FLAMINGO

European Seventh Framework Network of Excellence

`http://www.fp7-flamingo.eu/`

WP7 — Economic, Legal and Regulative Constraints

Deliverable D7.3 — Fine Design and Prototype

University of Twente, The Netherlands (UT)
Institut National de Recherche en Informatique et Automatique, France (INRIA)
University of Zurich, Switzerland (UZH)
Jacobs University Bremen, Germany (JUB)
Universität der Bundeswehr München, Germany (UniBwM)
University Politecnicà de Catalunia, Spain (UPC)
iMinds, Belgium (iMinds)
University College London, United Kingdom (UCL)

Project funded by the European Union under the
Information and Communication Technologies FP7 Cooperation Programme
Grant Agreement number ICT-FP7 318488

Document Control

Title:	WP7 — Economic, Legal and Regulative Constraints
Type:	Public
Editor(s):	Radhika Garg, Burkhard Stiller
E-mail:	garg@ifi.uzh.ch, stiller@ifi.uzh.ch
Doc ID:	D7.3
Delivery Date:	31.10. 2015
Authors:	Anna Sperroto, Bram Naudts, Burkhard Stiller, Christos Tsiaras, Corinna Schmitt, Daniel Dönni, Daphne Tuncer, Guilherme Sperb Machado, Joan Serrat, Javier Rubio Loyola, Marinos Charalambides, Mario Flores, Patrick Poullie, Radhika Garg, Rashid Mijumbi, Sacha Uhlmann, Sebastian Seeber, Sofie Verbrugge

For more information, please contact:

Dr. Aiko Pras
Design and Analysis of Communication Systems
University of Twente
P.O. BOX 217
7500 AE Enschede
The Netherlands
Phone: +31-53-4893778
Fax: +31-53-4894524
E-mail: <a.pras@utwente.nl>

Legal Notices

The information in this document is subject to change without notice.

The Members of the FLAMINGO Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the FLAMINGO Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Contents

1 Executive Summary

WP7 develops cross-disciplinary methodologies for finding and determining technological dependencies on economical, legal, and regulative aspects. These interdependencies are the foundation for successful implementation, deployment, operation, and maintenance of services and networks. Therefore, the purpose of this document is to analyze and discuss key scenarios (in close collaboration with WP5 and WP6) in a use-case-based manner from these perspectives.

WP7 integrates three pillars of (a) business goals, (b) economic goals, and (c) legal and regulative constraints. The first pillar of business goals was studied in full along with relevant conclusions in Y2. To analyze the remaining two goals, the experience and engagement in the third year of FLAMINGO with those technologies under the umbrella of the Future Internet (FI) helps this deliverable D7.3 to identify major facts and achieves major findings for answering the two major questions:

1. What are the possible constraints of management technology and solutions from the economic, legal, and regulative domains that enable, border, or restrict operations and management of networks and systems?
2. What are the mechanisms that can be used to validate the assumptions, methodologies, and results followed on a per scenario basis, not only from technical perspective but also from economical and legal and regulative perspective?

In reply to these questions, WP7 identified relevant perspectives that include economics, and legal and regulative constraints. The economic analysis comprises of the following major facets: cost modeling, pricing schemes, and, where applicable, an incentives discussion. Additionally, legal and regulative constraints impacting network and service management in the field of data storage and processing retention, cross-border data flow, and network neutrality, form an integral part of this deliverable.

In order to numerically validate the current status of the work within WP7, three validation mechanisms (originating from the Y2 determination) have been applied in more depth on scenarios of Resource Management in Network Function Virtualization, ISP-oriented Content Delivery, and Legal and Ethical Facets of Data Sharing, where possible. First, the meta method termed “Tussle Analysis” allows to perform a socio-economic-aware analysis of future networks; this has resulted in the newly standardized ITU-T recommendation Y.3013 in August 2014. This method was applied to the scenario of ISP-oriented Content Delivery. Second, the validation by value networks and dynamic value network analysis enables the identification of the value a technology will create on the economic and the business landscape. Third, in collaboration with external experts, an interview-based verification of WP7 scenarios’ assumptions, methodologies, and mechanisms has been performed. Both second and third validation mechanisms were applied to all the three scenarios.

In conclusion, the design, analysis, and discussion of scenarios (in close collaboration with WP5 and WP6) within the scope of WP7 was able to verify the initial assumptions of a general interdependency of technological requirements and economic, legal, and regulative constraintsánalysis. This does form the basis to identify guidelines to deploy similar technologies in the field of network and service management in the last FLAMINGO year to come.

2 Introduction

Fast growing networks in today's world need to coherently address in an integrated manner operations, management, and maintenance of the networks with respect to economics, legal, and regulative constraints. While the business perspective has been completed in Y2 of FLAMINGO, Y3 delved into the economic dimension addressing the incentives, pricing, and cost benefit analysis. The integrated legal dimension will address major stakeholders imperatives in a certain country or region, and the integrated regulative dimension will address impacts and effects of country- or region-specific regulations.

2.1 Goals of D7.3

The first goal of this deliverable D7.3 is to cover the integration of traditional technological views with optimization-driven economic approaches as well as legal and regulative constraints in a cross-disciplinary methodology. The second goal of this deliverable is to identify and apply validation mechanisms in order to validate assumptions, approach, and results of all the scenarios within WP7. Details of several numeric validation approaches developed and applied in WP7 are available in Section 4 and Section 6. The third goal is to identify and analyze the legal and regulative constraints with respect to processing data, which forms a crucial part of managing the operation of the network (Section 5).

Thus, this section recalls the three tasks of WP7 along with their current status, introduces the methodology developed and to be applied for all investigations, and finally outlines the full deliverable structure.

2.2 Tasks of WP7

As mentioned in Description of Work, WP7 is divided into three major tasks as follows. The following paragraphs and tables describe the status and outcome of these tasks in Y3 of FLAMINGO. Task T7.2 has been completed in full in Y2, and therefore is not reported in D7.3.

- **Task T7.1: Outcomes for Economic Analysis**
  This task identifies detailed insights into economic analysis in the area of network and service management. The aim is to develop pricing models and cost models, identify incentives for stakeholders, and perform cost-benefit analysis for relevant scenarios in the field of network and service management (cf. Section 3 and Section 4). The set of current and detailed outcomes of T7.1 is summarized in Table 1.

- **Task T7.3: Outcomes for Legal and Regulative Constraints**
  This task aims to identify constraints from a legal and regulative point of view; specially in the area of data storage, retention, and sharing, cross border data flow, Schengen routing, network neutrality, and cloud federations and resource allocations (cf. Section 5). The set of current and detailed outcomes of T7.3 is summarized in Table 2.

Table 1: Task T7.1-Outcomes for Economic Analysis

No.	Task Activities	Status as of Y3	Description	Section	To be Addressed in Y4
1.1	Multi-actor cost-benefit analysis for network management and operations	IN PROGRESS	Cost model of Internet Service Providers is being studied (including caching infrastructure), multi-actor analysis is used to incorporate the interests of all actors	Section 4.3	Code implementation and results
1.2	Trade-offs between cost of operations and obtained Quality-of-Experience (QoE)	DONE	QoE measures were gathered via custom developed mobile application	D7.2	-
1.3	Pricing approach as a trade-off to match user's demand, Quality-of-Service (QoS), and resource availability	IN PROGRESS	Pricing model for virtualized resources is being studied	Section 4.2	Code implementation and results

Table 2: Task T7.3-Outcomes for Legal and Regulative Constraints

No.	Task Activities	Status as of Y3	Description	Section	To be Addressed in Y4
3.1	Determining QoS fulfillment aspects	FUTURE	-	-	Fulfillment aspects of QoS will be studied from legal and regulative perspective
3.2	Policy-based aspects in view of legal or regulative limitations	FUTURE	-	-	Legal and Regulative implications on business modeling will be studied
3.3	Cost and accounting models in view of legal or regulative limitations	IN PROGRESS	Regulative aspects of incentive auctions have been studied	D7.2	Legal and Regulative implications on cost and accounting models will be studied
3. 4	Network neutrality aspects for management	DONE	Regulative aspects of network neutrality are being studied	Section 5.2	-
3. 5	Investigating adoption of cloud-based solutions from legal and regulative perspective	DONE	Legal and Regulative aspects of cloud adoption have been identified and modeled	Section 5.4	-
3. 6	Investigating legal and regulative constraints of data sharing due to the analysis of data in network and service management	IN PROGRESS	Legal, regulative, and ethical aspects of data storing, data sharing, data retention are being studied	Section 4.4	Legal and regulative aspects in these areas will be completed on a use-case basis

By addressing the overall goal, the following three targets are addressed by the methodology chosen: First, to validate the assumptions, methodology, and results of scenarios with applying different techniques. Second, to establish guidelines for suitable models for techno-economic interdependencies, legal, and regulative recommendations (which will be covered in Y4 of FLAMINGO). Third, to perform detailed analysis of scenarios that are part of FLAMINGO's technical scope, especially from WP5 and WP6.

Taking the analysis ahead with the above mentioned goals in mind, appropriate and relevant scenarios were identified, which in terms of their technical content are based on the objectives of WP5/WP6. The area of research focusses on network and service monitoring, which also addresses virtualization strategies, content delivery, and automated configuration and repair of managed objects. To this end, three major scenarios are identified and analyzed (as described in Section 4). Based on the relevance and scope two of these scenarios (iMinds-UPC-NetVirt, UCL-iMinds-Cache) were already part of WP7 since the beginning of the project. The third scenario of UT-UZH-Ethics became part of WP7 in Y2 of FLAMINGO. In Y3, these three scenarios, have covered more in-depth analysis with respect to validation and identifying legal and regulative boundaries and implications, which form a foundation for identifying guidelines in Y4. The validation was based on three techniques of value network analysis, tussle analysis, and interviews with external industrial partners. The first two mechanisms validated the role of the stakeholders, their incentives, interests, value exchanges, and identify potential tussles between them. The third mechanism aimed to validate the assumptions, methodology, and partial/full results of the scenarios from technical, economical, and legal and regulative perspectives. In addition to that, WP7 also concentrated to numerically validate the approaches followed specifically from legal and regulative domain. The aim was to have the foundation of identified status of legal and regulative constraints on measurements and modeling of Internet traffic. This also consisted of modeling laws and regulations itself, in order to incorporate it in evaluating the compliance of a system or service provider to regional or country-specific regulations.

2.3 Document Structure

The remainder of Deliverable D7.3, entitled “Fine Design and Prototype”, is structured in the following manner.
Section 3 “Methodological Framework” describes two of the validation techniques-value network and tussle analysis- that are applied in Y3 to validate the scenarios.
Section 4 “Numerical or Policy-based Validations of Scenarios”, summarizes and describes scope of the scenarios involved in WP7. This is done based on boundary map, stakeholder analysis, and risk analysis. In addition, value network and tussle analysis are applied to validate the scenarios.
Section 5 “Legal and Regulative Considerations”, discusses the current status quo and open issues in regulations impacting the field of network and service management. In addition, modeling of relevant regulations in case of Cloud Computing, is described.
Section 6 “Validation of Scenarios” concentrates on validating the work within WP7 from external partners.
Section 7 finally summarizes, concludes the current work and discusses the work foreseen.
Section 8 “WP7 Objectives”, lists the objectives of WP7 as stated in the FLAMINGO Description of Work and reports their status.
Section 9 “Abbreviations”, lists all the abbreviations used in the deliverable D7.3.
Section 10 “References”, contains details of all the references used within the deliverable.
Section 12 “Appendices”, contains all filled in questionnaires from the external partners collected during the interview-based validation approach.

3 Methodological Framework

Several of the scenarios described in Section 4 propose a technological evolution away from conventional network management architectures. One such example is of ISP oriented content delivery scenario in which network providers deploy server infrastructure inside their network. Another example is that of resource management in network function virtualization scenario in which virtualization techniques are used to consolidate network equipment onto high volume compute, storage and networking resources. These scenarios have the potential to address current challenges in a network provider's network such as ever growing user traffic and the need for cost containment via technological change. What remains the same, however, is that the Internet is a platform composed of a patchwork of technologies that interconnects multiple interacting actors. A technical solution therefore needs to address the techno-economic and socio-economic viewpoint. In techno-economic analysis, different system solutions are evaluated one next to the other via a simulation based approach. Socio-economic analysis on the other hand is used to gain an understanding of system requirements and to design a flexible and successful Internet architecture.

To provide some context, we will first present our methodology for identifying the network of actors, the mapping of roles to the actors as well as the dynamics and the tussles that may exist between different roles. This is done via value network analysis, a newly proposed method coined dynamic value network analysis and tussle analysis. An overview of the validation mechanisms and their interrelationship is given in Figure 1. We also describe the interrelationship between these methods. In order to make things more concrete, we apply these tools to relevant scenarios in the next section.

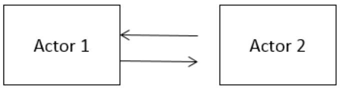
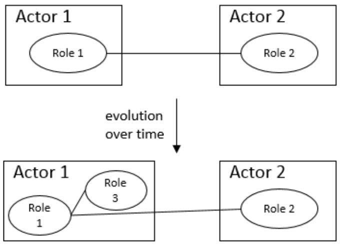
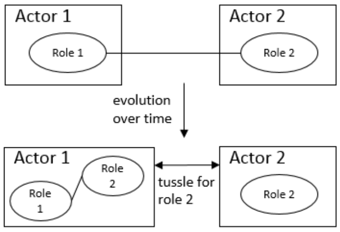
method	analyses	studies	example diagram
value network analysis	how is value created	the static relationships at the level of actors	
dynamic value network analysis	how does value evolve over time	the dynamic relationships at the level of roles	
tussle analysis	how to resolve conflicts between actors	the competition between actors at the level of roles	

Figure 1: Overview of Validation Mechanisms and their Interrelationships.

3.1 Value Network Analysis

Value network analysis is used to answer the question of "How is value created?" by investigating the dynamic exchanges between one or more enterprises, customers, suppliers, strategic partners and the community [1]. The exchanges involve a medium of exchange called a currency. Three types of currency are defined:

1. Goods, services and revenues
2. Knowledge
3. Intangible benefits

The first step of value network analysis is the identification of all primary actors and their characteristics. Examples of actors are a network provider, an equipment vendor, a regulator, a subscriber, etc. The second step of value network analysis is to interconnect the different actors by mapping the value network exchanges on a value network diagram. These value exchanges represent a flow of goods, services and revenues, a knowledge flow or a creation of intangible benefits. After the value network diagram has been prepared, it can be used to perform three complementary analyses:

1. Exchange Analysis: investigation of the general pattern of the exchanges in the network, sufficient reciprocity, existence of weak or inefficient links
2. Impact Analysis: how an involved party can create value from the received inputs
3. Value Creation Analysis: assessment of the value increases that an output triggers for the customer and how the company itself benefits from it

Value network analysis focusses on mapping the situation as is currently. The next method, dynamic value network analysis, will be used to analyze how the value network will evolve with time.

3.2 Dynamic Value Network Analysis

Value network analysis provides an understanding of how value is created today. When new technological solutions emerge and are adopted, the value network will evolve from one state to the next. To analyze the underlying dynamics of change in a value network, we apply dynamic value network analysis. Value networks are used at an abstraction level that includes actors and their interrelations. This level of detail is however not adequate for dynamic value network analysis. Below, we extend the value network analysis to include value network configurations. By using value network configurations instead of value networks it is possible to study how changes (such as technological advances) have an impact on the value network. We therefore move away from the abstraction level of an actor towards the level of a functional role. The difference between an actor and a functional role is defined as follows: a functional role is a set of activities that cannot be divided between separate actors, an actor on the other hand can perform one or multiple roles in a scenario. Examples of roles in a network management environment are network planning, content network management (*e.g.,* path selection) and cache management (*e.g.,* content placement).

At the level of roles, value network analysis is replaced by the dynamic value network analysis method. This method separates the actors from the functional roles performed by an actor. This allows to analyze multiple role combinations instead of limiting to a single value network. The first step of dynamic value network analysis identifies the different roles that each actor in a value network is responsible for. This is done based on the value network diagram that was established in the previous section (Section 3.1). The result of this step is a list of roles with a description and the responsible actor. In most scenarios, relationships between the roles exist to provide the functionality under investigation. In case of a technical scenario the focus will be on the technical interfaces between roles. The second step of the methodology is therefore to identify these relationships. The result of this step is a diagram that maps the relationships between the different roles. So far this method is in line with other methods such as the value network configuration method (*e.g.,* applied in [9]). The next steps are used to examine how the value network will change due to, for example, technological advances. This is done by examining the impact of technological advances on the roles in the value network configuration:

- A role or multiple roles can switch from one actor to another actor
- A new role or multiple roles may emerge, which are performed by existing actors or a new actor
- A role or multiple roles may no longer be relevant as such actors may disappear or their economic relevance/ strategic importance may be reduced
- A role may gain importance as such an actor may gain economic relevance/strategic importance

The third step analyses if one of the above listed changes occurs in the value network configuration. If so, a new value network configuration is drawn. In the final step, the timing of this evolution is analyzed. This means that certain changes can require more time than others. By completing these steps, an evolution (over time) from one value network configuration to the next value network configuration can be visualized. The logical separation of actors and roles allows for a visualization of the dynamics in the value network by quantifying the value creation potential or strategic importance of each actor via an actor's roles. This analysis is used to describe how the value a company offers will evolve over time. It shows which companies can gain from a technical advance and which companies' value creation potential is at stake.

In this analysis we assume that actors accept the evolution from one state to the next. Actors may however compete against each other for a role. In such cases tussles emerge which are analyzed via tussle analysis.

3.3 Socio-economic-aware Design of Future Networks by Tussle Analysis

The value network configurations that have been defined during the dynamic value network analysis are used to study which tussles occur and how to circumvent them depending on which actors control a role. In a given value network configuration, several actors may compete for the same role for strategic reasons or because they believe the role can provide financial value.

In such cases, tussles emerge between the actor that is currently holding the role and the actors affected by it. The third step in the methodology is the identification of tussles. Due to ever-growing speed of end- as well as intermediate Internet devices, ways to interact and rates to exchange information with, result in the interaction of countless stakeholders of virtually all commercial, industrial, and private sectors interacting through the Internet. Therefore, the Internet is carrier for innumerable socio-economic conflicts. These colliding socio-economic interests make the Internet unpredictable. This was pointed out first by [11], which termed these conflicts tussle. Accordingly, the "Design for Tussle" of Internet technology, to preclude these conflicts, was postulated. The Tussle Analysis is a meta-method to assess, if a technology or a standard for FNs is designed in a socio-economic aware and incentive-compatible manner. It was standardized in [28]. However, well before this standard, Tussle Analysis was applied by research projects to enrich technology development [37], [31], [56]. To achieve the same advantages for technologies developed by FLAMINGO, the Tussle Analysis was introduced in Deliverable D7.2, and is applied in this section for Y3. Application of tussle analysis assesses the mid-term and long-term impact to each stakeholder and identifies potential mitigation strategies to circumvent negative impacts and the resulting losses. By applying a mitigation strategy, new tussles may arise. As such this method is iterative. This validation mechanisms is applied to the ISP oriented cache management scenario.

