infrastructure. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.
- **Hypervisor isolation failure**. The hypervisor technology is considered as the basis of cloud infrastructure. Multiple virtual machines co-hosted on one physical server share both CPU and memory resources which are virtualized by the hypervisor. This threat covers the failure of mechanisms to isolate attacks that could be launched on a hypervisor to gain illegal access to the memory of other virtual machines.
- **Service unavailability**. Availability is not specific to the cloud environment. However, because of the service-oriented design principle, service delivery may be impacted while the cloud infrastructure in not available. Moreover, the dynamic dependency of cloud computing offers many more possibilities to an attacker. A typical denial of service attack on one service may blog the whole cloud system.
- **Abuse by Cloud Service Provider**. For a Cloud Service User, migrating a part of its own IT to a cloud infrastructure, implies to partially give control to the Cloud Service Provider. This may lead to a mis-configuration or malicious insider attack.

The Security and Privacy issues reported on NIST guidelines on Security and Privacy in Public Cloud Computing [41] are very much the same or similar to those listed above. The following first two issue descriptions can be seen to further explain the issues above. The third issue (Visibility) is complementary to the issues above.

- **Loss of control** (see Loss of governance above). Transitioning to Clouds architecture requires a transfer of responsibility and control to the Cloud Service Provider over information as well as system components that were previously under the organization's direct control. The transition is usually accompanied by the lack of a direct point of contact with the management of operations and influence over decisions made about the computing environment. This situation makes the organization dependent on the cooperation of the Cloud Service Provider to carry out activities that span the responsibilities of both parties, such as continuous monitoring and incident response.
- **Data Ownership** (see Ambiguity responsiblity above). The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for the trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved. Ideally, the contract should clearly state that the organization retains exclusive ownership over all its data; that the Cloud Service Provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the Cloud Service Provider does not acquire and may not claim any interest in the data due to security.
- **Visibility.** Knowledge of a Cloud Service Provider's security measures is also needed for an organization to conduct its risk management. For example, the process of identifying vulnerabilities should include an analysis of the system security features and the security controls used to protect the cloud environment. The Cloud Service Providers can be reluctant to provide details of their security and privacy measures and status, however, since such information is often considered proprietary and might otherwise be used to devise an avenue of attack.

  Transparency in the way a Cloud Service Provider operates is a vital ingredient for effective oversight over system security and privacy by an organization. To ensure that policy and procedures are being enforced throughout the system lifecycle, the service arrangements should include some means for the organization to gain visibility into the security controls and processes employed by the cloud provider and their performance over time. For example, the service agreement could include the right to audit controls via a third party.

6.3.2 Security and Privacy issues in Network Functions Virtualization

The concepts of the Network Virtualization and the Network Functions Virtualisation (NFV) are different. **Network Virtualisation, or a virtualized network,** uses a single physical infrastructure to support multiple logical networks. Each logical network provides its users with a customized set of protocols and functionalities. An important aspect of Network Virtualization is that the participating entities are independent and driven by different objectives, see Appendix A.1. Thus, it cannot be assumed that they always cooperate to ensure that all aspects of the virtual network operate correctly and securely. Instead, each entity may behave in a non-cooperative or malicious way to gain benefits [28]. Security issues in virtualized network architectures impose significant challenges and require effective solutions. The problem of hosting network protocols and services on third party infrastructures raises serious questions on the trustworthiness of the participating entities.

Physical network functions assume a tight coupling of the Network Functions software and hardware which, in most cases, is provided by a single vendor. In the **Network Functions Virtualisation (NFV)** scenario, multiple vendors are expected to be involved in the delivery and setup of different virtualised elements (e.g., hardware resources, virtualisation layer, virtualized network functions (VNF), virtualised infrastructure manager, etc.). As a result, due to the virtualisation process, new security issues need to be addressed [26][27]. Examples are:

- The use of hypervisors may introduce additional security vulnerabilities. In general, to reduce the vulnerabilities of hypervisors in use, it is essential to follow the best practices on hardening and patch management.
- The usage of shared storage and shared networking may also add additional dimensions of vulnerability.
- The interconnectivity among the virtualised end-to-end architectural components exposes new interfaces that, unless protected, can create new security threats.
- The execution of diverse VNFs over the NFV infrastructure can also create additional security issues, if VNFs are not properly isolated from others.
- Hardware, hypervisors, VNFs and cloud resource control solutions may be provided by different vendors, increasing the risk of security holes due to mismatched assumptions and expectations.

According to ETSI NFV ISG report on virtualization requirements [33], the NFV framework shall implement appropriate security countermeasures to address:

- Security vulnerabilities introduced by the virtualization layer.
- Protection of data stored on the shared storage resources or transmitted via shared network resources.
- Protection of new interfaces exposed by the interconnectivity among virtualised end-to-end architectural components, e.g., hardware resources, VNFs and management systems.
- Isolation of distinct VNF sets executing over the NFV infrastructure to ensure Security and separation between these VNF sets.
- Secure management of VNF sets by other third-party entities (e.g., VNPaaS, enterprise virtual CPE, and virtual consumer home gateways).

The NFV Infrastructure shall be able to use standard security mechanisms wherever applicable to authentication, authorization, encryption and validation [33].

6.3.3 Security and Privacy issues in Software Defined Networking (SDN)

Software Defined Networking (SDN) provides a centralized intelligence and control model that can offer much-needed flexibility for network security deployments. Along with many benefits, SDN also poses new threats, particularly with the emergence of cloud and virtualized environments [34]. The central control of the SDN architecture could give an attacker the command over the entire network [30].

OpenFlow-enabled SDN offers a wide range of **benefits for security implementation** and management [34], including:

- Fine-grained enforcement and control of multiple simultaneous security policies throughout the data center.
- Validation of security policies, and quick identification and resolution of any policy conflicts that may arise.
- Incorporation of a trust model with live rule-conflict detection and resolution at the controller layer.
- Synchronization of distributed policy insertion and removal.
- Dynamic assertion of extensions to the security policy when new threats are detected.
- Provision of a mechanism for auditing and audit trails, etc.

The separation of the control and data planes and aggregating the control functionality to a centralized system opens up also **new challenges**. The control plane can become a single point of failure and render the whole network down in case of compromise. The malfunctioning or malicious software can compromise the whole network having access granted to the control plane [32].

Basically, the security issues in SDN are concentrated around the main areas of i) application plane, ii) control plane, iii) data plane, and iv) communication security. SDN enables applications to interact with and manipulate the behavior of network elements through the control layer. SDN has two properties which can be seen as attractive to malicious users. These properties are 1) the ability to control the network by software, and 2) centralization of network intelligence in network controllers. Since there are no standards or open specifications to facilitate open APIs for applications to control the network services and functions through the control plane, applications can pose serious security threats to the network resources, services and functions [32].

The Open Networking Foundation (ONF) organisation has launched a study to determine how to make SDN more secure. The ONF is considering, for example, the idea of using distributed protocols, which are more resilient and harder to attack simply because they are not concentrated [29].

Security needs to be everywhere within SDN. It needs to be built into the architecture, as well as delivered as a service to protect the availability, integrity and privacy of all connected resources and information [31].