4 Numerical or Policy-based Validations of Scenarios

The overall WP7 work as well as all WP7-related tasks had been structured efficiently by applying project management and research techniques. Especially for describing the clear design scope of a scenario and to work within each scenario with appropriate techniques and valid assumptions (1) a Boundary Map, (2) a Stakeholders' Analysis and Stakeholders' Map, and (3) a Risk Analysis have been applied, as was done in Y2. In this section, the mechanisms are introduced again, for the completeness of information in this deliverable. This leads to a well-determined set of boundaries, which are essential to carefully target the scenarios' findings. In addition, this section also presents the result of validation analysis in terms of value network analysis and tussle analysis. The value network analysis focusses on identifying role of stakeholders involved, their incentives, and value exchanges. The tussle analysis concentrates on identifying any tussles between the stakeholders due to their varied interests or policies.

4.1 Techniques

To provide a brief overview on these techniques, the basic principles of the Boundary Map, the Stakeholders' Analysis and Stakeholders' Map, and the Risk Analysis are outlined here as was done in Y2, too. In turn in subsequent subsections those three techniques have been applied to all WP7 scenarios ensuring a determination of key assumptions, stakeholders involved, and the related risks.

Boundary Map: Research projects are in their nature never-ending. New questions appear as results are generated. Thus, defining the boundaries is an important step towards managing such projects. The project group discussions are done to identify where are the boundaries of the project as seen from the scenario today.

"The boundaries of a project are measurable and auditable characteristics that define what belongs to the project and what does not belong to it. Project boundaries are closely linked to project objectives, they create a holistic perception of project work, and they define the content of the project in terms of expected results. A clear boundary statement helps direct the things that are applicable to those areas within the project scope" [7].

Stakeholders' Analysis and Stakeholders' Map: The purpose of this is to visualize (i) the interest, (ii) the influence, and (iii) the attitude of each stakeholder that is involved in a scenario.

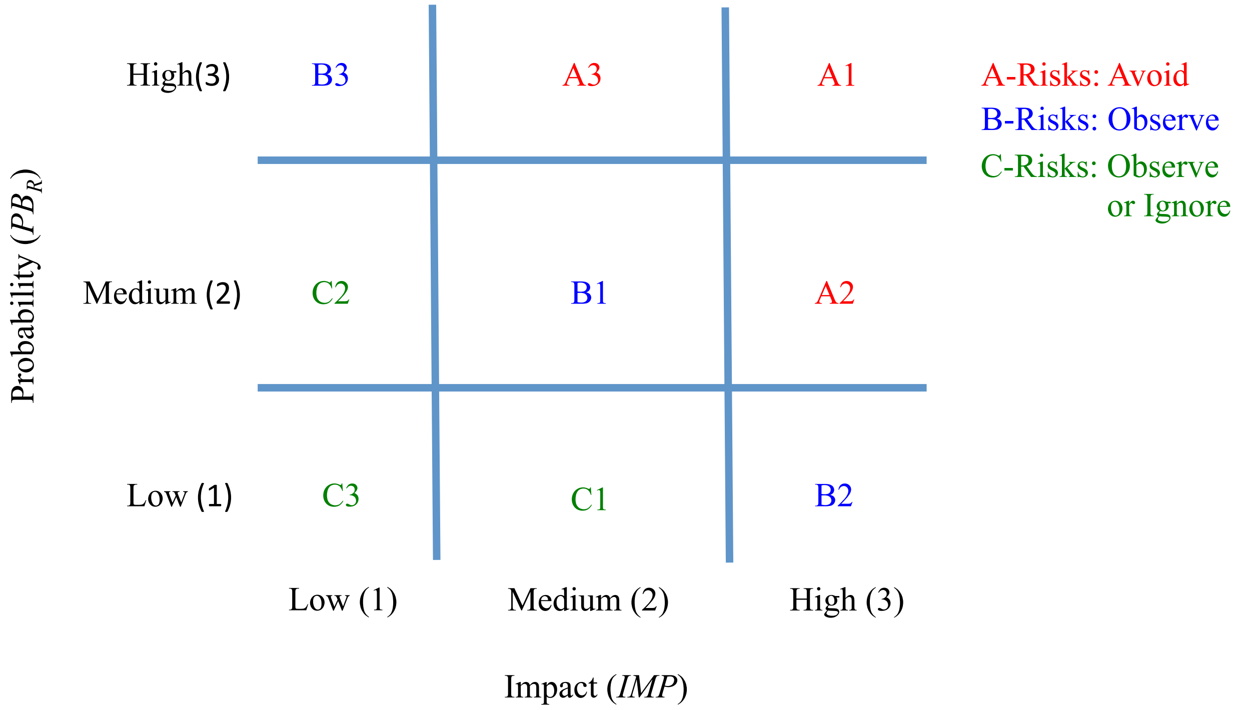
Approach:

1. Create a list of all stakeholders
2. Define their interest in the project (Low, Medium, High)
3. Define their influence in the project (Low, Medium, High)
4. Define their attitude in the project (Positive, Neutral, Negative)
5. Draw the stakeholder map

Risk Analysis: The risk analysis helps to define the potential problems that might occur, and help to think in advance of possible measures to eliminate or reduce the risk. Stakeholders that identified during the stakeholders' analysis to have a negative attitude should be also reflected in the risk analysis.

Approach:

1. Collect possible risks that are related with (a) Content, (b) Resources, (c) Time dependencies, (d) Stakeholders, and (e) Context
2. Estimate the probability (PB_R) of a risk (Low=1, Medium=2, High=3)
3. Estimate the impact (IMP) of a risk (Low=1, Medium=2, High=3)
4. Calculate the risk factor $R = PB_R \cdot IMP$
5. Identify A-risks, B-risks, C-risks according to the risk matrix (cf. Figure 2)
6. Identify the possible causes of each risk
7. Propose possible measures that can eliminate or reduce the risk
8. Address first risks with high risk factor R



Probability (PB_R) \ Impact (IMP)	Low (1)	Medium (2)	High (3)
High(3)	B3	A3	A1
Medium (2)	C2	B1	A2
Low (1)	C3	C1	B2

A-Risks: Avoid
B-Risks: Observe
C-Risks: Observe or Ignore

Figure 2: Risk Table.

Approach:

1. Ask yourself:
   What is the project all about?
   What do we have to know?
   What is interesting for us?
   What does this scenario have to deliver?
   What are the possible applications of the outcome of this scenario?
   Which topics have to be worked on in the scenario to reach the scenario's/FLAMINGO's objectives?
   Which not?
   Where could we limit the scope?

2. Draw the project's boundary to include the topics that (a) definitely, (b) maybe, and (c) certainly not belong to the project.

These approaches of project management are used in the following sections to describe the scenarios, which are studied within WP7. These approaches provide a unified and homogeneous method to describe the scenarios under the umbrella of WP7.

4.2 Resource Management in Network Function Virtualization

This joint research activity, is a collaboration between Universitat Politècnica de Catalunya (UPC) and iMinds, and is referred by UPC-iMinds-NFV. Network function virtualization (NFV) [47, 49] is being proposed as a path towards cost efficiency, reduced time-to-markets, and enhanced innovativeness in telecommunication service provisioning. NFV leverages advances in virtualization technology to consolidate many network equipment types onto high volume servers, switches and storage, which could be located in datacentres, network nodes and in end user premises. Therefore, Service Providers (SPs) depend on virtual networks (VNs) to deploy their virtualized network functions (VNFs) in the cloud whose resources, in form of substrate networks (SNs), are owned by Infrastructure providers (InPs). However, efficiently running virtualized functions is not trivial as, among other initialization steps, it requires first mapping virtual networks onto physical networks (also known as virtual network embedding [46]), and thereafter mapping and scheduling VNFs onto the VNs. This collaboration is divided into two sub-tasks, each of which is focused on one of the above problems.

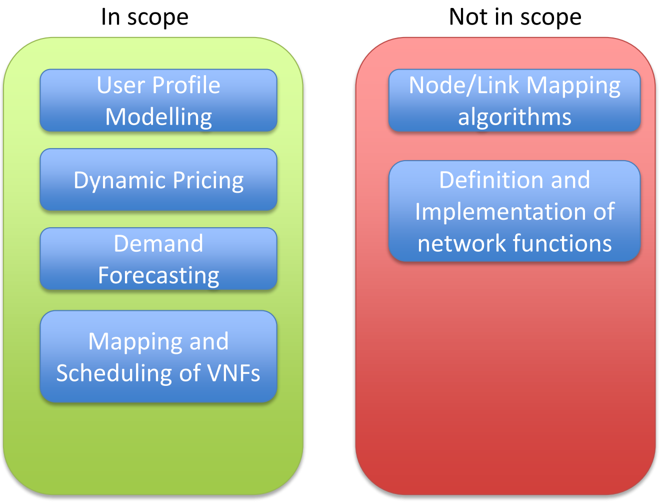

In scope
User Profile Modelling
Dynamic Pricing
Demand Forecasting
Mapping and Scheduling of VNFs
Not in scope
Node/Link Mapping algorithms
Definition and Implementation of network functions

Figure 3: Boundary Map of Resource Management in Network Function Virtualization

Virtual network embedding (VNE) allocates physical network resources to virtual nodes and links based on the specification in the VN requests. In the online VNE, one VN request arrives and is mapped at a time. It is therefore possible that VN requests with a low revenue per constrained resource are accepted and use up resources of the constrained node or link at the expense of VN requests that arrive later and have a higher revenue per constrained resource. The first task is to define a dynamic pricing approach that uses historic information about the resources to find the optimal price that should be charged per constrained resource based on the arrival rate, utilization rate and the number of resources requested of the constrained node or link.

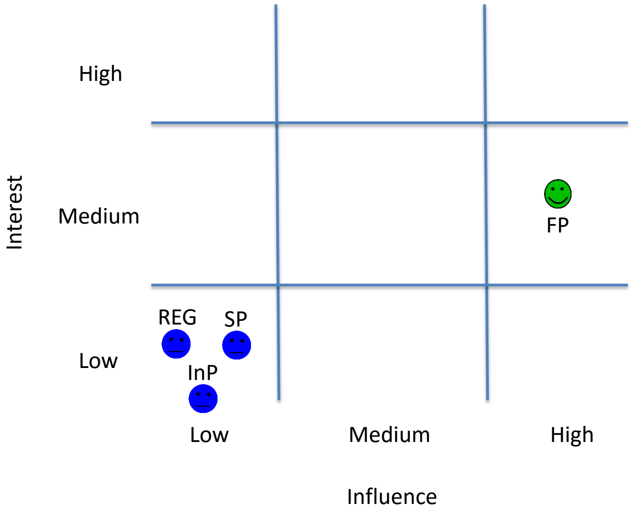


Figure 4: Stakeholders Map of Resource Management in Network Function Virtualization

In addition, since the actual load of substrate networks varies with time [45, 48], we can combine these aspects to ensure that the revenue of infrastructure providers is maximized. The second task is based on the observation that it is possible to over-sell the SN resources with the objective that the mapped VNs load the substrate network in an efficient way, and hence improve the profitability of InPs. To this end, the proposal is to continuously forecast expected demand for SN resources, and based on this, to make both dynamic SN resource pricing decisions, as well as an evaluation of an opportunity cost that can be used to either accept or reject VN request. The main difference between the focus of this work and the state-of-the-art is that the decision to accept or reject VN requests is not only based on the availability of resources. This means that an InP could decide to reject a VN request even if resources are available, it this will result into better profitability from the projected future VN requests. The contribution of this collaboration sub-task will be three-fold: (1) a user demand modelling approach that can be used as a basis for forecasting VN resource demand, (2) a dynamic pricing scheme that uses virtual network traffic predictions and hence expected opportunity cost (with respect to InP profit from VNE) to price substrate nodes and links, and (3) a virtual network embedding algorithm that uses future demand forecasts other than actual resource constraint to accept or reject virtual network requests.

Function Placement and Scheduling: One of the objectives of NFV is to achieve fast, scalable, on-demand and dynamic composition of network functions to a service. However, since a network service requires a number of VNFs, achieving a NFV environment raises two questions; (1) how to define and implement network services, and (2) how to efficiently map and schedule the VNFs of a given service onto a physical network. The European Telecommunications Standards Institute (ETSI) through its NFV technologies group is partnering with network operators and equipment vendors to promote the NFV approach and are currently progressing with regard to the first question above. Specifically, they have already defined the NFV problem, some use cases and a reference framework and architecture [47].

The second task of this collaboration is formulating the online virtual function mapping and scheduling problem and proposing algorithms for solving it. We propose three greedy algorithms and a tabu search-based heuristic. We carry out evaluations of these algorithms considering parameters such as successful service mappings, total service processing times, revenue, cost etc, under varying network conditions. Simulations show that the tabu search-based algorithm performs only slightly better than the best greedy algorithm. In particular, we propose some algorithms that perform the mapping and scheduling of VNFs based on a greedy criterion such as available buffer capacity for the node or the processing time of a given VNF on the possible nodes. The algorithms perform both mapping and scheduling at the same time (one-shot), i.e. at the mapping of each VNF, it is also scheduled for processing. In addition, we propose a local search algorithm based on tabu search (TS) [49]. The TS algorithm starts by creating an initial solution randomly, which is iteratively improved by searching for better solutions in its neighborhood. Finally, we also propose an optimal mixed integer linear programming formulation of the problem, and a heuristic approach based on hard variable fixing. These algorithms are aimed at being used as benchmarks for future algorithms in this area.

The **boundary map** in Figure 3 shows the items that are in-scope and out-of-scope for each of the two sub-tasks in this collaboration. It is worth mentioning that the items that are out-of-scope have already been well studied in the state-of-the-art and where necessary, will be used as input to some of our proposals.

Stakeholders Analysis and Stakeholders Map: The stakeholders list is summarized in Table 3 and the stakeholders map is illustrated in Figure 4. The goal is (a) to increase as much as possible the interest of every stakeholder, and (b) to change the attitude of the stakeholders, if possible, negative to neutral, or even to positive.

Risk Analysis: The list of the potential risks that has been identified during the risk analysis phase are in Table 4. The risk analysis shows that the main risk that this collaboration is facing is to not be able to get reliable cost data from the InP.

Table 3: Stakeholders Analysis of the Resource Management Network Function Virtualization

Stakeholder	Interest	Influence	Attitude
Service Provider (SP)	Medium	Low	Neutral
Infrastructure Provider (InP)	Medium	Low	Neutral
Regulator (REG)	Low	Low	Neutral
FLAMINGO partners (FP)	Medium	High	Positive

Table 4: Risks of of the Resource Management Network Function Virtualization

Risk	PBR	IMP	R	Priority	Possible Cause	Measure
Lack of reliable cost data	1	2	4	B1	data is sensitive	collect early and work with relative values

4.2.1 Validation of Resource Management in Network Function Virtualization

For validating the scenario of Resource Management in Network Function Virtualization, above described validation techniques are applied in the following sections.

4.2.1.1 Value Network Analysis Value network analysis is used to understand how value is created today (before the proposed solution is introduced). The analysis focuses on the value network embedding problem. The work done has a goal to develop a pricing approach that provides a higher total revenue to the network provider than a competitor's static pricing approach.

First, the value network diagram is drawn (Figure 5) and the value exchanges are described in Table 5.

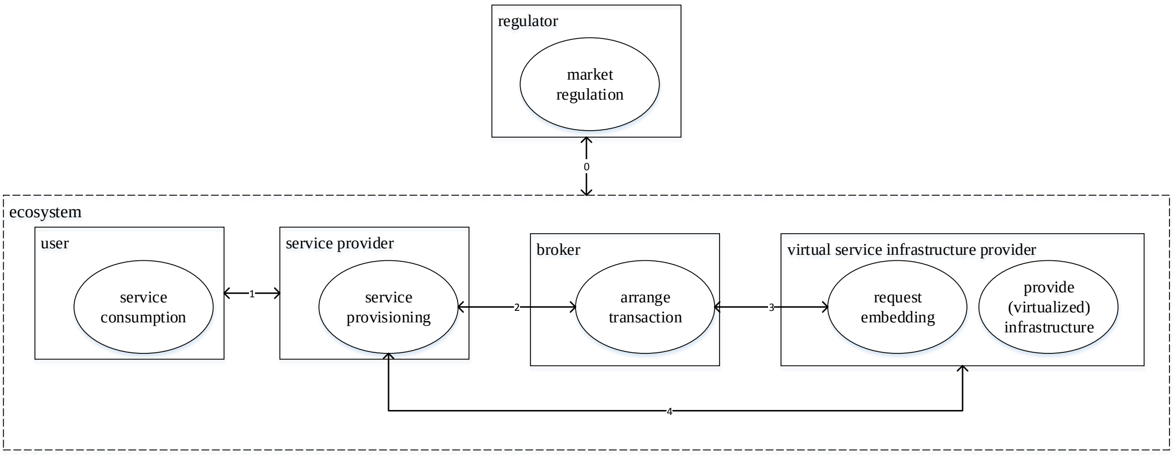


Figure 5: Value Network Diagram from the Initial User Demand to the Final Virtual Network Request Embedding.

Table 5: The Value Exchanges that Take Place Between the Actors in the Value Network Diagram, the IDs Match With Those on Figure 5.

ID	actor 1 (start)	actor 2 (end)	description
0	regulator	*ecosystem*	supervision and regulation of the industry (intangible)
	ecosystem	regulator	information about the current market structure (intangible)
1	user	service provider	service fee
	service provider	user	services (*e.g.,* IP VPN)
2	service provider	broker	brokerage fee
	broker	service provider	best offer
3	broker	virtual service infrastructure provider	market knowledge and customer acquisition
	virtual service infrastructure provider	broker	information about the availability and price of resources
4	service provider	virtual service infrastructure provider	fee based on amount of virtualized resources used
	virtual service infrastructure provider	service provider	(virtualized resources)

Based on the value network diagram, we conduct three complementary analyses:

1. Exchange analysis: to understand the general pattern of value exchanges and check if there are any inefficient links as well as to check if there is no lack of reciprocity in the value exchanges.

2. Impact analysis: to understand if each actor is able to generate value from the value exchanges

3. Value creation analysis: focuses on the value created by the actor, it considers which value creation each output generates for the customer and how the actor benefits from this

The results of these analysis are summarized in Table 6. It indicates that their is room for improvement for the pricing algorithm that is used by the virtual service infrastructure provider.

Table 6: Conclusions of the validation via value network analysis.

type	**result**
exchange analysis	The user (a consumer or business) demands a certain service (*e.g.,* IP TV or IP VPN) and negotiates with one or more service providers who offer that type of service. A rational user will choose the service with the best price versus quality ratio. A service consists out of a chain of virtualized network functions which can be deployed on a virtualized infrastructure. It is the role of the broker to find out which virtual service infrastructure provider is able to map the virtual network request at the highest price versus quality ratio. In return, the broker receives a commission. The virtual service infrastructure provider embeds the request on its virtualized infrastructure and receives a fee in return.
impact analysis	Each actor is able to generate value from the value exchanges. The virtual service infrastructure provider can increase its revenue by selecting the virtual requests that generate the most revenue while charging a premium for request that have a lower revenue per constrained resource according to a traditional static pricing approach.
value creation analysis	The end user is, in general, not so much interested in how the service is technically realized. The value added can be found in the role of the service provider and the virtual service infrastructure provider. The broker on the other hand is an intermediary who can optimize the interaction between the service provider and the virtual service infrastructure provider.

4.2.1.2 Dynamic Value Network and Tussle Analysis The second type of analysis, dynamic value network analysis indicates how the value network changes due to the introduction of the proposed solution. The roles in the value network are not impacted by adapting the pricing approach of the virtual service infrastructure provider. If successful, the dynamic pricing approach will be able to attract more valuable virtual network requests to the virtual service infrastructure provider that uses the approach. The total revenue and profit of that provider would as such increase while the revenue and profit of its competitors would decrease. We do not redraw the value network diagram as it would be the same as Figure 5. Tussles do not emerge, as the roles are not impacted.

4.3 ISP-oriented Content Delivery

This joint research activity, is a collaboration between University College of London (UCL) and iMinds, and is referred by UCL-iMinds-Cache. Content Distribution Networks (CDN) are distributed systems of servers spanning different geographic locations. The goal of a CDN is to serve content to end-users across the Internet. Current content delivery services operated by large CDN providers can exert enormous strain on Internet Service Provider (ISP) networks. This is mainly attributed to the fact that CDN providers control the placement of content in surrogate servers spanning different geographic locations, as well as the decision on where to serve client requests from (*i.e.,* server selection). In contrast, CDNs lack knowledge of the precise network topology and state in terms of traffic load. This may result in network performance degradation.

In this joint research activity, a scenario where ISPs deploy its own caching infrastructure is being investigated. The service, ISP oriented content delivery, is an extension to the traditional role of an ISP. To this end, as shown in Figure 6, The ISP provides both caching space and connectivity infrastructure for the distribution of content to end users.

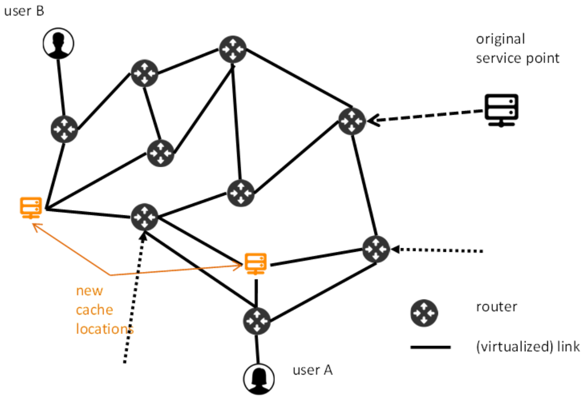


Figure 6: The ISP-oriented Cache Management

The objective of the work is to develop a model to quantify the benefits for an ISP of deploying their own caching infrastructure. These benefits are expressed as business indicators (BI). The BI considered in the ISP oriented content delivery scenario are: (1) the (long-term) investment cost for the ISP and (2) the Quality-of-Experience (QoE) for the end user and service provider.

To analyze the investment cost for the ISP, we determined the network setting to be considered. This concerns the physical topology to use, the configuration of the caching infrastructure, the traffic demand to consider, as well as the routing and cache management policies. Next, we have started collecting data to build a cost model for the different network elements. In this context those are IP/MPLS routers, transponders, photonic switching gear, fiber links, caching equipment and peering rates.

To analyze the effect on the QoE, the delay between requesting the content and consuming it will be considered. The deployment of caching infrastructure operated by the ISP will allow some requests to be directly served from within the network. This can, therefore, affect the delay in accessing content and a such the QoE as perceived by the end user.

To further analyze this scenario a boundary map, stakeholders' map, and risk analysis were conducted, as described below.

The **boundary map** that has been identified between this collaboration's members is illustrated in Figure 7. Any task that is out-of-scope, can become the starting point of either a new collaboration, or an extension of this collaboration for the future.

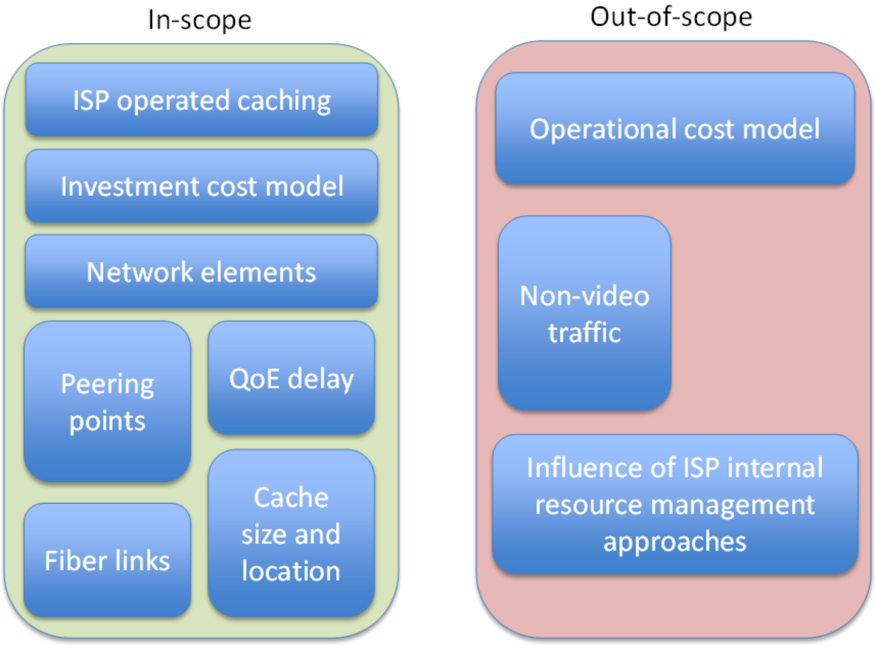


Figure 7: The Boundary Map of ISP-oriented Cache Management

Stakeholders Analysis and Stakeholders Map: The stakeholders list is summarized in Table 7, and the stakeholders map is illustrated in Figure 8. The goal is (a) to increase as much as possible the interest of every stakeholder, and (b) to change, if possible, negative to neutral, or even positive, the attitude of stakeholders with high influence.

Table 7: Stakeholders Analysis of the ISP-oriented Cache Management

Stakeholders	Interest	Influence	Attitude
Content Producer (CP)	Medium	Low	Neutral
Content Delivery Network (CDN)	High	Low	Negative
Internet Service Provider (ISP)	High	Medium	Positive
Regulator (REG)	Medium	Medium	Neutral
FLAMINGO partners (FP)	Medium	High	Positive

Table 8: Risks of the ISP-oriented Cache Management

Risk	PB_R	IMP	R	Priority	Possible Cause	Measure
Lack of reliable cost data	2	2	4	B1	Data is sensitive	Collect early and work with relative values
Unpredictability of the traffic dynamics	1	2	2	C1	Demand dynamics	Favor reactive approaches compared to proactive ones

Risk Analysis: The list of the potential risks that have been identified during the risk analysis phase are in Table 8. The risk analysis shows that the main risk that this collaboration is facing is, to not get reliable cost data from the infrastructure provider.

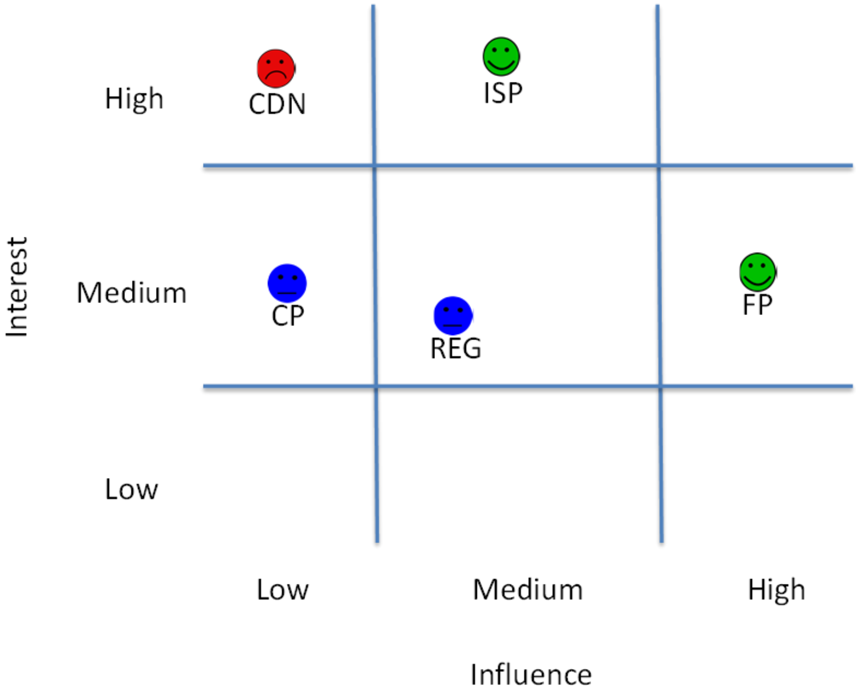


Figure 8: The Stakeholders Map of the ISP-oriented Cache Management

4.3.1 Validation of ISP oriented cache management scenario

To validate this scenario, three complementary methods are used:

1. Value network analysis: to understand how value is created today before the proposed solution is introduced
2. Dynamic value network analysis: to understand how value creation evolves over time due to the introduction of the proposed solution
3. Tussle analysis: to understand how to resolve conflicts between actors that may arise due to the introduction of the proposed solution

In these analyses we focus on the flows of goods, services and revenues (mostly ignoring knowledge and intangible benefits).

4.3.1.1 Value Network Analysis Value network analysis is used to understand how value is created today (before the proposed solution is introduced).

First, the value network diagram is drawn (Figure 9) and the value exchanges are described in Table 9.

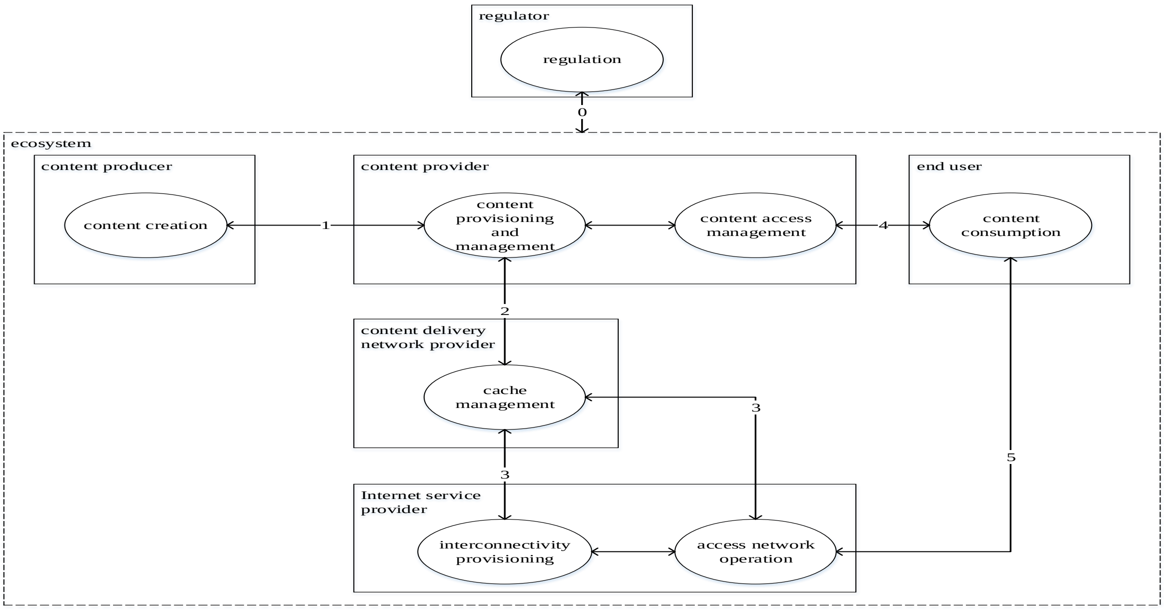


Figure 9: Value Network Diagram of a Video-on-demand Service Provider With the Traditional Split Between the Content Delivery Network Provider and the Internet Service Provider.

Table 9: The Value Exchanges That Take Place Between the Actors in the Value Network Diagram, the IDs Match With Those on Figure 9.

ID	actor 1 (start)	actor 2 (end)	description
0	regulator	*ecosystem*	supervision and regulation of the industry (intangible)
	ecosystem	regulator	information about the current market structure (intangible)
1	content producer	content provider	content
	content provider	content producer	license fee
2	content provider	content delivery network	monetary fee
	content delivery network	content provider	content distribution to the end user
3	content delivery network	internet service provider	monetary fee
	internet service provider	content delivery network	connectivity
4	content provider	end customer	a video-on-demand service
	end customer	content provider	monthly fee or fee based on usage
5	internet service provider	end customer	connectivity
	end customer	internet service provider	monthly subscription

Based on the value network diagram, we conduct three complementary analyses:

1. Exchange analysis: to understand the general pattern of value exchanges and check if there are any inefficient links as well as to check if there is no lack of reciprocity in the value exchanges.
2. Impact analysis: to understand if each actor is able to generate value from the value exchanges

3. Value creation analysis: focuses on the value created by the actor, it considers which value creation each output generates for the customer and how the actor benefits from this

The results of these analysis are summarized in Table 10 and indicate that their is room for improvement in the collaboration between the CDN and the ISP. To understand how the value network diagram could evolve over time, we conduct dynamic value network analysis.

Table 10: Conclusions of the Validation via Value Network Analysis.

type	result
exchange analysis	Content flows from the content producer via an intermediary content provider to the end user. In return, the end user pays a fee to the content provider for use of the service. The content provider pays its suppliers with that income: on the one hand, the content producer for the content and on the other, a content delivery network provider for the distribution of the content. Important for this scenario is that the content delivery network provider works together with an Internet service provider to bring the content to the end user. A potential lack of inefficiency exists in the interaction between the CDN and the ISP as they do not share all information (*e.g.,* content placement strategy, server selection strategy and network routing).
impact analysis	Each actor is able to generate value from the value exchanges. The quality of service could be potentially improved if the CDN and ISP exchange information about their strategies.
value creation analysis	For the end user, the only value creation activities are done by the content producer and the content provider who selects interesting content and provides additional information such as a summary, trailers, ratings and recommendations based on previously watched videos. The distribution of content is considered as waste according to the lean manufacturing principles but it is at the same time essential for the service.

4.3.1.2 Dynamic Value Network Analysis The second value network diagram (Figure 10 and Table 11) indicates how the value network changes due to the introduction of the proposed solution. The cache management role is now internalized by the internet service provider who is able to offer an integrated content delivery service to the content provider. The ISP now controls server selection, content placement as well as routing decisions. As such, it could optimize its service and develop a competitive advantage against competing CDNs. The ISP, however, also cannibalizes a revenue stream (from the CDN).

By internalizing the cache management role, the ISP is able to offer a value added service to the content provider and the value network diagram could evolve to the new situation:

1. cache management role is internalized by the ISP
2. actor CDN turns obsolete (its role is now performed by the ISP)
3. value exchange 2 and 3 of Figure 9 are consolidated to a single value exchange (value exchange 2)

The result is an increase in the importance of the ISP in the value network and a disappearance of the CDN. An alternative scenario is one in which the CDN internalizes the roles of the ISP. This could disrupt the business model of the ISP.

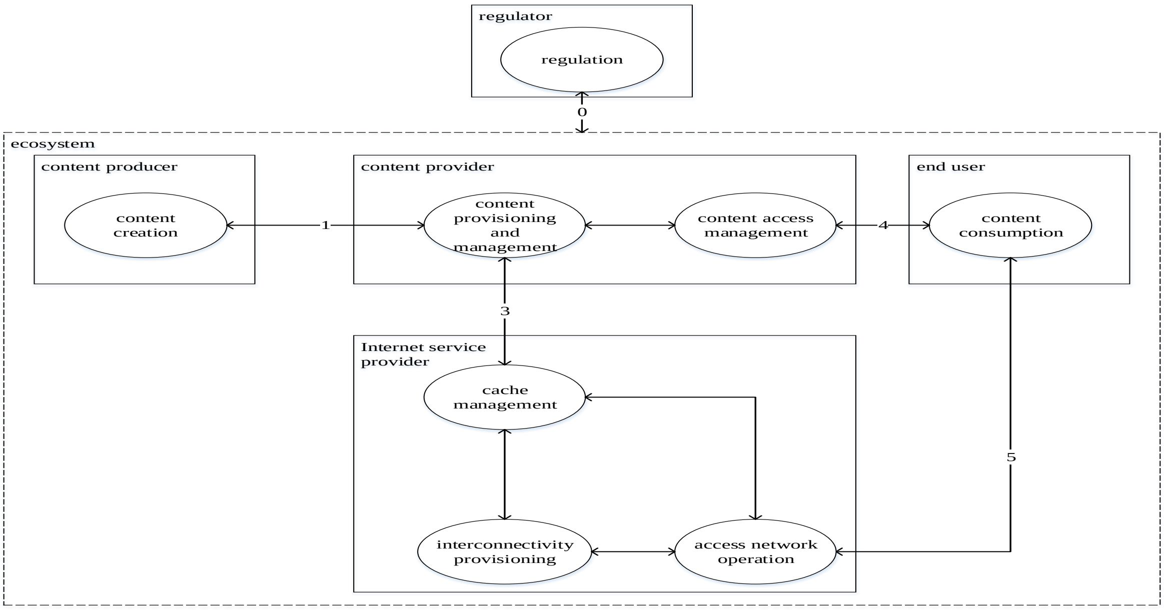


Figure 10: Value Network Diagram of a Video-on-demand Service Provider in which the Internet Service Provider Internalizes the Cache Management Role.

Table 11: The Value Exchanges That Take Place Between the Actors in the Value Network Diagram, the IDs Match With Those on Figure 9 and 10.

ID	actor 1 (start)	actor 2 (end)	description
0	regulator	*ecosystem*	supervision and regulation of the industry (intangible)
	ecosystem	regulator	information about the current market structure (intangible)
1	user	service provider	service fee
	service provider	user	services (*e.g.,* IP VPN)
2	service provider	broker	brokerage fee
	broker	service provider	best offer
3	broker	virtual service infrastructure provider	market knowledge and customer acquisition
	virtual service infrastructure provider	broker	information about the availability and price of resources
4	service provider	virtual service infrastructure provider	fee based on amount of virtualized resources used
	virtual service infrastructure provider	service provider	(virtualized resources)

The results of the exchange analysis, impact analysis and value creation analysis are summarized in Table 12. The ISP, by internalizing the cache management role, will become a competitor with the CDN. At the same time, the ISP remains a supplier for the CDN (network connectivity). As a reaction, the CDN may partner with another ISP or rollout its own network. The conflicts that may arise and the strategies to mitigate these are discussed in the next section.

Table 12: Conclusions of the Validation via Dynamic Value Network Analysis.

type	result
exchange analysis	The general pattern of value exchanges has not changed due to the introduction of the proposed solution. The content provider now directly pays a fee to the ISP for distributing the content to the end user. Content can now be distributed more efficiently as all information is internal to the ISP.
impact analysis	Each actor is able to generate value from the value exchanges. By internalizing the role of cache management, the ISP is able to reduce inefficiency in the transportation steps and increase his role in the value creation process of this value network.
value creation analysis	The distribution of media can be optimized as all information resides under a single roof (ISP). Of course, an alternative situation is possible in which the CDN internalizes the roles of the ISP and becomes a network operator itself.