6.3.4 Summary of Security and Privacy issues in the context of technologies under study (Clouds, NFV, SDN)

From the previous sections one can conclude that the new mobile network concepts will open up numerous new Security and Privacy challenges or issues. May of them originate from those identified in the context of the Clouds concept. They are, however, relevant also to other concepts as the implementations of those concepts are very much exploiting the clouds technologies.

Security and Privacy issues which are assumed to be the most relevant in the context of new technologies and regulation have been listed below. Their importance against the regulatory goals is further assessed in Section 6.3.5. The focus is on the issues which can be resolved by the mutual agreements by the involved parties, or by the intervention of the Regulatory Authority. Such issues which are purely technical have been left out of the discussion.

A. **Responsibility ambiguity.** Different user roles, such as Cloud Service Provider, Cloud Service User, client IT administrator and data owner, may be defined. Ambiguity of such roles and responsibilities may induce business or legal dissension.

   Very much similar to Responsibility ambiguity is **Data ownership.** The organization’s ownership rights over the data must be firmly established in the service contract to enable a basis for the trust and privacy of data. The Cloud Service Provider shall not be able to acquire and may not claim any interest in the data due to security.

B. **Bylaw conflict / Location of legal disputes.** Depending on the bylaw of the hosting country, data may be protected by different applicable jurisdiction. There are, at least, three possible locations to choose from: that of the victim, that of the offender, or that of the Service Provider. The specific issues here are: Location of sensitive asset/information, lack of physical control for data storage, and reliability of data backup.

C. **Shared environment.** The resources are virtualized and different Cloud Service Users (including MVNOs) - possibly competitors - share the same infrastructure. Any unauthorized and violent access to sensitive data may compromise both the integrity and confidentiality.

D. **Different objectives for Trust.** The participating entities – network infrastructure providers, MVNOs, MVNEs and CSPs - are independent and driven by different objectives. They may not cooperate to ensure that all aspects of the network operate correctly and securely.

E. **Interconnectivity.** The interconnectivity among new architectural components exposes new interfaces that, unless protected, can create new security threats. In the technology development phase, the standardisation of protocols and network equipments should be considered.

F. **Single point of failure.** The control plane in SDN can become a single point of failure and render the whole network down in case of compromise. The issue becomes even more complicated when the Controller is located in a CSP-operated Cloud.

G. **Loss of governance.** An enterprise, which migrates a part of its own IT system to a cloud infrastructure, has to partially give control to the Cloud Service Providers. This transition is accompanied by the lack of direct point of contact with respect to the management operations. The situation makes an organization dependent on the cooperation of the Cloud Service Provider to carry out activities that span the responsibilities of both parties.

   Similar to Loss of governance is **Loss of control.** Transitioning to Clouds architecture requires a transfer of responsibility and control to the Cloud Service Provider over information as well as system components that were previously under the organization's direct control. This situation makes the organization dependent on the cooperation of the Cloud Service Provider.

H. **Service Provider lock-in.** A consequence of the loss of governance could be the lack of freedom regarding how to replace a Cloud Service Provider by another.

I. **Visibility.** Knowledge of a Cloud Service Provider's security measures is also needed for an organization to conduct its risk management. The Cloud Service Providers can be reluctant to provide details of their security and privacy measures and status. Transparency in the way a Cloud Service Provider operates is a vital ingredient for effective oversight over system security and privacy by an organization.

J. **Protection inconsistency**. Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistent among distributed security modules.

6.3.5 Relevance assessment of Security and Privacy issues for regulation

Developing new technologies raises new issues and some of these issues require regulation as a solution. The new network technologies being studied in SIGMONA (Clouds, NFV, SDN) are not different in this aspect. In this section the relevance of the issues described and summarized in Section 6.3.4 has been assessed against the regulatory goals for Security and Privacy. Those goals, 1) – 7), have been summarized Section 6.1, and they are considered to be relevant for the technologies under the scope of the SIGMONA project.

The relevance of each issue is summarised in Table 3 with the scale *high (red)*, *medium (yellow)* or *low (green)*, where *high* means the issue will have a high impact on the given criterion and *low* means little impact. In case where the authors of this document disagreed on the level of relevance of an issue, a classification *unclear* was made (no colour). The arguments for each assessment are given in Annex A.5.

Note: The Table below includes separate columns for each technology (Clouds, NFV, SDN). In this assessment those technologies are considered as independent technologies, I.e, not as implemented using the Clouds technology.

Table 3. Relevance of issues for regulatory objectives.

Concern / Issue	**Relevance / Impact of an Issue on reaching the regulatory targets**		
	Clouds	**NFV**	**SDN**
Responsibility ambiguity / Data ownership	*high* 1), 3), 5), 6), 7)	*unclear*	*medium* 1), 4), 5) 7)
Bylaw conflict / Location of legal disputes	*high* 1), 2), 3), 5), 6)	*high* 1), 2), 3), 5), 7)	*low* 2), 3)
Shared environment	*high* 2), 3), 5), 7)	*high* 2), 3), 7)	*medium* 4), 7)
Different objectives for Trust	*high* 1), 3), 5), 6)	*low* 5)	*low* 5)
Interconnectivity	*high* 1), 2), 4), 5)	*high* 1), 2), 3), 4), 5)	unclear
Single Point of Failure	*low*	*low*	*low*
Loss of governance / Loss of control	*high* 4), 5), 6), 7)	*high* 4), 5), 7)	*low*
Service Provider Lock-in	*medium to high* 1), 4)	*low* 4)	*low* 4) -
Visibility	*high* 1), 7)	*unclear*	*low*
Protection Inconsistency	*medium* 1), 3), 4)	*low*	*low*

6.3.6 Summary of assessment

In the previous section, the relevance of issues of each technology on the regulatory goals was assessed. The assessments were given by different consortium partners [61] and were made separately for each technology, as if they were independent of each other. In this section, the relevance of issues is summarized across all technologies in question, assuming that also the NFV and SDN will be implemented in the clouds environment. Because three assessments did not always result in the same conclusion (*high* / *medium* / *low*), this summary is a kind of compromise of all of them.

The different regulatory targets are influenced by the regulatory issues of *high* relevance as summarized in Table 4 below.

Table 4. Summary of issues with high relevance for each regulatory goal.

Regulatory target	**Issues of high relevance and impact**
1 Promote Digital Single Market	Responsibility ambiguity/Data ownership, By law conflict/Location of legal disputes, Different objectives for Trust, Interconnectivity, Loss of governance/Loss of control, Service Provider lock-in, Visibility
2 Balance of interest	By law conflict/Location of legal disputes, Shared environment, Interconnectivity
3 Global context	Responsibility ambiguity/Data ownership, By law conflict/Location of legal disputes, Shared environment, Different objectives for Trust, Interconnectivity, Visibility
4 Foster interoperability and data portability	Interconnectivity, Loss of governance/Loss of control, Service Provider lock-in
5 Applicable law must be easy to define	Responsibility ambiguity/Data ownership, By law conflict/Location of legal disputes, Shared environment, Different objectives for Trust, Interconnectivity, Loss of governance/Loss of control
6 Right to be forgotten	Responsibility ambiguity /Data ownership, By law conflict/Location of legal disputes, Different objectives for Trust, Loss of governance/Loss of control
7 Increased responsibility and accountabiity	Responsibility ambiguity /Data ownership, By law conflict/Location of legal disputes, Shared environment, Loss of governance/Loss of control, Visibility

6.4 Analysis of potential regulatory approaches for Security and Privacy

There are at least three different levels where Security and Privacy could be regulated, each with benefits and drawbacks [35]. They are:

- **Government regulation**
- **Industry self-regulation**
- **Consumer or market regulation**

The most obvious place to regulate Security and Privacy is at the governmental level. The governments are responsible for writing laws and regulations, and people look to their governments to lay down such rules that prevent harms to the public.