4.3.1.3 Tussle Analysis As explained in the previous sections, each of the stakeholders involved have specific interests and incentives, as soon as the new mechanism of content delivery that is proposed in this scenario is deployed. Firstly the list below summarizes the major interests derived from above analysis:

1. End-users: End-users (people or organizations) request and often produce content (*e.g.,* pictures on Facebook) to be cached or prefetched. They also consumes the service (*e.g.,* video-on-demand). End-users may be willing to pay for the service, and therefore expect a certain QoE, otherwise they may switch to a competitor.

2. Internet Service Provider: Provides connectivity to the end user (both access network providers as well as inter-connectivity providers). With the introduction of the new scenario the ISP integrates the role of the content delivery network as it adds caching space to its network to distribute the content to the end users with high performance and availability. So earlier the role of ISP was just interconnectivity provisioning, but with this scenario ISPs, additionally, are responsible for cache management and content access management. Content access management now is part of their job as it is a legal obligation.

3. Content Delivery Network: CDNs are a distributed system of servers deployed in multiple data centers across the network. Content providers pay content delivery networks to deliver content to the end user with high performance and availability. Content delivery networks in turn pay ISPs for hosting its servers. They also do the cache management (server selection, content placement, content updating and cache location ownership), and content access management (including AAA-authentication, authorization, and accounting).

Therefore, based on mutually contradictory interests and incentives of the stakeholders, tussles as described below arise:

1. **Content Caching and Delivery:** The new scenario introduces tussles between the new role of ISP, that now can also be in control of content delivery, and the traditional CDN. The ISPs have a benefit in comparison to traditional CDNs as they own the transport infrastructure (routers and links) and they determine the routing decisions (*e.g.,* how traffic is distributed between the different paths to the end-user). By installing caches, the ISP need to invest more but then the ISP is also able to reduce the utilization rate of its nodes and links (if they use smart routing protocols), in turn delaying investments in these. The total cost for an ISP

should therefore be lower than the total cost of a CDN (who needs to pay the ISP for the use of its infrastructure).

Also, the network of the ISP may span different countries or geographic areas (as is the case with traditional CDNs). As the content provider may only have the rights to distribute the content in a limited number of countries, the placement of content outside of these locations may result in copyright violations. The ISP will therefore need a mechanism to determine if content can be cached in a location or not. Otherwise the rights of the content creator may be harmed. Such criteria are not taken into account when the cache placement is based on cost minimization, which may again lead to degradation of end-users' QoE.

2. **QoE vs. Cost of Content Delivery:** The ISP controls the connectivity infrastructure (routing of data) while the CDN controls server selection and content placement. The integration of both roles by the ISP (ISP+CDN scenario) allows full control (content placement, server selection and routing). The localization of content by the CDN may affect the strain on the network of the ISP. The ISP may as such change its routing algorithm to distribute traffic to nodes and links with lower utilization (but possibly higher delay). This may reduce the QoE for the user. That means that ISP may as such have an incentive to treat traffic from in a sub-optimal way (cost optimization), which conflicts with the goal end user (who needs good QoE). Similarly the CDN may choose to change its content placement strategy as a reaction to the lower QoE, which may possibly congest other ISP nodes and links, etc.

4.4 Legal and Ethical Facets of Data Sharing

The scenario and the collaboration described in this section is born in the context of the Dagstuhl seminar “Ethics in Data Sharing” [12], which took place in January 26th – January 31st 2014. The seminar, which accounted among the organizers also A. Pras (UT), brought together experts from the legal, ethical and technological aspects of data sharing and data consuming, and it started fruitful discussion about the pro and cons of data sharing and the options and needs of the various involved parties. A follow-up effort from the Dagsthul seminar is the collaboration between SURFnet BV (the Dutch National Research and Education Network), University of Twente, University of Amsterdam, Tilburg University and University of Zurich, and is referred as UT-UZH-Ethics.

Scientists often face the need for data on which the investigations and validation of approaches is based. A chief example of such data is, for the research conducted in this Network of Excellence, various flavors of network data. However, such data is not always directly accessible to researcher. For example, not every researcher has the possibility, equipment or is allowed to measure network data on his/her institution infrastructure; or the type of research calls for a larger measurements than an institution network; or again, the type of data needed for the research has to be collected with the permission of the end-users.

A pivotal role in data sharing and acquisition is played by ISPs and Network Operators (NO). However, sharing network data with third parties, although for academic research purposes, carries intrinsic ethical and legal concerns. This is because, although data is often aggregated, in some case they may still contain user-identifiable information, or the type of data is by law considered personal information.

The goal of this collaboration is to establish an ethical guideline for facilitating data sharing between operators and researcher. Such a guideline will provide a step forward from the current practice of data sharing, which is ad-hoc and essentially based on the idea of sharing with “trusted parties”,*i.e.,* with researcher we know and we can reasonably assume will conduct proper research. However, the current situation is far from optimal from several aspects. A strategy of establishing a common knowledge between the data provider and the data consumer is missing, the ethical aspects are left to the separate consideration of data provider and data consumer, Non-disclosure Agreements (NDA) are often too generic, and reproducibility of results by other researcher can become difficult.

The partners involved in this scenario are currently working on several aspect of the data sharing problem. From the one side, they are working on the creation of a policy for facilitating data sharing between operators and researcher. SURFnet is strongly leading this task and will implement the policy in its data sharing procedure. On the other hand, the partners are working towards educational measures to raise researcher awareness to the problem of consciously framing their research scope, structure their data requirements and identify ethical concerns.

A pioneer in data sharing: the case of SURFnet: As the National Research and Education Network in the Netherlands, SURFnet strives to be at the forefront of internet working. Part of its mission is to advance the state of the art in networking through facilitating academic research on the network itself. This research can only be effective if researchers in networking and network security have access to data on and from live large scale networks such as the SURFnet7 network.

For years, SURFnet has shared operational data with researchers to aid them in advancing their theories and testing and applying their algorithms on real network data. But they gradually realised that its data sharing practices have limits. SURFnet works with targeted NDAs that strictly limit use of the shared data, but that importantly requires researchers to destroy data after completing the research, this clashes with academic values of retaining any datasets used for a particular piece of research. In addition to this, data sharing is limited to researchers who are known and trusted personally by SURFnet *e.g.,* other academic researchers from reproducing research done by people they've worked with in the past if they are not in SURFnet's inner circle.

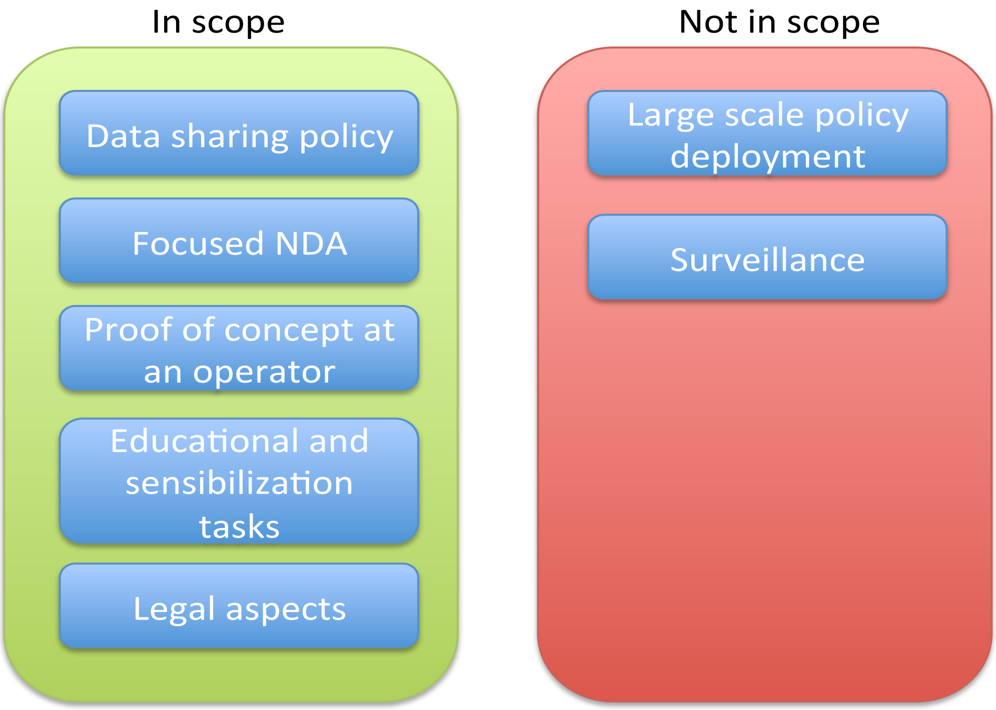

In scope
Data sharing policy
Focused NDA
Proof of concept at an operator
Educational and sensibilization tasks
Legal aspects
Not in scope
Large scale policy deployment
Surveillance

Figure 11: The Boundary Map of Legal and Ethical Facets of Data Sharing

For these reasons, SURFnet set out to define a new data sharing policy. The goal has been to create a more inclusive policy that helps SURFnet to share more data with more researchers more often. Obviously, SURFnet's data sharing practices have to comply with legal requirements from

Dutch law and the EU Data Protection Directive (soon to be followed up by the Data Protection Regulation). But SURFnet also wants to go beyond legal requirements and include ethics in its policy. In SURFnet's opinion this is an essential dimension to research on network data, especially where such data contains personally identifiable information and thus impacts the privacy of its users and connected institutions.

The new policy can be downloaded via `https://tnc15.terena.org/getfile/2829`.

The **boundary map** in Figure 11 describes the activities that will be carried in this scenario, and the ones that are out of scope at this point in time. The legal aspects of the scenario will be taken into consideration at a further moment in time.

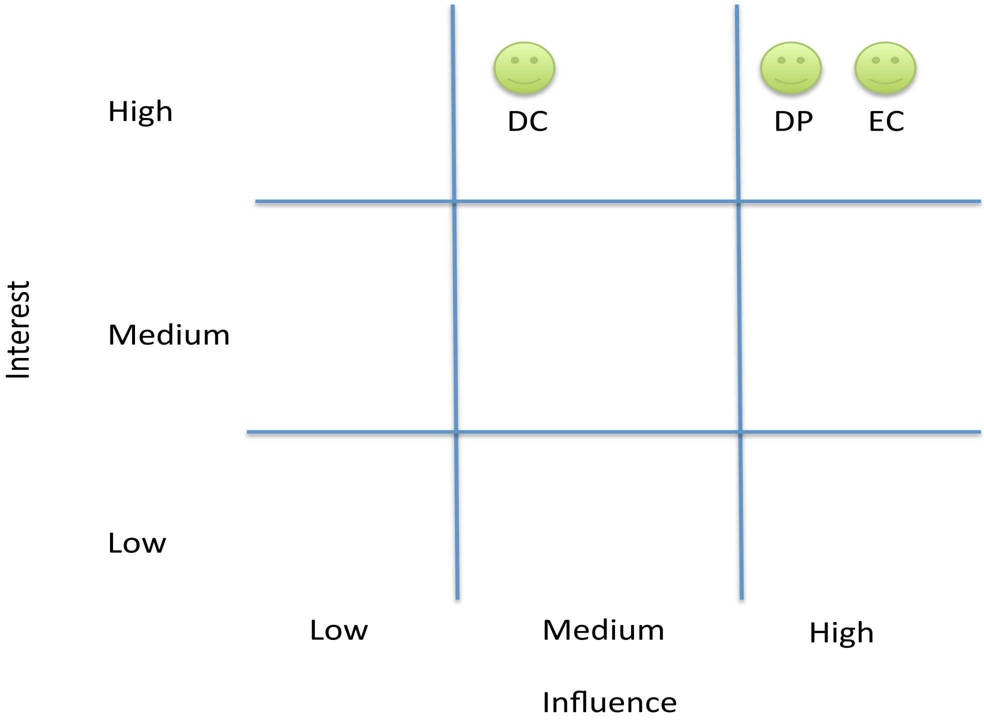


Figure 12: The Stakeholders Analysis of Legal and Ethical Facets of Data Sharing

Table 13: The Stakeholders Analysis of Legal and Ethical Facets of Data Sharing

Stakeholders	Interest	Influence	Attitude
Data provider/Network Operator (DP)	High	High	Positive
Data Consumer/Researcher (DC)	High	Medium	Positive
Ethical Committee (EC)	High	High	Positive

Stakeholders Analysis and Stakeholders Map: Table 13 summarizes the stakeholder analysis for the scenario, while Figure 12 depicts in graphical form the stakeholder analysis.

Risk Analysis: The list of potential risks for the considered scenario is listed in Table 14. The identified risks concern the possible side effects of the performed research in terms of ethical concerns. This is considered the risk with the highest impact, and the motivating one for the development of this scenario. The remaining risks cover issues such as how the results of the research can be disseminated and how the data should be stored and preserved (if necessary). Finally, the lastly

Table 14: Risks of the Resource Management of Legal and Ethical Facets of Data Sharing

Risk	PB_R	IMP	R	Priority	Possible Cause	Measure
Ethical concerns	3	3	9	A1	Research not properly framed	Policy and guidelines
Un-responsible disclosure	1	3	3	B2	Lack of communication; mis-aligned expectations; lack of carefulness	Policy and guidelines
Issues with data curation	1	2	2	C1	Lack of resources; lack of carefulness	Policy and guidelines
Lack of timeliness	2	1	2	C2	Lack of resources	No solution

identified risk cover the interaction between the data consumer and the data provider, in case the data consumer need data with urgency (e.g., to capture a transitory phenomenon on the Internet).

4.4.1 Validation of Legal and Ethical Facets of Data Sharing

The following section discusses the validation techniques in the context of the scenario Validation of Legal and Ethical Facets of Data Sharing.

4.4.1.1 Value Network Analysis Value network analysis is used to understand how value is created today (before the proposed solution is introduced). In this case the proposed change is an update of an available policy.

First, the value network diagram is drawn (Figure 13) and the value exchanges are described in (Table 15).

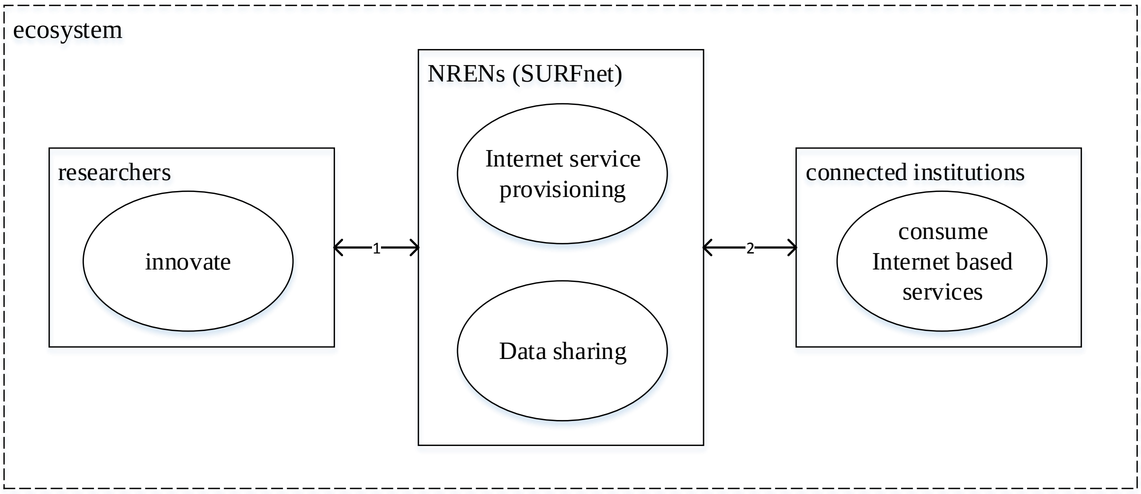


Figure 13: Value Network Diagram for the Ethical Facets of Data Sharing Scenario.

SURFnet is a nonprofit organisation that is publicly funded. A large proportion of its funding is

Table 15: The value exchanges that take place between the actors in the value network diagram, the IDs match with those on Figure 13.

ID	actor 1 (start)	actor 2 (end)	description
1	researchers	NRENs (SURFnet)	research results that benefit SURFnet in an operational sense
	NRENs (SURFnet)	researchers	sharing of data
2	NRENs (SURFnet)	connected institutions	Internet services
	connected institutions	NRENs (SURFnet)	service fee

through fees paid by users of the network (higher education and research institutes). Showcasing how SURFnet shares data with researchers within our own community and in the broader academic world demonstrates that its value to the community extends beyond that of a pure service provider. This helps demonstrate its relevance and secures future funding. The same is true for the other income stream through public funding that comes from the Dutch government.

Second, research results dealing with computer networking and network security benefit SURFnet in an operational sense. It helps SURFnet stay ahead of the curve in terms of networking and protecting its network against attacks. SURFnet has unique problems as an NREN in the sense that the bandwidth it has available is huge, which brings with it particular challenges that can only be tackled by applying research results in operational practice soon after they leave the academic realm. Data sharing helps SURFnet foster relationships with researchers and helps it stay up-to-date with novel developments. Applying novel research results in its operational practice in itself is a unique proposition that in turn it can use to demonstrate its relevance to connected institutions (’customers’), as discussed in the previous point.

Third parties that benefit from its data sharing policy will be:

- Researchers

For academic researchers in the networking and network security space, it is difficult to get access to ”ground truth” (data originating in a real, large scale, operational network). Commercial network providers are reluctant to share data with researchers. Organisations like SURFnet, however, have no commercial considerations and thus are prime sources for researchers for this kind of data that is vital to validating their research.

- SURFnet’s connected institutions (’customers’)

They benefit from this policy due to secondary effects. First, if SURFnet applies the results of research stemming from shared data in the operational context, this benefits the connected institutions. Second, if it allows SURFnet to demonstrate its relevance to society at large, this in turn can help secure funding which will ultimately benefit the connected institutions because they benefit from the innovations SURFnet are able to realise with this funding.

- Society at large

As a publicly funded body, SURFnet has a responsibility to society at large. If its sharing data can help realise breakthroughs in networking and network security, this will benefit society in the Netherlands and the European Union.

4.4.1.2 Dynamic Value Network Analysis and Tussle Analysis The second type of analysis, dynamic value network analysis indicates how the value network changes due to the introduction of the proposed solution. The roles in the value network are not impacted by adapting the data sharing policy. When successful, the new data sharing policy can result in more and more efficient usage of data by researchers and a generally higher quality of publications (as the results become repeatable). As the roles do not change, tussles do not emerge.

5 Legal and Regulative Considerations

Network and service management have been traditionally devoted to develop mechanisms to deliver end-to-end QoS in the Internet.

In the field of network and service management sharing, transferring, storage of data forms a crucial part for network operation, administration, maintenance, and configuration of resources. This however, entails various legal and regulative constraints and requirements, that should be considered while performing any of these tasks. The following section discusses two major aspects of such constraints.

5.1 Schengen Routing

Deliverable D7.2 discussed Schengen Routing at a glance, including details about the Schengen Agreement, Reasons for Schengen Routing and ideas about the applicability. This paragraph summarizes Schengen Routing issues that arise and gives details about a compliance analysis performed in Y3.

5.1.1 Schengen Routing in Practice

Discussing Schengen Routing implicitly raises questions about the applicability of such a strong routing mechanism for the Schengen Area. Having Schengen countries in mind, it becomes clear that some countries, (*e.g.,* Iceland) are only reachable via a non-Schengen country. This brings up the question how can these countries connect to the Schengen Routing area? Do we need new physically separated mediums for Schengen compliant routing? If this is necessary, who is willing to spend money for this physical medium? On the other hand there exist Schengen countries that are directly connected to each other (on physical and Internet infrastructure level), but the Internet service provider (ISP) is routing packets via a non-Schengen country, because it's cheaper.

Possible solutions for implementing Schengen Routing are not yet available. Until there is pressure from the governments or law restriction to use such kind of routing mechanisms nothing will change in order to implement Schengen Routing. Even if law is released to regulate Schengen Routing there arises the question: How to prove that traffic is routed the right way? This would infer that ISPs open their routing tables at least for the jurisdictions and apply a kind of traceability for already routed traffic. Taking these thoughts remind on a surveillance state, which should not be the goal of a EU country [30].

There exist already some ideas to overcome these issues and to implement a Schengen Routing or a kind of Schengen network without changing the equipment of ISPs and peering providers. On of the ideas is to provide a Schengen VPN that handles all connection from and to Schengen partners. The advantage of this is that only relevant partners need to change their configuration in their equipment [54]. This can be at the same time an issue, since the responsible for the Schengen compliance is the company or the user itself and no guarantee from the regulator is given or can be achieved by court. In addition, there exists another idea regarding a kind of Schengen firewall, that drops all connections and packets originating from countries not in the Schengen Area. The drawback of this solution is how to determine the correct origin of packets and connections. This is only possible by geolocation approaches that reach a high accuracy, *e.g.,* [36].

To give an idea about the Schengen compliance of the current network in Europe the following section summarizes the work done by UZH regarding Schengen Routing Compliance Analysis [17]. The details of the open source code of this tool has been added to Deliverable D1.3

5.1.2 Schengen Routing Compliance Analysis

The idea of Schengen Routing was proposed as a possible amendment to protect communication across Europe after the affair involving Edward Snowden and the National Security Agency (NSA) demonstrated that wiretapping large amounts of Internet traffic was applied on a regular bases by various intelligence agencies. These actions are clearly violations of privacy laws [39]. The general term Schengen refers to a treaty targeted at reducing border controls and implementing a harmonized legal framework. The Schengen Area consists of all countries who signed this treaty which is not the same as the European Union (*e.g.,* United Kingdom is part of EU, but not part of Schengen) [23]. Schengen Routing therefore, refers to a routing of Internet traffic between hosts located in the Schengen Area, not leaving the borders of the countries part of the Schengen treaty. The advantages of such a strict routing is that traffic not leaving the Schengen Area is more difficult to be wiretapped by non-Schengen intelligence agencies.

Nevertheless, the implementation of Schengen Routing infers the reconfiguration of routing tables and renegotiation of all agreements regarding the transit and peering points. The required effort to achieve this routing behavior is highly dependent on the current routing. If this complies already with Schengen routing the changes might be only slightly different. The paper [17] measured the Schengen Routing compliance through active measurements by analyzing TCP, ICMP and UDP traffic in oder to answer the following question: What is the Schengen routing compliance or non-compliance percentage of current traffic among Schengen countries based on the observation of active measurements?

The authors used RIPE Atlas [57]-a large-scale measurement platform-to perform a large number of traceroute measurements from various Autonomous Sysytems (AS) within the Schengen Area to a well-known host in Switzerland (Switzerland is part of the Schengen Area, but not part of the EU). These measurements take into account all IP addresses derived from the traceroute and combined with GeoLite [42] database. Using this database the approach obtained for each IP address the related AS, countries and, thus, places in- or outside Schengen.

All traceroute measurements - executed using the RIPE Atlas measurement infrastructure - allowed to specify an AS number as a measurement source and to select a suitable probe with an IP address within the AS automatically. The target IP address of all traceroute measurements was a machine located within Schengen at the premises of University of Zurich, Switzerland (within AS 559). Measurement requests were submitted for all 9967 ASes determined for the ICMP, TCP, and UDP protocol in turn. For each protocol, RIPE Atlas performed three traceroute measurements automatically. These measurements were limited to one target host and three traceroute measurements per protocol because the number of measurements that can be performed on RIPE Atlas is limited by the credit earned by the respective volunteer.

Original	Not	No Probes			Failed/Error			Outside Schengen			Remaining		
	Covered	T	U	I	T	U	I	T	U	I	T	U	I
9967	8661	44	47	50	25	24	25	105	104	106	1132	1131	1125

Figure 14: Number of ASes After Results Processing [17]

All results obtained from these measurements were processed in several steps (see Figure 14).

1. Measurement requests were submitted for 9967 ASes, out of which 8661 ASes were not covered by RIPE Atlas. They could, therefore, not be taken into consideration.

2. RIPE Atlas could not find suitable probing devices in all ASes covered. These ASes could not be taken into consideration.

3. Some measurements failed or produced invalid results (*e.g.,* error messages rather than measurement data) and were excluded.

4. ASes may have IP address ranges advertised in several countries, especially in ASes with large number of IP address subnets. Because RIPE Atlas chooses IP addresses within the AS at its discretion, an IP address outside the Schengen Area may be selected. Measurements executed from probes having IP addresses located outside the Schengen Area were excluded.

After this results processing, 1132 TCP, 1131 UDP, and 1125 ICMP valid measurements remained for an evaluation. The unprocessed traceroute as obtained from RIPE Atlas measurements have been made publically available [18].

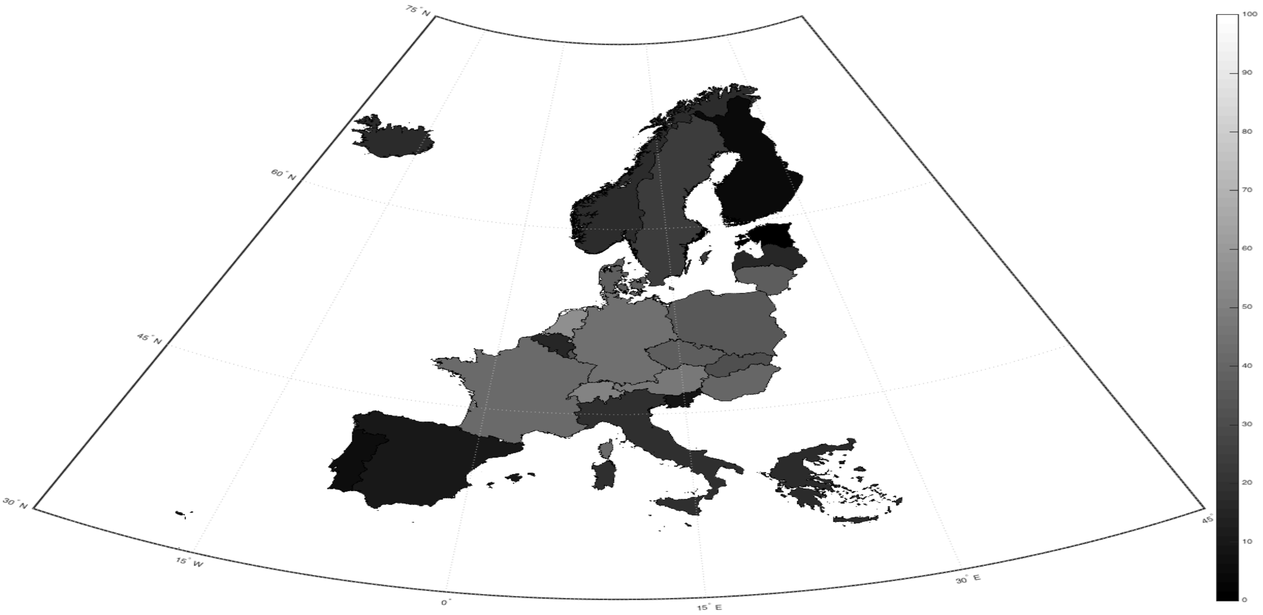


Figure 15: Schengen Routing compliance levels [17]

These obtained results were classified with respect to Schengen routing compliance as follows:

1. Measurements containing at least one IP address located outside the Schengen Area were classified as ”Non-compliant” (NC).

2. Measurements containing only IP addresses inside the Schengen Area were classified as ”Compliant” (C).

3. Measurements containing IP addresses for which no country information was available or for which traceroute did not produce an IP address were classified as ”Unknown” (U), if all other IP addresses were located within Schengen and ”Non-Compliant” otherwise.

To determine the geographic location of an IP address, Maxmind’s GeoLite database [43] was used, the same database as was used for the AS selection process. Figure 15 provides an overview of those results found. Light gray shades represent higher Schengen routing compliance levels while dark gray shades stand for lower compliance levels.

The results of the measurements showed that for 3388 TCP, UDP and ICMP traceroutes via RIPE Atlas probes located in over 1100 ASes in the Schengen Area compliance levels vary substantially among countries and range from 0% (TCP), 0% (UDP) and 0% (ICMP) in the case of Malta to 80% (TCP), 75% (UDP), and 80% (ICMP) in the case of Liechtenstein. Following this, the overall compliance levels range from 34.5% (TCP) to 37.4% (UDP) and 39.7% (ICMP). Therefore, the paper concludes that in no Schengen country a Schengen Routing compliance is achieved.
This fact is contradicting the claim that Schengen routing was already in place, as it has been stated by the Association of the German Internet Industry [13]. Next to these measurements, a tool termed chkroute [18] has been developed, allowing end-users to find out whether specific routes are Schengen-compliant.

5.2 Network Neutrality

Net Neutrality (NN) is a principle by which all the content on the Internet is treated equally, irrespective of its content, or source or destination of data. It is a complex issue that has generated several discussions across the globe. The outcome of this debate will shape how the future Internet will look like. The debate exists mainly due to the varied interest of the involved stakeholders, namely the ISPs, Over-the-Top (OTT) players, regulators, and end-users. The question under discussion is whether the ISPs should be allowed to prioritize or block network traffic from OTTs or other service providers. The reason behind this is that it leads to the possibility of discriminating or charging differentially on the basis of user, content, site, platform, application, type of attached equipment, or mode of communication. Over the years, the position of ISPs has become one of an essential gatekeeper, which puts them in control of the information flow on the web. With the rise of OTT applications and providers, a significant amount of Internet traffic is no longer fully controlled by the ISPs. The increase in Internet traffic that these OTT applications bring, demands for upgrades to the network, but does not return a direct revenue for the ISPs. This issue lies at the heart of the current debate about net neutrality and raises important questions about if and how it should be implemented by law [38].

When studying the current regulation about NN, significant differences can be noted worldwide [40]. In the US, no specific rules are in place yet, while certain countries (*e.g.,* the Netherlands) in Europe clearly specified earlier non-blocking rules [19], [3]. Also, as per the decision made by EU Commission on October 27, 2015, the rules enshrine the principle of net neutrality into EU law: no blocking or throttling of online content, applications and services. It means that there will be truly common EU-wide internet rules, contributing to a single market and reversing current fragmentation [22], [6]. Based on these regulations, as well as specific cases where operators breached (or tried to breach) the concept of net neutrality, different net neutrality and non-net neutrality scenarios could be defined [64]:

- **Basic Net Neutrality**: this is the current network with a NN obligation. The ISP will not upgrade its network, which results in congestion problems when applications require more bandwidth over time.
- **Network upgrade**: the ISP invests in upgrading its network upgrade to get rid of congestion.
- **Dominant ISP**: by installing Deep Packet Inspection (DPI) equipment, the ISP can give its customers all the bandwidth they need and leave only the remainder to the OTT customers, resulting in massive congestion for the latter. This scenario is based on the case of Deutsche Telekom, who decided to put data caps on all traffic, but exempt its own services from counting toward this data cap.

- **Service access fee**: the ISP installs DPI equipment to identify OTT customers and charge them an extra fee. This is similar to KPN's plans to charge its customers for the use of Skype and WhatsApp.
- **Preferential distribution**: the ISP uses half of his bandwidth capacity to create a fast lane on his network. Customers that are willing to pay the preferential distribution fee, receive access to this fast lane. Normal customers will suffer more congestion. This scenario can be compared to AT&T's aspirations to give preferential treatment to Google's data at a certain price.

To assess the effect of these specific scenarios on the access market, Van der Wee et al. [64] propose a game theoretic approach [60] on a fictitious market in which one ISP and one OTT compete for Video on Demand (VOD) customers. This game theoretic approach is combined with a market model that determines how the market gets shared among the players. The different calculation steps are shown in Figure 16.

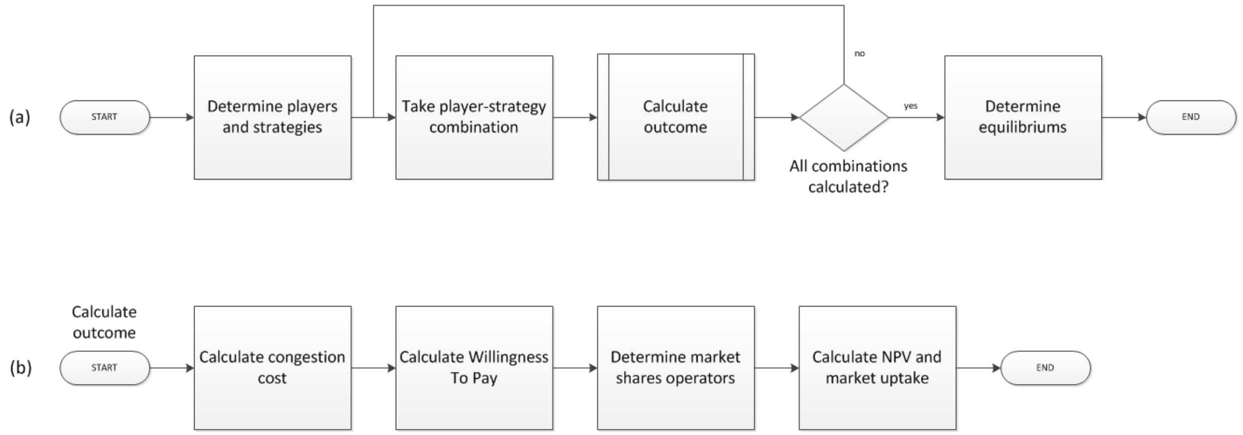
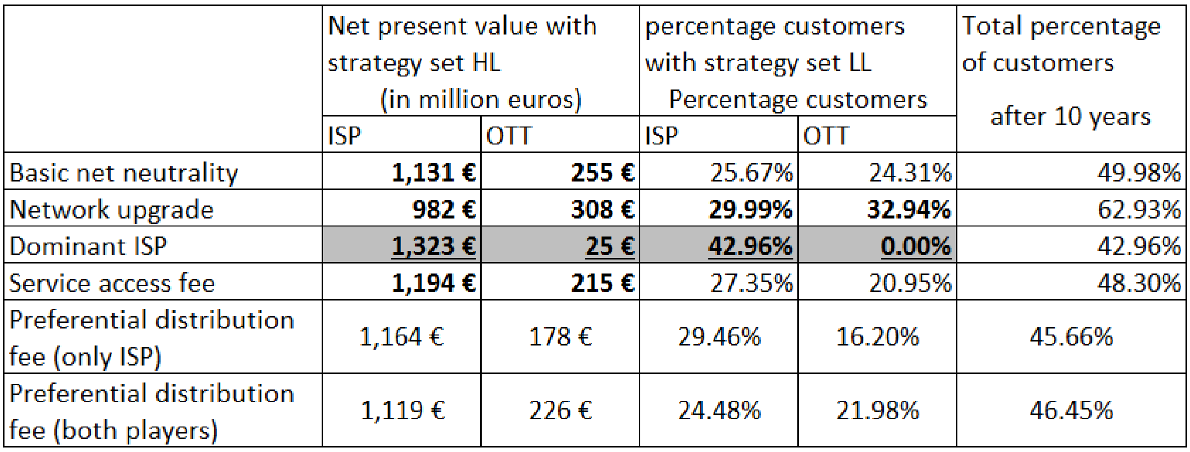

(a)
START
Determine players and strategies
Take player-strategy combination
Calculate outcome
no
yes
All combinations calculated?
Determine equilibriums
END
Calculate outcome
(b)
START
Calculate congestion cost
Calculate Willingness To Pay
Determine market shares operators
Calculate NPV and market uptake
END

Figure 16: Overview of the Game-theoretic Model

As shown in Figure 16(a), each scenario requires to determine the players (one ISP, one OTT in the case of this paper) and their respective strategies (both players can choose to charge a high or a low price). For each combination of strategies, the outcome for the market should be determined (Figure 16(b)), both in terms of Net Present Value (NPV) as well as market uptake. A first step in this process consists of calculating the congestion cost, which is modeled as an artificial price increase that reflects the lower degree of customer satisfaction. By comparing the normal VOD price to the "actual" VOD price, which includes the congestion cost, each customer's Willingness to Pay can be calculated. The pre-final step then includes calculating the market shares per player, using the market model [60]. A final step in the calculations for each strategy combination, is determining the outcome per player by calculating its NPV or actual market uptake. These parameters were chosen to represent the operators' perspective (NPV, i.e. maximizing profit) and the regulator's perspective (market uptake, i.e. maximizing the number of satisfied customers).

After each combination of strategies has been evaluated, game theory can be used to determine the equilibriums of the game, which indicate the preferred strategies of both players in a competitive setting. Both Nash and Pareto equilibriums are calculated. A Nash equilibrium is defined as a situation in which no player can gain by unilaterally changing its strategy. A change to a different strategy combination making at least one player better off without making another actor worse off is called a Pareto improvement. When no Pareto improvements can be made from a given strategy set, the set is Pareto optimal or efficient. A comparison of all scenarios is shown in the game matrix (Figure 17). The Nash equilibrium for both the NPV and the amount of customers are shown in grey, while the Pareto equilibriums are represented in bold. The high prices are indicated by the letter 'H', the low prices by 'L'; the first letter always refers to the ISP, the second to the OTT's strategy undertaken in each scenario.



	Net present value with strategy set HL (in million euros)		percentage customers with strategy set LL Percentage customers		Total percentage of customers after 10 years
	ISP	OTT	ISP	OTT	
Basic net neutrality	**1,131 €**	**255 €**	25.67%	24.31%	49.98%
Network upgrade	**982 €**	**308 €**	**29.99%**	**32.94%**	62.93%
Dominant ISP	**1,323 €**	**25 €**	**42.96%**	**0.00%**	42.96%
Service access fee	**1,194 €**	**215 €**	27.35%	20.95%	48.30%
Preferential distribution fee (only ISP)	1,164 €	178 €	29.46%	16.20%	45.66%
Preferential distribution fee (both players)	1,119 €	226 €	24.48%	21.98%	46.45%

Figure 17: Nash and Pareto Equilibriums Results for All Scenarios

If the ISP is left the choice of scenario, he will opt to dominate the market by giving preferential treatment to its own services, as the cost for DPI equipment is negligible to the additional gain in revenues from the VOD service. The dominance of the ISP will result in the OTT leaving the market. This is by far the worst scenario in the eyes of the regulator, who wants to preserve competition. If DPI equipment is prohibited, the ISP will not upgrade its network if he wants to maximize its profits instead of its number of customers. The results for the network upgrade scenario show that the ISP can easily pay the investment with its Internet revenues. This outcome invalidates the ISPs argument that they can no longer keep up with the investment costs caused by increasing bandwidth demands. On the other hand, the OTTs do provide about 50% of all data on the network, giving strength to the ISPs argument that the OTTs are part of the congestion problem. It should be noted that the results given above are only valid for the specific, fictitious market under study, which is described in detail in the paper of reference [64]. The model is generically applicable, but input values should be specified depending on the market setting, financial and economic context.