Another level where to regulate privacy is the industry level. Industries can develop principles and practices that reflect consensus on the best approach to privacy. In ‘Industry self-regulation’, a network of leading companies may require their business partners to meet industry standards on privacy.

Finally, there is consumer or market regulation. Consumers are in the best position to know their desires with respect to privacy, and they are in the best position to enforce the terms of their desires through their choices in the marketplace.

The different approaches have been analysed from the regulatory goals’ perspective in Table 5. The goals were introduced in Section 6.1. The most relevant Security and Privacy issues to keep in mind in this analysis have been elaborated in Section 6.3.4. The statement ‘Yes’ in the table means that there is positive impact on the regulatory goal in question, and the statement ‘No’ means that there is no impact. The color codes ‘green’, ‘yellow’ and ‘red’ mean a kind of average of different statements: green (‘Yes’), red (‘No’) and yellow (‘Yes’ and ‘No’).

Table 5. Assessment of regulatory approaches for Security and Privacy.

Criteria (Regulatory targets)	Government regulation	Industry self-regulation	Consumer or market regulation
1 Promote the Digital Single Market	Yes. The responsibilities have to be defined in the same way across country borders. Yes. Agreements between governments are needed to push the European-wide standards and practices. This is especially important for enabling new entries in the market. Yes. Citizens expect that governments lay down rules that prevent harms to the public.	Yes. The traditional telecom payers can reach consensus e.g. on the standards for interoperability. Standardisation work is already ongoing. No. New actors are emerging in the telecoms business. They do not have such experience / tradition on co-operation as the traditional telecom vendors do have. No. Industrial actors cannot agree e.g. on the single set of rules for managing security and privacy across different regions. The different actors may be driven by different objectives. No. A Service Provider dominating in the market would like to apply its own standards for interconnection and portability, for instance.	No. Different standards and rules for managing security and privacy may exist depending on the Service Provider.
2 Balance of interests	Yes. Balancing the interests in protecting security and privacy, on one hand, and fostering EU-wide of services on the other hand, can be agreed at least on the EU level. No. Balancing the interests across regions (Europe, America, Asia) is almost impossible. No. To control many types and uses of information in balance with encouraging the commercial exploitation of new systems and business models will be challenging.	Yes/No. Industrial actors try to realise the benefits of the new technologies. However, operating e.g. in the shared environment needs more trust between parties. And that may depend on the service in question. Yes. Consumers seem not to care so much about Privacy, in practice. No. There will be variations of balance in different regions and countries. No. Commercial interests may lead to breaches in using information and, thus, breaking the balance.	Yes. Consumers and corporate users can choose whether to deal with businesses who promise them a given level of security and privacy. Service Providers who offer security and privacy that pleases consumers and corporate users succeed. No. Where some consumers may have very strict senses of privacy, others have fewer reservations about revealing personal information and receiving benefits of participation on commercial life. Yes. Most consumers seem not to care so

			much about Privacy, in practice.
3 Global context	Yes. Security and privacy legislation and its compatibility with new technologies can be agreed at the European level. No. The compatibility of the security and privacy legislation with the new technologies is difficult to reach across regions. No. The different levels of privacy are difficult to regulate. Consumers may have • strict senses of privacy, or • less reservations about revealing personal information	No. Local actors may have very different views and interests abut Security and Privacy. Yes. Big international actors will have interests to agree on rules which are applied globally.	No. Market regulation is not allowed in some regions.
4 Foster Interoperability and data portability	Yes. Agreements between governments are needed to push the European-wide standards and practices. This is especially important for enabling new entries in the market.	No. A dominant actor may want to push their own closed standards on Interoperability (Note 1) Yes. The telecom actors have a tradition to agree on the Interoperability.	No. Consumers or coprporate users have no power to push Interoperability and data portability.
5 Applicable law must be easy to define	Yes. The governments (EU Commission) can agree on the applicable law in Europe. Yes. Responsibility and accountability of those storing and processing data can be defined. No. The agreement on the applicable law across regions would be difficult to reach (see Global context)	No. The Industrial actors have no mandate to agree on the applicable law. No. Depending on the bylaw of the hosting country, data may be protected by different applicable jurisdiction. This may lead to reduced use of new services.	No. Consumers have no mandate to agree on the applicable law.
6 Right to be forgotten	Yes. The governments can enforce the rule for ‘Right to be forgotten’.	Yes. The consensus on the right to be forgotten can be reached between the companies of good reputation. No. Rogue companies, that do not want to follow industry standards, may take the opportunity to charge.	No. Consumers cannot enforce to be forgotten by the Cloud Service Provider.
7 Increased responsibility and accountability	Yes. Governments define and enforce the responsibility and accountability for Service Providers.	No. Definition of responsibility and accountability across regions and countries is challenging for different kinds of industrial	No. Consumers have no power to define nor to enforce responsibility and accountability within and across regions and

	This may be challenging in case of Cloud Computing, however, because the data may be located anywhere.	actors. Lack of clear definition of responsibility among Service Providers and users may evoke conflicts.	countries.

Note 1): This may be true only for OTTs. This may not be a real problem for electronic communication service providers in the EU.

Table 5 above summarizes how the different regulatory approaches would contribute to the different regulatory targets. The 'Government regulation' would promote many of those targets and the 'Industry self-regulation' also many of them, at least slightly. Clearly, the 'Consumer or market regulation' would have most difficulties to promote any of the targets; in this approach the Service Providers, which offer such level of Security and Privacy that pleases consumers and corporate users, would succeed, but most of the issues would remain unresolved.

6.5 Summary of issues and impact of new technologies on Security and Privacy regulation

Several Security and Privacy issues related to the new network technologies were identified in this study both on the Service Provider side and on the customer side. These issues may be quite complicated arising from the inherently global nature of the Clouds, especially. The wide scale deployment of Cloud Computing, Network Function Virtualisation and Software Defined Networking can trigger a number of security and data protection risks stemming mainly from the new interfaces, shared environments, new actors with different views and objectives on Security and Privacy, and from the more complicated value networks.

Data is subject to specific legislative requirements that may depend on the location where they are hosted, and for what purposes they are processed. Different countries have different laws regarding which kind of data may be hosted where, and how it is to be protected. Clarification of applicable law governing the flow, processing and protection of data is desirable, so that both the Service Providers and customers (private and corporate) have clear understanding about which rules apply where and how [50].

On March 14, 2014, the European Parliament voted on the proposed Network and Information Security ("NIS") Directive [44]. The policy options for ensuring NIS have been assessed in the Impact Assessment of the NIS Directive, see Section 6.2.1. Three policy options identified there are 1) 'Business as usual', 2) 'Regulatory approach', and 3) 'Mixed approach'. In that assessment Option 1 and 3 are not considered viable for reaching the policy objectives, and are therefore not recommended. The reasons not to recommend are that their effectiveness would depend on whether the voluntary approach would actually deliver a minimum level of NIS. Regarding Option 3, it would depend on the good will of the Member States to set up capabilities and co-operate crossborder.

Option 2 is the preferred one given that under this Option the protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably. The analysis made in the SIGMONA project (previous section) supports the Impact Assessment of the NIS Directive: **Government regulation would best promote the targets for Security and Privacy.**

According to this study in the SIGMONA project, **the technology (Clouds, NFV, SDN) implications on Security and Privacy regulation** can be summarized as follows (in a random order):

- New technologies will allow new types of market structures with new types of actors in the telecommunications value chain. Different actors have different views, practices and objectives for securing Security and Privacy. The responsibilities and accountabilities for securing end-to-end Security and Privacy, and the ownership rights over the data have to be clearly and firmly defined across country borders.

- Due to the de-centralized architecture of the Clouds based implementations the protection mechanisms are likely to be inconsistent. Regulators have to push for the consistent systems with respect to Security and Privacy.
- Due to the de-centralized nature of architecture (Clouds, Virtualisation) the user related data may be located where-ever. In this new and more complicated environment the governments have to enforce also the rule for ‘right to be forgotten’.
- A loss of governance may lead to a Service Provider lock-in (one kind of loss of Security). Regulators need to take actions to foster interoperability and data portability, which boosts competition.
- Balancing on interests in protecting Security and Privacy, on one hand, and fostering EU-wide (and global) services, on the other hand, shall be agreed at least on the EU level. Different levels of Privacy may be difficult to regulate, however.
- The new Security and Privacy issues in the context of new technologies are more of global nature than ever before, and EU-wide (or rather global) approaches are needed in Regulation. EU-wide standards and practices are needed. This is also important for enabling new entries to the market. The location of legal disputes has to be clear and agreed.

7. Conclusions

The regulatory process is time consuming to administer and requires considerable expenditure of resources. Accordingly, Regulation should only focus on those parts of the ICT sector where there is a clear need for regulation and should aim to establish or restore the conditions that provide for effective competition on a sustained basis.

Regulation is affected by the technological development in different ways, and the same technology may affect the market structure and regulatory needs in several ways simultaneously. In the SIGMONA project we have at first identified the potential regulatory issues, which may emerge when deploying new network technologies, and analyzed their **direct impact** on Regulation. The focus areas in this work were **Interconnections** and **Security and Privacy**.

The **interconnection** scenarios discussed in this study have introduced new technical interfaces, new actors for running the business (a part of a value chain) and new roles for actors. It is clear that a key prerequisite for the deployment of the new technologies, and for running the business and boosting the competition, is that the interoperability across the technical interfaces and the fair Service Level Agreements (SLAs) between the involved parties have to be ensured. This may not happen, however, without any guidance from the regulatory authorities. Also, running business across countries and regions requires that the rules are harmonised between them. This, in turn, requires that the regulatory authorities in different countries and regions cooperate.

All identified interconnection issues seem have **high impact** on the regulatory goals for I*nvestments*, C*ompetition* and *Market entry*. The issues related to the 'Availability, Capacity and Quality of Interconnection' and 'Interconnection charges' seem to be the most important issues which the regulators need to pay attention to when the new technologies are deployed. The terms for Interconnection are of particular importance for small operators and new entrants, which are dependent on the access to incumbent operators' network facilities.

Several **Security and Privacy** issues related to the new network technologies were identified in this study both on the Service Provider side and on the customer side. These issues may be quite complicated arising from the inherently global nature of the Clouds, especially. The wide scale deployment of Cloud Computing, Network Function Virtualisation and Software Defined Networking can trigger a number of security and data protection risks stemming mainly from the new interfaces, shared environments, new actors with different views and objectives on Security and Privacy, and from the more complicated value networks.

Data is subject to specific legislative requirements that may depend on the location where they are hosted, and for what purposes they are processed. Different countries have different laws regarding which kind of data may be hosted where, and how it is to be protected. Clarification of applicable law governing the flow, processing and protection of data is desirable, so that both the Service Providers and customers (private and corporate) have clear understanding about which rules apply where and how.

In the proposed Network and Information Security ("NIS") Directive of the EU, three policy options for ensuring NIS have been assessed. Option 'Regulatory approach' is concluded to be the preferred one given that under this Option the protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably. The analysis made in this SIGMONA study supports the assessment of the NIS Directive: **Government regulation would best promote the targets for Security and Privacy.**

8. References

[1] Telecommunications Regulation Handbook, Hank Intven, McCarthy Tétrault [infoDev, ISBN 0-9697178-7-3], 2000.

[2] ICT Regulation Toolkit, http://www.ictregulationtoolkit.org/en/Sections.html

[3] A paper prepared for the 1998 EU Competition Workshop at the Robert Schuman Centre of the European University Institute, Henry Ergas, November 1998, http://www.greenwhiskers.com.au/papers_reports/papers-ergas-tslric-final-nov98.pdf.

[4] Application of Forward-looking Cost Models to Interconnection Pricing and Universal Service, William W Sharkey, http://www.iirsa.org/BancoMedios/Documentos%20PDF/oe_semtics03presentacionwilliamsharkey.pdf

[5] MVNO Pricing Structures in Finland, Ministry of Transport and Communications, Finland. http://www.lvm.fi/fileserver/mvno%20pricing%20structures%20in%20finland.pdf

[6] http://en.wikipedia.org/wiki/Mobile_virtual_network_operator

[7] Mobile Virtual Network Operator (MVNO) basics: What is behind this mobile business trend. http://www.valoris.com/docs/MVNO_basics.pdf

[8] Techno-economic analysis of mobile Virtual Network operators: Strategies, investments, and revenues, Timo Smura, Annukka Kiiski & Heikki Hämmäinen, Helsinki University of Technology, Networking Laboratory

[9] T. Casey, T. Smura and A. Sorri, “Value network configurations in wireless local area access,”Proceedings of 9th Conference on Telecommunications Internet and Media Techno Economics (CTTE), 2010

[10] “Designing Next Generation Telecom Regulation: ICT convergence or Multisector Utility ? Report on the WDR Dialogue Theme 2002” Anders Henten, Rohan Samarajiva, William H. Melody, January 2003

[11] CITEL Guidelines and Practices for Interconnection Regulation, draft June 1999, Inter-American Telecommunications Commission, http://www.citel.oas.org/ccp1-tel/guidelines/guidelines%20on%20Interconnection.pdf

[12] FP7-ICT-2007-1-216041-4WARD deliverable D1.2 Project-wide Evaluation of Business Use Cases, http://www.4ward-project.eu/index.php?s=file_download&id=76

[13] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[14] Computer World UK, Blog: Cloud computing and EU data protection law, 28 September 2011, http://blogs.computerworlduk.com/cloud-vision/2011/09/cloud-computing-and-eu-data-protection-law/index.htm