5.3 Legal and Ethical Facets of Data Sharing

The sharing of data, typically encompassing measured data in terms of traces, network access, usage, or even content, refers to a common practice of offering these data to other individuals or organizations for the purpose of an investigation of these.

Such investigations may address data structural facets, content-related details and trends, performance lines, or even individual events. Thus, data sharing between persons or organizations involves a clear privacy concern, which is typically encoded into country- or region-specific laws. However, besides those legal considerations data sharing under the research umbrella bears an additional facet of importance: Under the assumption that data collection and analysis are performed from a single organization, if a data analysis has resulted in a certain result *R* and if the methodology applied follows the approach *M*, a second party needs to have the scientific means to prove or not *R* by either applying the same methodology *M* in a new evaluation or by applying a different methodology *M'*. Thus, the original data needs to be available for such a verification.

Transparency and openness - in data and methodology - is a foundational principle of research. Thus, for networking research the access to data obtained from the operations of a network or parts of the Internet are not only ”interesting” from a research perspective (say for performance evaluations, optimizations of operations, or investigations on newly deployed services and functionality) they are crucial for security incident detection, security-related traffic analysis, and other operations-related aspects. Therefore, the public demand for an open clarification as well as justification of certain operational steps can be understood.

However, the privacy-related concerns as outlined earlier will apply in this case at the same priority and importance. This is due to the fact that network traffic data contains information of individual users, humans, and organizations, such as IP addresses, port numbers for applications, and timing information of the occurrence of respective packets with such content. This situation as such is not new, as research and marketing faced those questions in the past in different fields as well. In case of medical research, a possible quantification of the success rate for a certain medicine’s treatment can only be evaluated in its final stage, when humans participate. As human beings are individuals with many unique characteristics, such a medical quantification needs to ensure this human’s privacy, while being general enough to publish a useful success rate constrained be well-defined and -determined restrictions or assumptions. Such broad information range, though being aggregated to a certain extend, outlines the thin line between general interest and personal protection. In case of marketing and loyalty cards the same applies to the consumer’s behavior in a shopping mall, when does he stop at which location and what ends up in his cart compared to other decision taken. While the potential interest of the mall in such behavioral data is obvious (amongst others to optimize their selling), the interest of the consumer is very clear, too, to avoid a derivation of his (individual) shopping behavior as this belongs to his private decisions.

Thus, in general data sharing between parties, under the assumption of an analysis to be performed with clearly defined goals and targets, raises those tensions. As additionally multiple regional or country-specific laws and regulations exist, which define, restrict, prevent the data collection itself, others exist, which define how to store, handle, and maintain such collected data. While further regulations may exist on which analysis methodologies are allowed to be used or which methods have to be applied to result in comparable outcomes of investigations. Therefore, the range of openness and constraints of the legal side is complemented by the freedom of methodology and its application.

In that dedicated situation of counter-rotating demands of law and research, the public (and the individual as a representative of it) and privacy, and companies vs. consumers, the special case of data sharing arises for ISPs and their needs to operate a stable, efficient, and secured network. Due to the legal variability and too broad perspective, if addressed world-wide, which is even true on a European level, the relevance of ethics has been constituted as a valid and common basis for determining the does and don’ts in data sharing of networking traces [12].

Since FLAMINGO participated in that seminar, the ethics model developed is shown in Figure 16 and resulted in the cross-over of (a) stages, (b) roles, and (c) context to determine (d) ethical value. This model strives to examine ethical values in all stages of research, especially during the definition, the design, the data collection, the data storage, the analysis, the verifiability, the dissemination, and the curation phases. Thus, for each of those stages the role(s) of all actors is required to be determined explicitly and their context has to be defined in the closest possible detail. In turn, the ethical value of such analysis outcomes, findings, or results has to be specified on the data to be exchanged and analyzed.

While this approach was applied to National Research and Education Networks (NREN) by FLAMINGO in [16], its next step revealed that respective data sharing policies for the case of the Dutch NREN SURFnet can be developed [4], which happened in collaboration of Dagstuhl Seminar participants,

Table 16: A Model for Ethics in Data Sharing [16]

	The Pirate Bay Blockade Effectiveness	Internet Census 2012
Concept and Design	Design and implementation of the tools and experiments *Values: accountability, objectivity, fairness*	Port scanning with the use of middle nodes, changed over time to minimize bandwidth usage/ load, did not change passwords, did not erase disks, removed after reboot - minimized impact *Values: Non-maleficence, transparency, fairness, security, privacy, truth*
Data collection	Running the measurements, participating in the data exchanging process *Values: Truth, safety, objectivity, beneficence, transparency of tool, however not for the user*	Collection of data without harming the target system, creating bots, installed software, invasion of open systems *Values: as above*
Data storage	On an encrypted local disk *Values: Privacy, reputation, truth, accountability*	Most efficient way (technology perspective) *Values: Efficiency and effectiveness*
Data Analysis	Geo Location full data; IP to AS mapping through a third party service, aggregation and statistical analysis *Values: Objectivity, truth, accountability*	Hilbert curves, geographical distribution, standard analysis *Values: Objectivity*
Data Verifiability	Manual verification with random sampling *Values: Weighing of effectiveness and efficiency against full data analysis*	None
Dissemination	Publications, outcome in a technical report (public after review by lawyers) *Values: Truth, accountability*	Data on Web site, interpretation/results and full data set online *Values: Secrecy, awareness of security*
Data Curation	Stored offline; shared only aggregated data. *Values: accountability, privacy, truth*	Data shared publicly without warning *Values: None*

FLAMINGO Members, and SURFnet experts. In addition, FLAMINGO partners have closer research and operational contacts to SWITCH, the Swiss NREN, and performed an interview on the FLAMINGO's scenario of Legals and Ethical Facets of Data Sharing" (see. Appendix 12.3).

While all details of that SURFnet policy on data sharing can be found in [4], it has to be noted that this document states the current draft version. [4] states that "the main purpose of this information [traffic flow information] is to ensure the proper operation of the network and to protect customers and users of the network." In addition, the SWITCH interview revealed that for exactly the same technical and operational reasons as provided within [4], SWITCH falls under the Swiss law of telecommunication (Fernmeldegesetz) [61]([15]). This lead in their case to the decision to apply a very simple, but clear rule of not applying any options for data sharing of their network traffic traces. Obviously, the legal uncertainties in case of data sharing for research purposes (this case is not mentioned explicitly in [4]) have overruled any applicability of ethical guidelines.

In summary, legal and ethical facets of data sharing are diverse, contradictory, and not generally applicable. The reason for this unharmonized situation (here only shown in case of The Netherlands - member of the European Union - and Switzerland - part of Europe) can be clearly found in the differences of their legal system, special laws and acts, and in different prioritization and interpretations of those. As such, a country- or region-specific perspective of ethics in and for data sharing still has to be followed to enable an open, transparent, and at the same time privacy-preserving evaluation of Internet traffic.

5.4 Cloud Adoption in an Organization

Many of the legal issues are not unique to Cloud Computing (CC). They have been previously discussed in IT outsourcing or application service providing. However, in CC the relations between the different stakeholders are often more complex with entities from all over the world are involved [5]. Furthermore, the different service and deployment models increase complexity even further. Legal aspects that have to be considered in CC include data protection, contracts, copyright, environment and competition [5]. While all the different factors are considered, the focus in this work lies on data protection. This section introduces the relevant laws, discusses their implications on CC and issues that arise with different cloud federation scenarios.

5.4.1 Privacy and Data Protection

Art. 12 of the Universal Declaration of Human Rights 1948 acknowledges privacy as a human right [63]. However, it does not define how privacy should be protected. Many of the existing laws and regulations also apply to CC, most of them are derived from the principles of the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines and Transborder Flows of Personal Data [10]. This section is structured as follows: The nine core principles of the OECD Privacy and Transborder Flows of Personal Data are introduced, then the relevant articles from the EU are discussed including the relevant differences between the European Data Protection Directive (95/46/EC) and the General Data Protection Regulation, which is in draft state since 2012, and then the situation in the US is considered.

For this section, the deployment models can be split into two groups: Clouds in which a cloud is specifically assigned to one customer or a community of such, and clouds which are shared between independent customers (*i.e.* public clouds). In the first case, which includes private and community clouds, the organizational customer can dictate the necessary controls and safeguards. However, in the second group, the clouds are tailored according to the need of many customers. They try to be as generic as possible, to appeal to a wide diversity of customers.

Furthermore, the service levels that have to be considered can also be split into two groups: Service models that allow customers to install and run their own applications (*e.g.,* IaaS, PaaS) and service models in which the customers directly interact with a service which is under control of the provider (*e.g.,* SaaS). In the first case, the consumer, which we will be referred to as data user, has control over what information is collected and stored in the cloud. This is not the case in the second group, where it is difficult to assess what personal information is collected and for what purpose by the CSP, who also acts as data user. This is problematic, as the service providers receive more information than required to offer the service, such as time of usage and location (IP address) of the user [10].

1. **Core Principles of OECD Privacy Guidelines** To understand the implications in different service models, it is essential to understand the OECD privacy guidelines as mentioned below [53]:

   (a) Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject [53]. Personal data should be collected for business purposes only if required and, where appropriate, this should happen with the knowledge or consent of the user. In a SaaS scenario, the provider, which is also the data user, can collect more data than actually required, *e.g.,* location, usage patterns. This has to be carefully analyzed [10].

   (b) Data Quality Principle: The only data collected should be relevant to the purpose for which it is to be used, and should be accurate, complete and kept up-to-date. This implies that any CSP must only collect relevant information, and also attempt to ensure accuracy, completeness as well as keeping data updated.

   (c) Purpose Specification Principle: Defines that the purpose for which personal data is collected must be specified latest at the moment it is collected, and that it should not be used for any other purposes at a later stage. Data should not be kept longer than necessary, and if not required any longer, it should be anonymized or deleted.

   (d) Use Limitation Principle:

   The use limitation principle states that data should not be disclosed, made available or otherwise used for purposes that are not in accordance with the purpose specification principle. There are two exceptions to this principle: Data can be used for other purposes either with the consent of the data subject or by the authority of law.

   (e) Security Safeguards Principle:

   This principle is about the security of personal data, which should be protected "by reasonable security" safeguards against various risks (loss, unauthorized access, destruction, use, modification or disclosure of data). As further discussed in paragraph 8 in the detailed comments of [53], safeguards include physical (locked doors, identification cards), organizational (authority levels for accessing data), and information measures (usage of enciphering, monitoring and taking action in case of unusual activities). It further defines modification as unauthorized input of data. In public cloud scenarios, it is therefore the CSP's responsibility to ensure security of any personal data.

   (f) Openness Principle:

   This principle is about the open communication of the data user. The data user should have a "policy of openness" about their practices with personal data and disclosure of their identity and current address.

   (g) Individual Participation Principle:

This principle is about the right of individuals. Individuals should have the right to obtain data from the data user. This includes foremost the disclosure if they have any data relating to the individual, and a copy of the information within reasonable time. Data subjects also have the right to "have the data erased, rectified, completed or amended as appropriate"' [10]. Data users should therefore ensure that CSPs can fulfill these obligations.

(h) Accountability Principle: It is the data user's responsibility to ensure that all the above principles are assessed through a privacy impact assessment. It is also their responsibility to ensure that the chosen CSPs have "appropriate incident response and breach handling" [10].

(i) Basic Principles of International Application: Free Flow and Legitimate Restrictions:

Member countries should "take all reasonable and appropriate steps" to make data flows between borders secure and uninterrupted. Data should not be transmitted to jurisdictions which do not observe the foregoing data protection principles. Data users are therefore allowed to move data across borders, as long as they "establish the legal basis for entrusting personal data to CSPs".

2. **EU Data Protection Directive and General Data Protection Regulation** The current EU Data Protection Directive 95/46/EC (EU DPD) is the framework for all members of the EU, which implemented their own privacy and protection laws based on them. As previously stated, it is based on the general principles of the OECD. It is targeted to protect the privacy of all personal data that is processed for or about citizens of the EU [34].

   The General Data Protection Regulation (EU GDPR), which exists as draft since 2012, is expected to supersede the EU DPD. As a regulation, unlike a directive, it is valid, self-executing and applies to all members of the EU. Therefore, it does not require implementation on a national level by the members. This section will discuss both the implications of the EU DPD, which other countries legislations, such as Australia, Canada and Argentina also comply with (and Switzerland partially), and changes that were made in the working copy of the EU GDPR.

   (a) **Roles**

   The EU DPD and EU GDPR define personal data as "any information relating to an identified or identifiable natural person ('data subject')". The data subject must not be directly identifiable. It is sufficient that the data subject is indirectly identifiable by a reference number or by one or more factors specific to physical, physiological, mental, economic, cultural or social identity. Therefore, it is considered personal data and consequently covered by the EU DPD and EU GDPR. Personal data is all information related to a data subject.

   The EU DPD and EU GDPR both define three roles:

   - Data controller: The data controller (DC) is "the natural or legal person, public authority, agency or any other body" that determines the goal and means of processing personal data, *i.e.* the data owner.
   - Data processor: The data processor (DP) is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"
   - Recipient: The third role that is available in both EU DPD and EU GDPR is the recipient, "a natural or legal person, public authority, agency or any other body to whom data is disclosed". However, while in EU DPD "authorities which may receive

data in the framework of a particular inquiry shall not be regarded as recipients", this exclusion is missing from the working copy of the EU GDPR.

While the three above stakeholders are present in both the EU DPD and EU GDPR, the EU DPD explicitly lists third parties as "a natural or legal person, public authority, agency or any other body" that is not defined in the other roles. While not included in the definitions (Art. 4), the EU GDPR still references third parties in several articles. Both the data processor and data controller have several criteria they have to meet, which will be discussed in the next section.

(b) **Responsibilities of the different Roles**

According to the EU DPD, the data controller has the following responsibilities [34]:

- Ensure compliance with data protection law and added in the EU GDPR, transparent to the data subject
- Comply with Art. 6 of EU DPD/Art 5. of the EU GDPR. These articles define how personal data must be processed. They are based on the OECD core principles and define that data must be [20], [21]:
  - "processed lawfully, fairly and in transparent manner"
  - "collected for specific, explicit and legitimate purposes and not further processed"
  - "adequate, relevant and limited to the minimum necessary in relation to the purposes for which they are processed"
  - "accurate and kept up to date"
  - "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"
  - "processed under the responsibility and liability of the controller" (added in EU GDPR)
- Give consent to the processor
- Be liable for data protection violations

The data processor on the other hand [34]:

- Do the processing according to the mandate
- Act as agent of the mandate
- Must be a separate legal entity

However, depending on the cloud scenario, the separation of roles can be difficult to assess. For example in a SaaS scenario, unless parts are outsourced, there is no distinction between the data controller and data processor. While the above roles and responsibilities are valid for both the EU DPD and GDPR, the GDPR brings several changes that will be discussed next.

3. **Selected Changes in the EU GDPR Draft** While the roles and responsibilities are similar in both the EU DPD and EU GDPR, and both are based on the core principles of OECD, the EU GDPR introduces several changes.

The most noticeable difference between the EU DPD and EU GDPR is the change of instrument. The regulation will "contribute to having one single law applicable throughout Europe", enabling greater consistency in Europe [8].

The EU GDPR also clarifies that a CSP will fall under the EU legislation when they offer services to data subjects in the EU or monitor the behavior of data subjects within the EU. A non-EU CSP, which has an English website and a UK support phone number, offering services to UK customers, would thereby have to comply with the EU GDPR [8].

Other changes include:

- Introduce articles that clearly state and specify the responsibilities of the controller (Art. 22) and the processor (Art. 26).
- The responsibilities of the processor are increased: Changes include that data processors are explicitly required to “maintain documentation of processing operations”, carry out data protection assessment and ensure that data which is moved outside of the EU is processed with the same level of protection.
- Clarifies the criteria for determining the main establishment, *i.e.* the way to evaluate the applicable law in Art. 4 (13) within the EU and the need for a representative within the EU for controllers with their main establishment outside the EU (with exceptions) in Art. 25.
- Clarifies on international data transfer, explicitly mentioning Binding Corporate Rules (BCR) in Art. 42 and extending in Art. 43 for both the data controller and data processor. Further issues in international data transfer will follow in Section 2.
- The right of the data subjects are increased and clarified. This includes that they must be informed of data transfer to third countries and retention time (Art. 14), the right to be forgotten is strengthened (Art. 17) and introduces that data controllers must “establish procedures” to ensure the data subject’s rights. Art. 18 introduces the right to “data portability”. Data portability here referring to the personal data, which must be made obtainable by the controller “in an electronic and structured format which is commonly used”.
- Explicitly states the need for a Privacy Impact Assessment (Art. 33) when specific risks to data subjects are present. It further clarifies when prior authorization and prior consultation from a supervisory authority is required (Art. 34).
- Explicit rules on data security are introduced in Art. 30, in the EU DPD these were to be defined according to national law (EU DPD Art. 17). Art. 31 and 32 add the need for informing authorities and data subjects in case of data breach.

The EU GDPR draft therefore specifies and clarifies many points relevant to CC. However, as of the time of writing, it is still in draft stage and the full impact of the EU GDPR is to be seen.

4. **US and the Safe Harbor Agreement** Unlike in the EU, the US does not have a comprehensive data protection law, as no authorities have the power for a national privacy law. As for federated laws, the Privacy Act of 1974 regulates the collection and usage of data of personal information, but only for federal agencies and is only valid for personal data of US citizens [34]. While states in the US can have their own laws, and there are scattered laws that can apply to CC, some only applying to specific sectors such as financial services or healthcare, it can be concluded that there are “enormous differences” [33] between the regulation in the European Union and the United States [2], [27].

   Even though the level of regulation in the EU and the US varies greatly, the Safe Harbor Agreement[1] allows personal data transmission between the EU and the US. The US counterpart has to self-assess if they adhere to EU DPD and register with the Department of Commerce. Once this is completed, the US company is seen as safe harbor and personal data can be transferred as within the EU. While the recent revelations of Edward Snowden has led to discussion if the transmission is still legal in light of the US surveillance framework, in practice it remains the easiest solution for CSPs located in the US till October 2015 [59]. However, after the complaint of Maximillian Schrems, an Austrian citizen, EU Commission

[1] http://export.gov/safeharbor/

has declared US Safe Harbour as invalid, leading to examining the security of data being transferred to United States that belong to European subscribers [25].

It is therefore in the interest of US CSPs which want to increase their market potential to Europe to comply with the EU DPD.

5.4.2 Competition Laws

One of the major factors discussed in CC is the lock-in effect, which can be caused by a lack of standards. The competition/anti-trust laws goal is to protect customers [35]. As competition rules are "considered to be generally applicable norms" [65] and the lock-in effect harms customers, this chapter will explore the competition law and discuss the possibilities it has to prevent or decrease the consequences of the lock-in effect.