[15] Industry Recommendations to Vice President Neelie Kroes on the Orientation of a European Cloud Computing Strategy, November 2011, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/industryrecommendations-ccstrategy-nov2011.pdf

[16] University of London, Centre for Commercial Law Studies, News: Data protection law creates cloud of uncertainty for cloud computing, 21 November 2011, Cloud of Unknowing papers, http://www.ccls.qmul.ac.uk/news/2011/59982.html

[17] ITU Focus Group on Cloud Computing. FG Cloud Technical Report, Part 5. http://www.itu.int/en/ITU-T/focusgroups/cloud/Pages/default.aspx

[18] Cloud Computing Legal Issues: When does Directive 95/46/EC Apply? http://common-assurance.com/blog/files/2cf981cc32595f347ba14371ea17643f-11.html

[19] Industry joint paper on the review of the EU Legal Framework for data protection. http://www.orange.com/en_EN/group/european_policy/privacy/att00022388/1010_Industry_Joint_Paper_on_Data_Protection.pdf

[20] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing (Adopted July 1st 2012)

[21] Eurescom mess@ge, The magazine for telecom insiders, 1/2012

[22] Joep Ruiter, Martijn Warnier: Privacy Regulations for Cloud Computing Compliance and Implementation in Theory and Practice. http://www.iids.org/aigaion/indexempty.php?page=actionattachment&action=open&pub_id=316&location=spcc10.pdf-9869f6a896824ba29d27ad19e6da5585.pdf

[23] EU, L 201/37: DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002. *Official Journal of the European Communities*. [online][Accessed on 12 Dec 2011] at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[25] Security in Telecommunications and Information Technology, 2003, ITU-T, http://www.itu.int/itudoc/itu-t/85097.pdf

[26] NFV 0010, Network Functions Virtualisation; Architectural Framework

[27] Alcatel-Lucent: NETWORK FUNCTIONS VIRTUALIZATION ! CHALLENGES AND SOLUTIONS. STRATEGIC WHITE PAPER http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2013/9377-network-functions-virtualization-challenges-solutions.pdf

[28] Security Issues in Network Virtualization for the Future Internet, Sriram Natarajan and Tilman Wolf Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA, USA. http://www.ecs.umass.edu/ece/wolf/pubs/icnc2012.pdf

[29] SDN security challenges alongside the potential of a new technology. http://searchsdn.techtarget.com/tip/SDN-security-challenges-alongside-the-potential-of-a-new-technology

[30] McAfee Blog Central, Software Defined Networking Promises Greater Control While Increasing Security Risks. http://blogs.mcafee.com/mcafee-labs/2014-threats-predictions-software-defined-networking-promises-greater-control-while-increasing-security-risks

[31] SDN Central. Security Challenges in SDN (Software-defined Networks). http://www.sdncentral.com/security-challenges-sdn-software-defined-networks/

[32] SIGMONA Internal Report IR4.1, State-of-the-Art in Mobile Transport Networks

[33] NFV 0012, Network Functions Virtualization; Virtualization Requirements

[34] Open Network Foundation (ONF), SDN Security Considerations in the Data Center

[35] Privacilla.org. http://www.privacilla.org/business/howtoregulate.html

[36] ITU-T Recommendation X.805 “Security architecture for systems providing end-to-end communications, http://www.itu.int/rec/T-REC-X.805-200310-I/en.

[37] Hyland, N., 2011. Loss of Personal Data is Sufficient to Advance Privacy Lawsuit. [online] [Accessed on 9 May 2011] at http://www.cyberlawcurrents.com/?p=1394.

[38] Wong, N., 2006. Response to the DoJ motion, The Official Google Blog. [online] [Accessed on 9 May 2011] at http://googleblog.blogspot.com/2006/02/response-to-doj-motion.html.

[39] Gilbert Tobin Lawyers, Economic study on IP interworking, February 2007, http://www.gsmworld.com/documents/IP_Interconnection_Economic_Study_on_IP_Networking.pdf

[40] Commissioner Kroes speech on the Digital Economy and exchange of views on Internet Governance in Parliament: Why the digital economy matters. Düsseldorf 26 March 2014

[41] NIST, Draft Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing. https://cloudsecurityalliance.org/wp-content/uploads/2011/07/NIST-Draft-SP-800-144_cloud-computing.pdf

[42] InsidePrivacy. http://www.insideprivacy.com/international/european-parliament-votes-to-ensure-that-the-proposed-network-and-information-security-directive-foc/

[43] Press Release: The EP successfully votes through the Network & Information Security (NIS) directive. http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm

[44] Commission Proposal for a Directive on Network and Information Security COM(2013) 48 final. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666

[45] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

[46] SWD(2013) 31. EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT *Accompanying the document* Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_res_en.pdf

[47] Reforming Europe's Telecoms Regulation to Enable the Digital Single Market (ETNO Report). https://www.etno.eu/datas/publications/studies/BCG_ETNO_REPORT_2013.pdf

[48] SIGMONA Internal Report IR1.1c, Software Defined Mobile Networks state-of-the-art

[49] Joep Ruiter, Martijn Warnier: Privacy Regulations for Cloud Computing Compliance and Implementation in Theory and Practice. http://www.iids.org/aigaion/indexempty.php?page=actionattachment&action=open&pub_id=316&location=spcc10.pdf-9869f6a896824ba29d27ad19e6da5585.pdf

[50] FP7-ICT-2009-5-257448-SAIL, *Deliverable D-2.8 – Evaluation of Business Models*, 2012

[51] EC Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, 7 March 2002, http://ec.europa.eu/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00070020.pdf

[52] ITU Focus Group on Cloud Computing. FG Cloud Technical Report, Part 4. http://www.itu.int/en/ITU-T/focusgroups/cloud/Pages/default.aspx

[53] Economic Rationale for Interconnection and Different Mobile Interconnection Regimes, ACTECON Competition and Regulation Consultancy, August 1, 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2176058

[54] Leimeister, Stefanie, Riedl, Christoph, Böhm, Markus, Krcmar, Helmut: THE BUSINESS PERSPECTIVE OF CLOUD COMPUTING:ACTORS, ROLES, AND VALUE NETWORKS. http://home.in.tum.de/~riedlc/res/LeimeisterEtAl2010-preprint.pdf

[55] Antti Tolonen: Dynamic Virtualized Network Functions on an OpenStack Cloud. AALTO University Master’s Thesis 2014

[56] Johanna Heinonen, Tapio Partti, Marko Kallio, Kari Lappalainen, Hannu Flinck, Jarmo Hillo: Dynamic Tunnel Switching for SDN-Based Cellular Core Networks. 4th Workshop on All Things Cellular: Operations, Applications and Challenges 2014, Chicago, USA (co-located with ACM SIGCOMM 2014)

[57] ETSI Leaflet: Network Functions Virtualisation http://www.etsi.org/images/files/ETSITechnologyLeaflets/NetworkFunctionsVirtualization.pdf

[58] Uwe Janssen, DTAG: The Impact of NFV on Future Mobile Networks. ETSI Future Mobile Summit, 21 November 2013. http://docbox.etsi.org/workshop/2013/201311_FUTUREMOBILESUMMIT/10_DTAG_JANSSEN.pdf

[59] Mobicell Blue Ocean Wireless, http://mobicellblueoceanwireless.com/mvno-modes.html

[60] SIGMONA Internal Report IR5.1, Regulation State-of-the-Art

[61] Madhusanka Liyanage, Oscar Lopez, Jukka Salo

[62] Squire Technologies: Assessing and Resolving Challenges for MVNOs. To build a more profitable business. http://www.squire-technologies.co.uk/solutions/mvnos-mvnes

[63] "The Future Networked Society, A White Paper from the EIFFEL Think Tank", Petri Mähönen, Dirk Trossen, Dimitri Papadimitriou, George Polyzos, David Kennedy, December 2006, http://www.fp7-eiffel.eu/

[64] "Trends in Telecommunications Reform 2007, the road to the next-generation networks (NGN)", ITU, September 2007

[65] FUTURE BOTTLENECKS IN THE INFORMATION SOCIETY, Report to the European Parliament, Committee on Industry, External Trade, Research and Energy (ITRE), June 2001, EUR 19917

[66] U.S. Federal Communications Commission: Unofficial announcement of Commission action. [online] [Accessed on 11 May 2011] at http://www.telecomlawmonitor.com/uploads/file/NN%20Public%20Notice.pdf.

[67] Kiss, J., 2008. Sony's Blu-Ray wins HD DVD battle. *The Guardian*. [online] [Accessed on 11 May 2011] at http://www.guardian.co.uk/media/2008/feb/19/digitalmedia.sony.

[68] SAIL Deliverable DA7: New Business Models and business dynamics of the future networks

[69] Architecture and Design for the Future Internet: 4WARD EU Project, Luis Correia, Henrik Abramowicz, Norbert Niebert, KlausWünstel. Springer 2010.

[70] Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office

[71] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

[72] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services

[73]

Appendices

A.1 Mobile Virtual Networks – business concepts

According to [6], The Mobile Virtual Network Operator (MVNO) is a wireless communications services provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a mobile network operator to obtain bulk access to network services at wholesale rates, and then sets retail prices independently. An MVNO may use its own customer service, billing support systems, marketing and sales personnel or it may employ the services of a mobile virtual network enabler (MVNE).

The different business models in the Mobile Virtual Network Operator (MVNO) market are based on how the value chain is restructured. Therefore, four main business models that emerge are: Branded Reseller, Light MVNO, Full-MVNO and Network enablers [7] [62].

> **Branded reseller** is the lightest MVNO business model, where the venture just provides its brand and, sometime, its distribution channels. While the mobile network operator (MNO) provides the rest of the business, from access network to the definition of the mobile service offer. This is the model that requires the lowest investment for a new venture, therefore the fastest to implement. However, most of the business levers remain with the network provider (MNO or MVNE). Therefore, the new venture has a very limited control of the business levers and value proposition of the service.
>
> **Full-MVNO** is the most complete model for a new venture, where the mobile network operator just provides the access network infrastructure and, sometimes, part of the core network, while the new venture provides the rest of the elements of the value chain. This MVNO business model is typically adopted by telecom actors that could gain synergies from their current business operation.
>
> **Light-MVNO** is an intermediate model between a branded reseller and a full-MVNO. This model allows new ventures to take control of the marketing and sales areas and, in some cases, increase the level of control over the back-office processes and valued-added services definition and operations.
>
> **Network enabler**, typically known as **Mobile Virtual Network Enabler (MVNE)**, is a third party provider focused on the provision of infrastructure that facilitate the launch of MVNO operations. An MVNE can be positioned between a host MNO and an MVNO venture to provide services ranging from value added services and back office processes to offer definition. MVNEs reduce the entry barriers of MVNO ventures, given that an MVNE aggregates the demand of small actors to negotiate better terms and conditions with host MNO.

The MVNO market is flourishing and growing around the world, but it is a fiercely competitive environment. As of October 2012 there were 634 active MVNO operations worldwide, which in turn are operated by 503 companies (some companies operate multiple MVNOs in the same country).The largest multi-country MVNO is Lycamobile, which operates in 17 countries [6] [62].

Full-MVNOs provide their services as network operators having their own interconnection links with other network operators and their own interconnection agreements. MVNOs need to be able to efficiently deliver traffic across and between networks. Instead of relying on the hosting partner to manage all traffic routing, an MVNO can create its own interconnection relationships either directly or via hubs, in order to capitalize on better margins for delivering a call.This can be particularly advantageous if there is a significant proportion of traffic for specific destinations [62].

A.2 Key concepts of Security and Privacy

According to [25], the concept of privacy is a fundamental motivation for security. Privacy is commonly understood as the right of individuals to control what information related to them may be collected and stored and by whom and to whom that information may be disclosed. By extension, privacy is also associated with certain technical means (e.g., cryptography) to ensure that this information is not disclosed to any other than the intended parties, so that only the explicitly authorised parties can interpret the content exchanged among them.

Most commonly, privacy and confidentiality are used as the same term, but it should be noted that differentiation between privacy and data confidentiality exists [36], the former relating to the protection of the association of the identity of users and the activities performed by them (such as online purchase habits), and the latter relating to the protection against unauthorised access to data content. Encryption, access control lists, and file permissions are methods often used to provide data confidentiality.

Information security is related with the requirement that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information on this (e.g., in accordance with EC Directive 95/46/EC), inter alia about the purposes of the processing, and the subscriber is offered the right to refuse such processing by the data controller.

Network security is related with the requirement to protect sensitive data from unauthorised access or accidental disclosure. The network security problem is typically divided into integrity and confidentiality. The integrity problem affects public information (e.g., stock information) and can be addressed by signatures and checksums *that need to be verified*, while confidentiality requires encryption. The more problematic aspect of trust in a network is related to authentication, access control and authorisation, when the first question to be checked is whether you are connected to the entity you intended, with no malicious middlemen.

The communication security dimension is a new dimension defined in [36] that ensures that information flows only between authorised end points. This dimension deals with measures to control network traffic flows to prevent traffic diversion and interception.

Data integrity is the property that data have not been altered in an unauthorised manner. By extension, data integrity also ensures that information is protected against unauthorised modification, deletion, creation, and replication and provides an indication of these unauthorised activities.

The availability security dimension ensures that there is no denial of authorised access to network elements, stored information, information flows, services and applications due to network interruption. Network restoration and disaster recovery solutions are included in this category.

Authentication is the provision of proof that the claimed identity of an entity is true. Entities here include not only humans, but also devices, services and applications. There are two kinds of authentication: data origin authentication and peer entity authentication.

Lawful interception is the interception of telecommunications by law enforcement agencies (LEA's) and intelligence services, in accordance with local law and after following due process and receiving proper authorisation from competent authorities.

Network dependability summarises that without reliable communication networks and services, public welfare is endangered, economic stability is susceptible, other critical sectors are exposed, and state security is threatened. The long-term benefits of reliable communication networks are incomparable. The people of Europe stand to greatly benefit from the anticipated economic efficiency, citizen connectivity, functional flexibility and speed.