Art. 102 TFEU states that "any abuse (...) undertaking of a dominant position (...) shall be prohibited". This includes situations where CSPs are excluded from competing for customers of dominant CSPs [24]. However, the competition law is only partially applicable for the implications that exist in CC. Not only has the behavior to be "abusive", but a CSP must also be in a dominant position. While there is no clear cut where a CSP is dominant, generally market shares above 40% are considered problematic and are looked into further [58]. Another factor that is considered are the market entry barriers [65].

The current situation in CC, however, has no clear market leader, competition between provider (including Google, Microsoft, Amazon, Salesforce) is fierce [58] and it is unlikely that one of these providers will find itself in a dominant situation within the foreseeable future. Furthermore, while entry barriers exist, *e.g.,* high initial costs, they cannot be considered "insurmountable" [58]. Therefore, even though the lack of standards, and issues with data portability, interoperability and other technical factors, can lead to disadvantages for customers, there is no evidence that there exists a situation which would call for an intervention from competitive law. However, if the leading CSPs act in a way to specifically shield their services, it might become a case for competition law. Competition laws should encourage open cloud systems, promoting open standards and monitor the market carefully [65].

5.4.3 Contracts and Service Level Agreements

The stakeholders in CC are typically in a relationship which is based on contracts. This does not only apply to the cloud customer and the CSP, but also applies for brokers. The SLAs have a central role in CC, they define the specification and quality of the service. They also define the consequences when a party does not deliver as agreed and can act as specifications, when services are defined in great detail[5].

CC SLAs typically include as derived from [32], [5]:

1. Definition of Services: This section includes the services agreed upon and how they are delivered. They must be accurate and include specific information for each agreed on service [32]. The terminology used within the SLA should also be clarified in this section.
2. Availability and Service Response Time/Latency: Of special interest for CC is the (technical) availability and agreed upon maximal response time of the service. These technical thresholds are an essential part of any SLA. For both of these factors, the SLA only applies to issues that arise at the CSP. If the cloud-based service is not available due to a third party (*e.g.,* outage of Internet connection on the CSC's premises), the CSP cannot be made accountable.

3. Perfomance Management: To ensure that customers can recognize and take action on deviations from the agreed service levels, performance management is required. It is important that all agreed upon service levels can be measured. This section of the SLA specifies where the performance management monitored and measured results and benchmarks are available. Many of the public cloud solutions offer “best-effort-service”, for which performance management is less relevant. If specific thresholds are defined, this section becomes more important.

4. Problem Management: This section covers how incidents and issues are resolved. It often includes the timeframe in which issues have to be resolved by the CSP after an issue has been reported by the CSC. As with the availability and service response time, this only applies to issues where the CSP is responsible. This section should also include preventive measures.

5. Customer Duties and Responsibilities: The SLA does not only define the responsibilities of the CSP, but also of the CSC. This can include how, when and how many users can access the service. If physical access to the CSP’s premises is required, procedure and restrictions are also outlined here.

6. Warranties and Remedies: The penalties describe the consequences of when the service and quality levels agreed upon are not met. This can include fines but also termination (without cancellation period) of the service [5]. This section should also include third party claims, remedies for breaches and the exclusion of force majeure.

7. Security: The agreed upon security settings that have to be adhered to by the parties. This is especially important, as cloud services are available from everywhere. Therefore, the required authentication process and how authorization is granted has to be considered. Furthermore, it should be defined what information is logged, who has access to the logs and how anomalies are treated.

8. Disaster Recovery and Business Continuity: Cloud-based computing often leads to high dependencies for CSC, disaster recovery should be reflected within the SLA. At the highest level, this section typically states “that there must be adequate provision for disaster recovery and business continuity planning to protect the continuity of the services being delivered” [32].

9. Termination: The termination agreement of the contract. It should cover how the terms of termination at the end of initial term, termination for convenience, termination for cause, and payments on termination [32]. As [5] points out, this section should also include how data is to be treated. This includes deletion of data and transferring data back to the CSC. For both of these, the level of security also has to be considered.

10. Subcontractors, Applicable Law and Place of Jurisdiction: This section covers further legislative questions. It is to be defined if the CSP can use subcontractors and define the accountability of using them, which laws are applicable and which is the place of jurisdiction[5].

    Many details can therefore be covered in the SLA. However, it is important to note that SLAs have to comply with all legal aspects and are otherwise not valid.

5.4.4 Other Legislation and Industry Specific Regulations

While contracts and SLA are essential for CC in general, there exist legislations and industry specific regulations which can affect CC in specific cases, but consequences are case specific and therefore out of scope for this section. Several examples will be introduced within this section of the deliverable.

1. **Copyright** CC introduces new challenges regarding copyright, both to the (public) CSP and the CSC. These challenges include whether CSPs are responsible for copyright infringements by their users and if the existing Internet Service Provider's (ISP) safe harbor legislation, which protects the ISPs from consequences of their subscribers regarding copyright infringements, is sufficient to satisfy all stakeholders.

   While CC might increase the complexity, [62] concludes that "there is no immediate need to strengthen the protection of online intermediaries and CC providers". Furthermore, as [34] explains, it is difficult to derive common requirements for CC from copyright laws, as they are typically case specific.

2. **Ecological Legislation** Data centers typically require large amounts of energy and with the target of reducing greenhouse gas emissions [44], ecological regulation can become a factor to be considered in CC. According to [41], (public) CC is attractive to "large IT infrastructures that want to reduce their carbon footprint". Further goals in greenhouse gas reduction and corresponding laws and regulations can increase pressure on companies to reduce their carbon footprint, making CC a valuable option. Of course, CSPs are also affected by such laws. However, the eco-friendliness depends on many factors [34] and no regulations that specifically apply to CC exist.

3. **Industry Specific Regulations** Unlike the previous discussed laws, there are also many regulations which only apply to specific industries. This is especially the case in industries where confidential personal data is required. There are more industries and many local regulations for different sectors, exemplarily we will consider the US financial and healthcare sector.

   (a) Financial Services: The financial industry in the US has to comply with the Gramm-Leach-Bliley Act (GLBA). It covers many topics, including information privacy and sets standards to ensure security against unauthorized access and other threats [27].

   (b) Healthcare: The healthcare sector is another example that is highly regulated. For the US, both the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) have to be considered by organizations which possess personal health data. HIPAA requires organizations to take specific actions to ensure confidentiality, integrity and availability of personal data [27].

5.4.5 Cloud Specific Issues

The different laws and regulations that are specifically applicable to CC. Such issues include the general concept of outsourcing, the location of the different stakeholders, subcontracting in relating to the contracts and SLAs.

1. **Outsourcing** Public cloud-based computing is a form of outsourcing. This leads to several challenges [10]:

   (a) Technical Safeguards for Identity Management and Authentication: Cloud-based computing services, especially in the case of public clouds, are often accessible from everywhere, all the time. While this increases the user's mobility, it introduces the need for identity management and authentication to comply with the data security principles and laws.

   (b) Proper Exit Plan, Data Erasure and Data Portability: Data processors are responsible to comply with the collection limitation, use limitation and that data subjects can have their data deleted. It is essential, that a proper exit plan is agreed upon and it is ensured that data is deleted on termination of any contracts. Since under the EU GDPR it is also required, that data subjects can receive a copy of data stored in a common format, data portability must also be considered.

   (c) Limitations on the Data Use in the Cloud: Public CSPs might receive data from several of their customers on data subjects, in some cases the data subjects might use them directly. This leaves CSPs in a position, where they can combine data of different sources on data subjects. However, this is prohibited by the use limitation principle and laws derived from it. Data processors should include limitations on how data is to be used by CSPs in the contract.

   (d) Formal Data Breach Management and Notification Arrangements: Data subjects must be informed on data breaches. Plans for all eventualities should be in place from the very beginning, ensuring that in case of data breach data subjects are informed.

2. **Location and Cross-Border Data Flow** CSPs often have data centers all over the world, or offer services in other regions than where they offer their services. CSPs can optimize use of their resources, increase availability for the consumers and act more flexible. While this makes sense for CSPs, it is problematic from a legal perspective as many legislations prohibit data flow between borders. Even if data is only stored in applicable states, it is still possible that the data is transmitted via third-party countries.

   (a) Personal Data in other Jurisdictions: As explained before, having data in different locations is beneficial. However, the data controller is responsible to comply with the law. When transmitting data to different locations, it is important to consider any exceptions to the prohibition of transmitting data between borders. In the EU, the already discussed safe harbor agreements and binding corporate rules can be applied. It must also be remembered, that depending on the legislation, data subjects must be informed that data is transmitted across borders.

   If clouds are located in several territories, the question which laws and courts are responsible arises. In civil law the CSPs and CSCs can choose the law and responsible court. However, it must be either one of the locations of the CSP or the CSC. In private law, the applicable law is geo-location determined by the location of the CSP [52]. It is important for CSCs and providers to consider the competent court and the consequences of it. The EU GDPR will have consequences on place of jurisdiction, to what extent is still to be seen.

3. **Subcontract Offerings** Scalability and elasticity are great advantages of CC. However, to achieve this, many CSPs work with several infrastructure providers. If the CSP cannot provide the capacity itself, subcontractors will allocate resources. Subcontractors might use subcontractors themselves for the same reasoning. From the perspective of a CSP, this is a reasonable action. However, it increases the risk of loosing control over data for the CSC. While data subjects have to be informed about data movements to third countries under the EU GDPR, very few CSPs are transparent about subcontracting arrangements as of now. The use of subcontracts leads to several implications [10].

   (a) Lack of Formal Contractual Relationship: The CSC has no formal contract with the subcontractors of the CSP. In many cases, the CSC might not even be aware of the different subcontractors. In the case of a data breach or misuse, the CSC cannot hold the subcontractors contractually liable for any consequences. The missing direct link can reduce the perceived responsibility and loyalty of the subcontractors, leading to less sensitive handling of direct data. In the case of data breaches, the legal and reputational damages to the CSC can often not be "realistically compensated for by suing either the CSP or its subcontractors".

(b) Lack of Privacy Awareness and Legal Sanctions: Subcontractors in different locations might have a different attitude towards data privacy and lack the respect for it. This can be caused by the lack of legal sanctions available in their operating environment.

(c) Standard Offerings, Terms of Usage and Service Level Agreements: CSPs often only provide a predefined set of services. These offerings include terms of usage and service level agreement. This is especially true for personal CSPs. The contracts in such offerings often include clauses that are "detrimental" to the CSC. Smaller costumers often lack the market power to receive better contracts, due to scale, size and resources [33].
CSCs should not consider CSPs' standard offers that do not comply with their security requirements. Failing to do so puts personal data and personal data and business reputation at risk. While it can be difficult for smaller organizations to retrieve personalized contracts, the terms should always be discussed to ensure compliance with the different OECD core principles.

5.4.6 Modeling of Legal and Regulative Constraints

The decision to adopt a cloud-based services in an organization is a complex task because of the influence of numerous Non-Functional Requirements (NFR) *e.g.,* availability, interoperability, and presence of several alternatives, *e.g.,* service providers can offer multiple packages. In addition, the decision is also effected by various legal and regulative constraints. Therefore, it is crucial to understand, identify, and model the effect of such constraints on the evaluation of NFR and available alternatives. For example, when an organization wants to retrieve data from the cloud in a re-usable format, they also need the meta-data from the CSP. However, the Service Level Agreement (SLA) may not clearly state if both data and metadata are included when the data is returned to the customer. In such cases it is important to identify who bears losses and how liability is distributed, when the data, which is stored in the cloud, cannot be re-used by the organization. Clarification of this will help organizations to rank several alternatives differently (provided by different cloud service providers) on the criteria of portability. This section, therefore, uses the Goal-oriented Requirement Language (GRL) to model the effect of legal and regulative constraints on ranking available alternatives with respect to NFR [26]. GRL is a modeling language used in system developments to support goal-oriented modeling and includes requirements, specifically non-functional requirements [29]. The syntax of GRL is as shown in Figure 18. These regulations are complex and vague, and can be interpreted in different ways based on the specific scenario. An organization, therefore, must evaluate the legal and regulative constraints specifically (but not exhaustively) from following perspectives:

- Data in terms of its control, storage, processing, deletion, leakage and loss.
- Interoperability and portability
- Security and privacy

Therefore, the interrelations between these factors and the relevant laws (with the EU) are identified, and modeled using GRL. To illustrate this, lets consider an example of data storage and deletion. Following relevant constraints, as mentioned in European Data Protection Directive (DPD) [20], have to be abided:

- A CSP has to abide with the local laws of the region where computing node is located. This is valid also for the CSP from the United States of America, who hosts the data on a server located in an EU member state, has to abide by the laws of the EU member state for transferring data.

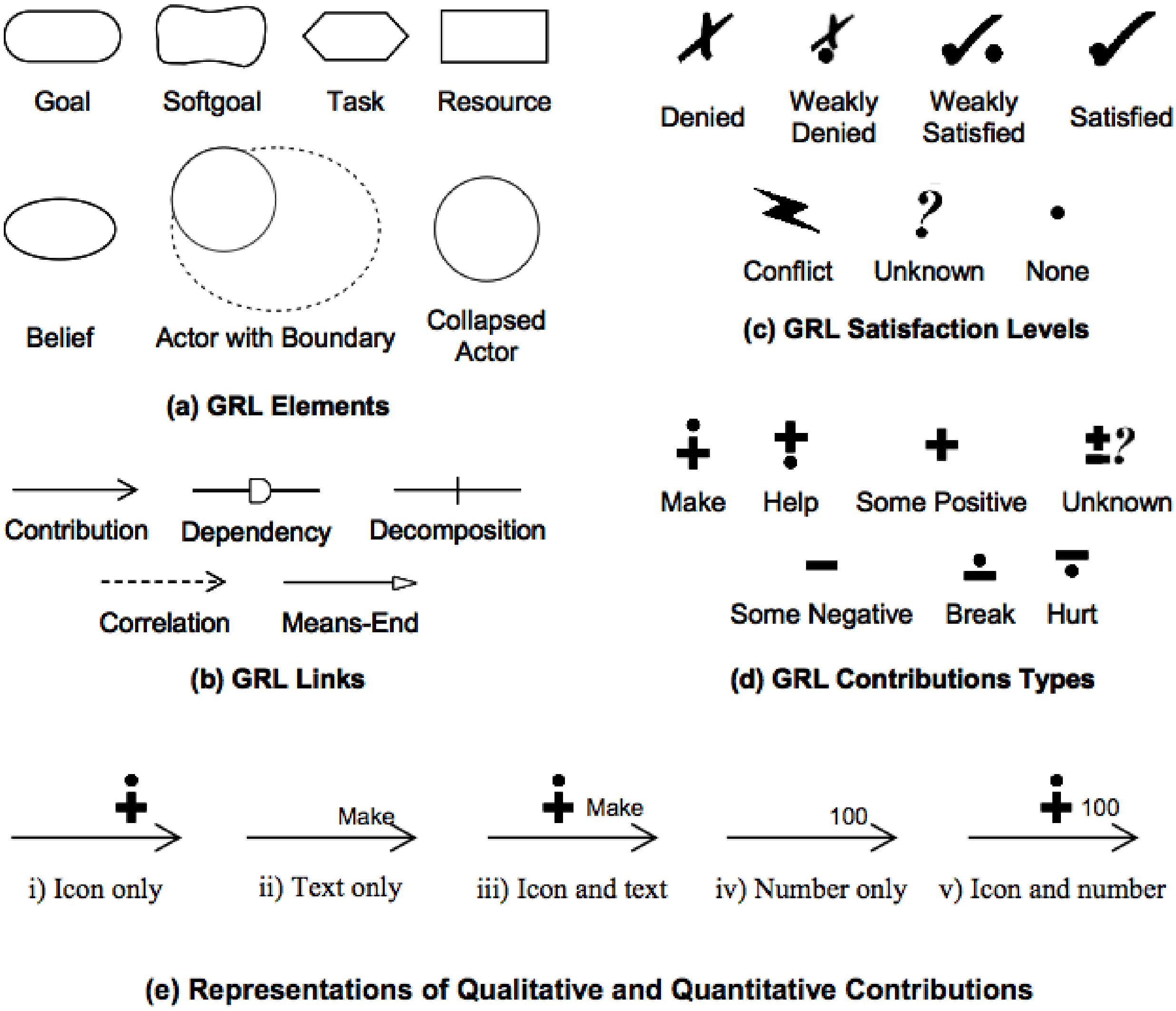


Figure 18: Basic Elements and Relationships of GRL [14]

- DPD introduces two responsibilities with the role of a data controller and a data processor. Rules of the EU Directive on data protection states that the location of the data controller determines the national law applicable for data processing, as he is liable for data protection violations. Only in cases where the user modifies the data without the involvement of the CSP, he becomes the controller as well. In case of multiple locations, the responsibility of data controller can be on the CSP and/or the Infrastructure Provider (InP).
- During the negotiation of the contract with the CSP, customers also have to be aware of licensing terms, intellectual property rights, indemnities and protection, or content access rights to the service provider.
- Data security also has to be taken into consideration from the side of CSP. It includes en-

crypting the data as well as applying correct policies for data sharing.

It is important to note here that the applicability of these constraints is dependent on the use-case under consideration. The following subsection explains one GRL graph generated and the logic behind the modeling of one of such use-cases.

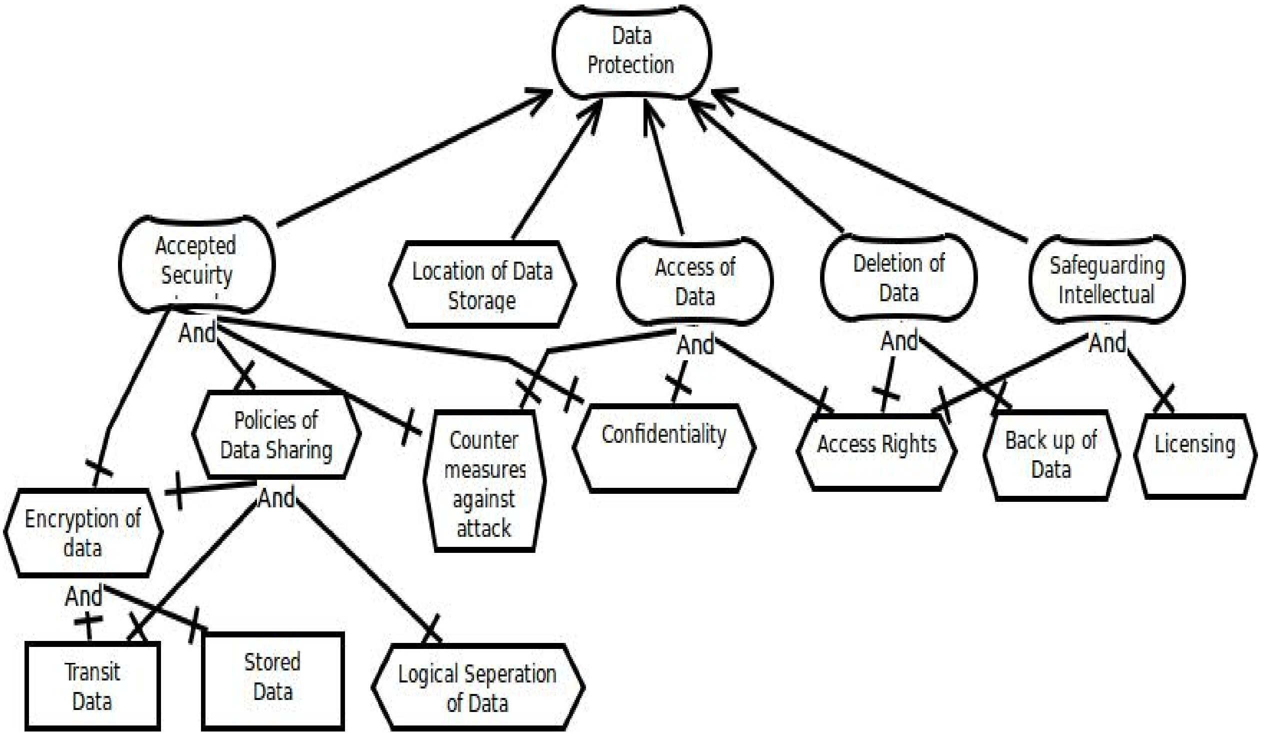


Figure 19: GRL Graphs for Data Protection [26]

As shown in Figure 19 the soft goal of data protection compliance comprises of soft goals of 1) Accepted Level of Security, 2) Location of data Storage, 3) Access of data, 4) Deletion of Data, and 5) Safeguarding Intellectual Property. Each of these soft goals comprises of multiple tasks to be completed so that the soft-goals are completed. For example, in case of Accepted Level of Security, three tasks have to be completed as that of 1) Encryption of data, 2) Policies of data sharing, and 3) Counter-measures against attacks. These tasks in-turn might need some resources in order to successfully complete the task. This is shown in Figure 19 in case of task for policies of data sharing. For more details on this, we refer to [26].