A.3 Regulatory Objectives in Cloud Computing

The key regulatory targets for Security and Privacy in Cloud Computing are listed in the following [15], [19], [20]:

1) **Promote the Digital Single Market** to encourage efficient cross border cloud services; harmonised implementation of all relevant Directives and legislative instruments are needed in the EU and in the global context.
2) **Balance of interests** in protecting privacy and in fostering the EU-wide and global use of cloud computing services; Europe to become not only cloud-friendly but cloud-active to fully realise the benefits of cloud computing; Note: the current laws may discourage non-European users from using EU-based cloud computing providers or making use of European data centres.
3) Privacy legislation is looked at in a **global context** and its compatibility with Cloud Computing has to be ensured; Cloud Computing has to be facilitated in Europe and at a global level; Different jurisdictions / regions shall cooperate to develop interoperable requirements that facilitated information flows with appropriate security and privacy protection.
4) **Foster interoperability and data portability in the Cloud**; Endorse technology neutrality and promote competition; Avoid mandated standards or preferences that could frustrate, rather than promote, on-going interoperability efforts of the industry at large and among the vendors providing Cloud services and solutions.
5) **The applicable law must be easy to define**; A single set of rules on data protection, valid across EU, shall be set up; A legal framework is needed that can be applied across borders, which gives users the means to exercise their rights across borders, which is based on the concept of accountability and draws on technological controls and self regulatory codes and mechanisms as supported by Articles 17 and 27 of the Directive 95/46/EC.
6) **The right to be forgotten**, i.e., the right for the individual to request deletion of his/her personal data.
7) **Increased responsibility and accountability** for those processing personal data.

A.4 Guidelines for Security and Privacy by National Institute of Standards and Technology (NIST)

The key guidelines from the National Institute of Standards and Technology (NIST) [41] are summarized and listed below and are recommended to federal departments and agencies.

Carefully plan the security and privacy aspects of cloud computing solutions before engaging them.

As with any emerging information technology area, cloud computing should be approached carefully with due consideration to the sensitivity of data. Planning helps to ensure that the computing environment is as secure as possible and is in compliance with all relevant organizational policies and that data privacy is maintained. It also helps to ensure that the agency derives full benefit from information technology spending.

- The security objectives of an organization are a key factor for decisions about outsourcing information technology services and, in particular, for decisions about transitioning organizational data, applications, and other resources to a public cloud computing environment.
- Understand the public cloud computing environment offered by the cloud provider and ensure that a cloud computing solution satisfies organizational security and privacy requirements.
- Cloud providers are generally not aware of a specific organization's security and privacy needs. Adjustments to the cloud computing environment may be warranted to meet an organization's requirements. Organizations should require that any selected public cloud computing solution is configured, deployed, and managed to meet their security, privacy, and other requirements.
- Ensure that the client-side computing environment meets organizational security and privacy requirements for cloud computing.
- Cloud computing encompasses both a server and a client side. With emphasis typically placed on the former, the latter can be easily overlooked. Maintaining physical and logical security over clients can be troublesome, especially with embedded mobile devices such as smart phones. Their size and portability can result in the loss of physical control. Built-in security mechanisms often go unused or can be overcome or circumvented without difficulty by a knowledgeable party to gain control over the device.
- Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments.
- Organizations should employ appropriate security management practices and controls over cloud computing. Strong management practices are essential for operating and maintaining a secure cloud computing solution. Security and privacy practices entail monitoring the organization's information system assets and assessing the implementation of policies, standards, procedures, and guidelines that are used to establish and preserve the confidentiality, integrity, and availability of information system resources.

A.5 Arguments for impact assessment of Security & Privacy issues

A. Responsibility ambiguity

Responsibility ambiguity/Clouds (1, 3, 5, 6, 7)

- 1), 3): New system elements may bring new actors and roles to run the networks and business on it. The roles and responsibilities have to be clear and defined in the same way across country borders. Harmonised implementation of Directives is important to for the Digital Single Market in Europe. Harmonised rules and their implementation are needed for deployments in the global context
- 5): The applicable law has to be easy to define, but also, when defined, the law has to be easy to apply. A prerequisite for that is that the Responsibilities have been clearly defined.
- 6): When you own your data, you shall have the 'Right to be forgotten'.
- 7): Privacy is a key issue when discussing about the wide exploitation of the Clouds technologies. In the Clouds environment the access to the personal data is made possible to such actors and people, who are not in the business where that data is needed. I.e, they are outsiders, who are not familiar with the rules and practices of the business in question. The responsibility and accountability have to be made clear.

Responsibility ambiguity/NFV (4)

- 4): It has to be avoided that that the pieces of SW (VNFs) could be delivered to an operator by a single SW vendor, only. This can be ensured by the standardised interfaces between the different SW and HW layers.

Responsibility ambiguity / SDN (1, 4, 7)

- 1): The interfaces of the SDN controller have to be clearly defined (standardised) to allow wide markets for the product and competition between vendors.
- 4): SDN controllers may need to interoperate between the network layers of the same operator, or between the controllers of different operators. Clearly defined and standardised interfaces enable competition between the SDN controller vendors.
- 7): SW in SDN may be delivered by several vendors. In the installation phase the installing personnel may have access to personal data. The responsibility and accountability –requirements are not valid only for operating personnel but also for those doing installations.

  When implementing SDN with the Clouds technologies, the impacts on the regulatory targets are very much the same as stated above.

B. Bylaw conflict

Bylaw conflict / Location of legal disputes / Clouds (1, 2, 3, 5, 6)

- 1), 3), 5), 6): Promoting the Digital Single Market implies that the jurisdictions for data protection are very much the same (or similar) across countries and regions. The applicable law has to be easy to define, globally.
- 2): As the same data may be located in different countries and regions, the balance of interest with respect to protecting privacy has to be understood and agreed in the same way across countries and regions.

Bylaw conflict / Location of legal disputes / NFV (1, 2, 3, 5, 7)

- 1), 2), 3), 5): An important aspect of virtualisation is that the participating entities (network infrastructure providers, mobile virtual network enablers, virtual network operators, users) may be independent, and operating and locating in different countries.

Thus, it cannot be assumed that they always cooperate to ensure that all aspects of the system operate correctly and securely. Joint and balanced rules w.r.t. the location of legal disputes would promote competition.

- 7): In addition to different participating entities above, also multiple vendors are expected to deliver and set up the different virtualised elements. Clear rules w.r.t. the location of legal disputes would increase responsibility and accountability.

Bylaw conflict / Location of legal disputes / SDN (2, 3)

- 2), 3): The communication channels between the control plane and user plane elements, and between applications, open up new threats for Security and Privacy. The communication security has to be agreed and guaranteed such a way that the balance of interests is maintained in a harmonous way EU-wide and across regions.

C. <u>Shared environment</u>

Shared environment / Clouds (2, 3, 5, 7)

- 2), 3): The resources are virtualized and different users - possibly competitors - share the same infrastructure. This may take place within a country or region, or across countires and regions. The balances of interest may be different in different countries and regions, i.e., the rules are not the same. This will cause difficulties to run a global business.
- 5): A legal framework is needed that can be applied across borders, which gives users the means to exercise their rights across borders. Who are the competitors who share the same resources depends on how the virtualised environment has been distributed across countries and regions. In the home countries of those competitors very different rules may be applied.
- 7): Responsibility and accountability are most important in the shared environments and should be authorised and monitored by an authority.

Shared environment / NFV (2, 3, 7)

- 2), 3): The interconnectivity among the virtualised architectural components exposes new interfaces that, unless protected, can create new security threats. And more so in the shared environment. Both EU-wide and global agreements are needed to find the right balance of interest in protecting privacy and in fostering global use of new network concepts.
- 7): In the shared environment multiple parties – possible competitors – share the same infrastructure. The access to products delivered by a vendor shall be allowed only to authorised persons of the operator, or to the maintenance people of the vendor in question.

Shared environment / SDN (4, 7)

- The new SDN concept opens the doors for new SW vendors, but the prerequisite for that is that the open interfaces have been defined between different system elements. The responsibilities have to be clear so that the personal data can be protected e.g. in the SW installation phase,

D. <u>Different objectives for Trust</u>

Different objectives for Trust / Clouds (1, 3, 5, 6)

- 1), 3), 5), 6): The participating entities are independent and may be driven by different objectives. The digital single market at the EU level can become a reality only if the same rules for Trust can be agreed upon by every entity of the business environment. The global level of digital single market implies that the rules for Trust can be agreed across regions. No entity shall be allowed to follow its own rules.

Different objectives for Trust / NFV (5)

- The virtualised network functions may be run by MVNOs with the home base in different countries. Their MVNEs, which also be be operating in different countries, may have different objectives for trust.

Different objectives for Trust / SDN (5)

- The SDN controller will probably belong to the same participating entity as the network which is controlled by it. If not and in a case that an MVNO's controller is located in a different country than some parts of the controlled network, it is important to know the applicable law if the conflict of interest would arise. Whether this is a real case, will be elaborated more when the businss aspects of these new systems become more clear.

E. Interconnectivity

Interconnectivity / Clouds (1, 2, 4, 5)

- 1): The interconnectivity between the systems of different CSPs exposes new interfaces that, unless protected, can create new security threats. Standardization of the interfaces and potential encryption methods would increase and enable the level of Security and Privacy and, hence, promote Digital Single Market.
- 2), 4): The level of standardisation and encryption in interconnecting Clouds has a direct impact on the balance of interest between protecting privacy and fostering EU-wide and global use of services.
- 5): The parts of the clouds may be located in different countries, but are interconnected. The applicable law in case of the security frauds has to be known.

Interconnectivity / NFV (1, 2, 3, 4, 5)

- 1), 2), 3), 4), 5): The new acrcitecture opens up opportunities for new participating entities and promote Digital Single Market only if interfaces are open. This requires harmonised views on the legislation.

Interconnectivity / SDN (1, 2, 3, 4, 5, 7)

- 1): Different elements of the system (applications, control plane, data plane) are tightly interconnected. and potentially delivered by different vendors, and run by many participating entities. Almost all regulatory objectives can be promoted by clearly defined open interfaces.

F. Single point of failure

Single Point of Failure / Clouds, NFV, SDN

- The networks are the critical infrastructure and the basis for many governmental and commercial services. A Single Point of Failure is not acceptable in the system. This issue, however, has little impact on the listed regulatory objectives.

G. Loss of Governance, Loss of control

Loss of governance, Loss of control /Clouds (4, 5, 6, 7)

- 4): An enterprise, who is migrating a part of its own IT system to a cloud infrastructure, gives partially the control of its operations to the Cloud Service Provider. However, that enterprise can reduce its dependency on that Cloud Service Provider, if the Interoperability and data portability between the systems of the Cloud Service Providers have been implemented.
- 5): The Clouds components may be located in different countries and regions. For a Cloud Service Provider and for an enterprise user, irrespective of where are their home bases, it is vitally important that the rules for applicable law are clearly defined.
- 6): 'The Right to be forgotten' is important for a private user, probably also for an enterprise user. When the control is lost to a third party, how to ensure the data related to you is deleted when you change the Service Provider?

- 7): En enterprise or a private person takes a risk when migrating its data to be stored by a third party like a Cloud Service Provider. The responsibilities and accountability have to be clear.

Loss of governance, Loss of control /NFV (4, 5, 7)

- Loss of governance in the context of NFV may become true if the Network Operator would outsource the running of some virtualised network functions to a SW provider. In that case interoperability, right to be forgotten and responsibility should be paid attention to. This case may not be so probable in the near or mid-term future, however.

Loss of governance, Loss of control /SDN

- It may not be realistic to assume that a Network Operator would give the control of its network to an external actor.

H. <u>Service Provider lock-in</u>

Service Provider lock-in /Clouds (1, 4)

- 1): Digital Single Market implies that no Service Provider is dominating the markets, and applying e.g. its own standards for Interconnection and data portability. From an enterprise user’s point of view Digital Single Market means that there are several competing Cloud Service Providers and the portability has been implemented between their systems.
- 4): An enterprise can reduce its risk on the Service Provider lock-in, if the Interoperability and data portability between the systems of the Cloud Service Providers have been required and implemented.

Service Provider lock-in /NFV (4)

- 4): A Network Operator can reduce its risk on the SW Provider lock-in, if the Interoperability and data portability between the system functions have been defined and implemented.

Service Provider lock-in /SDN (4)

- In the SDN concept, the SDN controller and other functions are implemented with SW. To avoid the lock-in to a SW provider the Interoperability and data portability between the system functions have to be defined and implemented.

I. <u>Visibility</u>

Visibility/Clouds (1, 7)

- 1): Transparency in the way a Cloud Service Provider operates is a vital ingredient for effective oversight over system security and privacy by an organization. The transparency across country borders and regions is vital for Digital Single Market. However, by disclosing its operating practices a Cloud Service Provider may also lose its key competitive advantages.
- 7): What-ever the level of transparency of the operations of the Cloud Service Provider is, the responsibilities and accountability have to be clear and agreed.

Visibility/NFV, SDN

- The NFV concept, and perhaps also the SDN concept, may allow that new MVNOs, for instance, have easier entry to the market than currently is the case, and the visibility and transparency of the Security and Privacy measures are of key importance. However, regarding these new technologies there seems to be no direct impact of Visibility on the regulatory targets.
- In the NFV and SDN contexts, the visibility or transparency seems not to be relevant w.r.t. impact on the regulatory objectives.

J. <u>Protection inconsistency</u>

Protection inconsistency/Clouds (1, 3, 4)

- 1): The protection mechanisms of the distributed security modules which may be resided in different clouds, or not in a cloud at all, may not be consistent.This will have a big impact on the development of the Digital Single Market.
- 3): Since the Clouds and protection elements may be located in different countries and regions, the consistency and interoperability have to be reached globally.
- 4): Interoperability is a key requirement when implementing the consistency of protection mechanisms with distributed modules.

Protection inconsistency/NFV, SDN

- It is difficult to see a reason for that the protection mechanisms within the network, which is implemented with the NFV or SDN technologies, would not be inconsistent. The functionality of the network is not expected to change with the emergence of these two technologies.