5.4.7 Findings on Legal and Regulative Perspective of Cloud Adoption

This section identified and discussed various constraints that are present from legal and regulative perspective when an organization decides to adopt Cloud-based services to fulfill its IT requirements. These constraints can be specific to be the jurisdiction of the CSP, location of data storage, and location of the organization itself. Also, the constraints are very much dependent on the specifications of the SLA, the requirements of the organization, and the offerings of the CSP. Also, as the laws and regulations itself are interpretation dependent, it is important to model the implications at least qualitatively. Therefore, based on the methodology presented above, modelling of regulations and requirements of the organization can be done. This will lead to evaluate the CSPs in terms of their compliance to legal and regulative specifications.

6 Interview-based Validation of Scenarios

As defined in D7.2, Interview-based validation approach is a qualitative method that aims to have an in-depth analysis of the topic under consideration. As per the generality of interview-based approach, the scenarios within WP7 followed the following sequence: (1) Identification of relevant questions in order to achieve the target (in this case validation of assumptions, approach, and results of scenarios), (2) conduct an interview, with relevant experts, and (3) analyze the collected information in terms of relevance, reliability, and validity. This application was done based on a questionnaire, which was filled in during interviews with the external experts. The outcome of such interviews is a validation of those approaches, assumptions, and partial/final results of those WP7 scenarios. While this Section here summarizes the major findings on a per interviewed scenario basis, the detailed outcome of each performed interview is documented within the appendix to D7.3 in Section 12.

6.1 Resource Management in Network Function Virtualization

The scenario of resource management in NFV was discussed with Telefonica S.A., a Spanish broadband and telecommunications provider with operations in Europe, Asia, North America and South America. Operating globally, Telefonica is the sixth largest mobile network provider in the world.

The validation was performed by email correspondence, between Joan Serrat, Juan-Luis Gorricho and Rashid Mijumbi from the Universitat Politècnica de Catalunya (UPC), and Alfonso Tierno, an engineer who is focused on the development of Network Function Virtualization solutions for Telefonica (I+D).

This validation was aimed at building on the validation that was performed the year before (involving resource management in virtualized networks) in which the industry experts had proposed that FLAMINGO aligns the scenario to NFV, which was their focus. In fact, during the email correspondences, the industry expert re-confirmed that Telefonica as a company was involved in many aspects related to NFV. With regard to the placement of functions in NFV [49] as considered in the scenario, the expert noted that it is important because function placement will impact the amount of traffic to be moved through the network as well as on the delays that the traffic will experience. On the dynamic management of resources [48, 45, 51], he stated that while resources were currently statically allocated to the functions , a solution that automates this process and makes it more dynamic, as proposed in the scenario, would be of interest to the industry. Finally, with regard to the server placement problem [50], the expert noted that, in the case of Telefonica, server location is usually linked to the physical buildings owned by the company (old central exchanges) and/or to the location of third parties (i.e. Amazon). This implies that there would be little or no flexibility left.

As a whole, the expert stated that the sub-problems considered in the scenario considers relevant and important challenges in NFV, which were interesting for the industry. Finally, building on the relationship established with Telefonica, a joint article (submitted for publication) on the management and orchestration in NFV has been authored by FLAMINGO and Telefonica.

6.2 ISP-oriented Content Delivery

The ISP-oriented cache management scenario was discussed in the previous year with a Belgian-based and an UK-based ISP. The outcome of these interviews have been documented in D7.2. We shortly summarize the main feedback. Both ISPs validated the scenario as relevant and indicated that they have themselves started to deploy caches inside their network to improve customers' QoS. The ISPs also pointed out that the peering cost for inter-domain traffic will be similar for a scenario with a centralized caching locations as well as for a distributed caching location. Based on that feedback we focus on the cost savings that can be gained by reducing the multi-year investment cost in node and link infrastructure (*e.g.,* optical fiber, routers) and compare those to the investment cost in caching infrastructure.

This year we focused on the validation of the cost points for our analysis. Technical staff from the Flemish broadcaster VRT was therefore interviewed. Their optical distribution and contribution wide-are network, was taken as a reference point for equipment prices. In addition, cost point from [55] were validated. The main learning point from the discussions is that there exists a large variation between the official price list and the price paid by large customers. High levels of discounts apply. As such different organizations may pay a different price for the same product. The same is true for the lease price of dark fiber. To overcome these variations and provide meaningful results, we plan to conduct sensitivity analysis on the cost input points. Our contact point did not wish that the price information was made publicly available as the data is confidential. As such that data is not included in this deliverable. This is not an issue for the study itself as it is possible to work with relative values for the cost points. The results will also be presented as relative differences.

6.3 Legal and Ethical Facets of Data Sharing

The scenario of Legal and Ethical Facets of Data Sharing was discussed, based on the questionnaire provided by WP7, with the Dr. David Douglas, who acts as Ethical Adviser for the Center of Telematics and Information Technology at the University of Twente. As Ethical Adviser, Dr. Douglas supports UT researchers in reasoning about ethical aspects of their research. In particular, his role is to help researchers making decision about values that goes beyond their technical expertise. As such, Dr. Douglas has been asked to act as independent expert for this use case.

The Legal and Ethical Facets of Data Sharing scenario in general, and SURFnet draft policy for Ethical Data Sharing, were positively welcomed, and the scenario perceived as well worked out. The overall feeling was that the problem is of high relevance, given that it has a direct impact on network management and security, and on the QoS finally perceived by the users. The identified stakeholders essentially cover the most important aspects of the scenario, in the way this has been defined. However, Dr. Douglas also identified the role of final users as being of central importance. From an ethical point of view, single users are those whose privacy we aim at protecting while trying to share more data. During the discussion, we identified that the role of stakeholder "Network Operator" could already include the final user, in case the network operator recognizes its duty to act in the interest of its users (as it happens for example in the case of the draft policy). It also emerged that the stakeholder Ethical Committee should include in its role to advocate with the Network Operator in place of the final user, i.e., the Ethical Committee will ensure that the interests of the final users are taken into consideration.

In addition to above mentioned interaction, there was an interview conducted with Daniel Bertolo, who is a System Engineer, Team Leader Global LAN, and Esther Zysset who is Attorney-at-law, General Counsel at SWITCH. This interview also concentrated on finding the applicability and relevance of SURFnet draft policy for Ethical Data Sharing. It was discussed that such a policy work and guidelines, is an indication of an organization taking its responsibility of protecting the data seriously. However, for SWITCH the board has made a decision of not sharing data with external parties. In addition network measurement data was discussed with respect to associated data protection and privacy.

7 Summary, Conclusions, and Future Work

The work performed in project year Y3 within FLAMINGO's WP7 on "Economic, Legal, and Regulative Constraints" has lead to relevant observations, results, and conclusions, especially with respect to those WP7 scenarios that show a close collaboration with WP5 and WP6.

The overall work done and achieved within FLAMINGO's year 3 and in Deliverable D7.3 follows a cross-disciplinary approach of understanding the inter-dependency of technology on economic, legal and regulative constraints. A selected set of specified use cases have been studied and discussed in terms of (1) a multi-actor analysis and cost modeling, (2) investigation and modeling of legal and regulative requirements, (3) validation of methodology and results with help of value network analysis and tussle analysis between relevant stakeholders. The major findings of this deliverable are summarized as follows:

1. In order to successfully deploy, and operate any technology in the field of network and service management, economical, legal and regulative interdependencies and constraints need to be studied and modeled. This was achieved by the multi-cost analysis, cost modeling, value network analysis, and modeling of legal and regulative constraints. The interdependency between the technical and regulatory domain was studied in the scenario of Schengen Routing, where still many open questions exist, especially from the technical and practical domain. Especially the need of a realistic setting, if that may ever exist, have to be determined before Schengen Routing may become a reality.

2. The economic analysis builds in depth and further on the work done in previous years. In the ISP-oriented content delivery scenario, multi-actor analysis and cost modeling are used, while in the resource management in virtualized networks scenario, the focus is on the (dynamic) pricing of virtualized resources.

3. Three approaches were applied to numerically validate WP7 scenarios. The first approach validates the economic impact of WP7 scenarios by applying (dynamic-) value network analysis. The second approach of a Socio-economic-aware Design of Future Networks by Tussle Analysis resulted in the ITU-T Recommendation Y.3013 in FLAMINGO year 2 already as a meta-methodology being applied in year 3 for selected scenarios. The third approach applies an interview based method for validating the scenarios' approach, their assumptions, and related results with the help of external industrial experts.

4. The value network analysis was conducted for current situations of three scenarios: (1) resource management in virtualized networks, (2) ISP-oriented content delivery, and (3) legal and ethical facets of data sharing. This type of numerical analysis clearly showed the different roles and their diverging targets that are involved within these scenarios. The complementary exchange analysis, impact analysis and value creation analysis indicated that in the current value network configuration each actor is able to generate value from value exchanges, but that there is also room for scenario- and situation-dependent improvement.

5. Dynamic value network analysis was used for the first time to show how the conducted research will change the value network in comparison to the current situation. For the ISP-oriented content delivery scenario, the relationship between the actors and roles in the value network do change, which may potentially lead to tussles. For the resource management in virtualized networks scenario and the legal and ethical facets of data sharing scenario, there are now changes in the relationships between the actors and the roles and, as such, we do not foresee any potential tussles.

6. The lack of proper understanding of regulations and laws by more technology-oriented stakeholders (*e.g.,* service provider, operator, and network provider) lead to law, policies, and mandates not being completely incorporated in any business strategy. Thus, D7.3 takes a step in modeling carious regulations and identifying various implications of law and regulations in the field of network and service management. This is specifically done with respect to regulations relevant in Cloud Computing, Schengen routing, and Network Neutrality.

7. In order to facilitate the understanding of legal and regulative constraints and its implications in the field of Cloud Computing, D7.3, also presents a methodology to model policies and laws. This supports the evaluation of different Cloud Service Providers in terms of their compliance of legal and regulative requirements.

7.1 Conclusions

The conclusions and major observations drawn after the end of third project year of FLAMINGO are as follows: First, interdependency between technology, economical goals, and legal and regulative goals exists and has to be identified and modeled for a successful monitoring, managing, and operating of the Future Internet. Second, it is important to evaluate the technology, service providers, or developed system to determine whether it conflicts with legal requirements; *e.g.,* a data processing system must comply with the local data protection regulations, before adopting it to fulfill any other IT requirements. This is complemented by the fact that current legal interpretations do not always exist in a stable form. Even further, as the Safe Harbor case and court ruling in the early days of October 2015 reveals, a legal framework - already in place and in operation for a longer period of time - may not hold forever. Thus, technology changes and legal changes do reflect the need for a continuous evaluation of legal constraints and changes. Third, it is important to understand the change in numeric value exchange, new interest, incentives, and tussles of stakeholders involved, when a new technology is deployed in real world scenario.

In turn, this work of WP7 and its related documentation within this deliverable D7.3 act as a basis for network and service management decisions, multi-actor and cost modeling analysis, country-specific and region-specific regulative settings identification and modeling. Note, that especially the legal perspective - and to a certain extend the regulative, too - will always lead to a case-by-case investigation in case of disagreements between stakeholders involved. As such, no general solution can be provided, however, a check-pointing and guidelining will be possible to a certain level of detail, as to be addressed in FLAMINGO's year 4 work.

7.2 Future Work

All of these findings in D7.3 will be refined and finalized in the final year of the FLAMINGO Network of Excellence. This will be continued in the line of tasks T7.1 and T7.3. This will also lead to the identification of guidelines, which will be based on scenario specific learnings.

The next steps will be to identify a list of checks to be performed with respect to network and service management facets in the economic, legal, and regulatory domains, before a technology is deployed in the real world. These checks will include specific technical, economical, and legal and regulative factors that must be evaluated to ensure a successful deployment and operation of a technology, similar to any scenario of WP7 under study today. Also, a set of feasibility aspects of the scenario will be studied, which will include an interpretation of results obtained in WP7 under the operational perspective and, as far as possible, in-line with technology specifics of WP5 and WP6.

8 WP7 Objectives

FLAMINGO's WP7 objectives are determined by the key areas of networking systems in which relevant stakeholders interact in a cross-disciplinary manner. The focus of WP7 is on the challenges of economic, legal, and regulative constraints of selected network and service management technology, mechanisms, and solutions. Core objectives concentrate on the integration of those dimensions, the respective dissemination of results, and joint Ph.D. works. Therefore, the objectives are summarized, as defined in the Description of Work (DoW), in the following sections.

8.1 WP7 Objectives

WP7 objectives focus on achieving cross-disciplinary methodologies so that technological dependency on economical, legal, and regulative aspects can be studied. The progress in this scope of these objectives is summarized in Table 17. This section provides a high-level summary of the WP7-specific objectives. These objectives have been grouped into two categories: Section 8.1.1 describes the status of the objectives in which WP7 researchers are currently active. We refer to these as *ongoing and completed-objectives*. Section 8.1.2 includes the objectives for which so far no progress has been made. Activities related to these objectives will be part of Y4 of FLAMINGO. These are termed as *open objectives*.

8.1.1 Ongoing and Completed Objectives

Objective 1: To integrate European network and service management research regarding Economic, Legal and Regulative constraints – WP7 works with a close collaboration with work packages WP5 and WP6 that deal with various research activities regarding network and service monitoring, and automated configuration and repair of Future Internet. In Y1, 9 scenarios were identified, which were analyzed within WP7. In Y2, based on scope, relevance, and in order to deepen the analysis from economic, legal, and regulative view point, 6 scenarios have been identified and studied within WP7. In Y3 the following ones have been studied: (a) Resource Management in Virtualized Network (b) ISP-oriented Content Delivery, and (c) Legal and Ethical Facets of Data Sharing, combined with specific and new scenarios of (d) Schengen Routing, (e) Network Neutrality, and (f) Cloud Adoption. The new scenarios specifically focussed on legal and regulative perspectives in these specific domains.

Objective 2: To create and maintain articles within Wikipedia and other online systems in this area – The research conducted in Y1 and Y2 has allowed us to generate valuable knowledge that can be used for contributing to Wikipedia. In collaboration with WP2, WP5, and WP6, WP7 in Y3 has identified a set of Wikipedia articles where a contribution would be beneficial. For more information on this topic, we refer the reader to D3.3.

Objective 3: To address in an integrated manner operations, management, and maintenance with respect to economics, legal, and regulative constraints coherently – In order to facilitate operations and management of various technologies of Future Internet, three aspects were studied in Y2. These are the a) identification of business indicators and policies, and their mapping functions, b) economic interdependencies of the business indicators and goals, and c) regulative frameworks, which decide the boundaries and constraints for the operations of these technologies. The methodologies for operations, management, and maintenance of technologies within network and service management are completely identified with the end of Y2. In last year this integrated methodology will be taken a step ahead to identify the first set of guidelines, needed to successfully deploy such scenarios from an operational point of view.

Objective 4: To apply cross-disciplinary methods and approaches on technology as well as economic, legal, and regulative dimensions – This objective was marked as completed with the end of Y2. For details, please refer to Section 4 of D7.2.

Objective 5: To define a model, architecture, and mechanisms for three stakeholders in an integrated manner: especially covering the operator, the application provider, and the end-user – This objective is also marked as completed with the end of Y2. For more information please refer to Section 6.2 of D7.2.

Objective 6: To support an integration of the following five factors: (a) cost-awareness, (b) incentives for service provisioning, (c) fulfillment schemes, (d) business policies, and (e) legal/regulative frameworks – Y2 included analysis with respect to multi-actor analysis, service level agreement, pricing and cost modeling for relevant scenarios. Also, various regulative frameworks have been studied with country-specific, partially region-specific settings. Business policies are also completely identified for all relevant scenarios, as shown in Section 4 and Section 5 of D7.2. Y3 fulfilled these factors by utilizing them to evaluate and validate the scenarios within the scope of D7.3. This validation is done using value networks and tussle analysis, thus, marking the completion of this objective. Please refer to Section 3, Section 4 and Section 6.1.

Objective 8: To evaluate mechanisms under scenarios determined and derive guidelines for stakeholder defined –Y3 includes evaluation of scenarios with respect to value networks and tussle analysis, depending on their respective applicability. In addition, the assumptions, methodologies, and results of the scenarios were also validated with the help of external partners. Based on these validations and analysis, Y4 will specify a set of guidelines, which will be based on scenario-specific examples.

8.1.2 Open Objectives

Objective 7: To investigate related operational costs for service offerings by Internet Service Providers (ISP) and telecommunication system providers – Even though the cost modeling for various scenarios was part of work done in Y2 and Y3 of FLAMINGO, operational cost from the perspective of ISPs and telecommunication system providers will be part of research that will be done in Y4 of FLAMINGO.

Table 17: WP7 Objectives

No.	Objective	Status as of Y3	Description	Section/Deliverable	To be Addressed in Y4
1.	Integrating network and service management research regarding economic, legal, and regulative constraints	IN PROGRESS	Analyzing various scenarios in these dimensions. Economic analysis focuses on multi-actor analysis, service level agreements, pricing and cost modeling. Legal and regulative constraints focus on Network Neutrality, adoption of cloud, Schengen routing	Section 4, Section 5	To be refined and studied in further depth
2.	Maintaining Online Informative Systems	IN PROGRESS	Details of content and topics included in D3.2	D3.2	To maintain articles online *e.g.,* Wikipedia, once terminology in this cross-disciplinary area has settled.
3.	Integrating operations with economic, legal and regulative constraints	IN PROGRESS	Business indicators and policies were identified based on economical and legal interdependencies	D7.2	Identify set of guidelines, needed to successfully deploy such scenarios from an operational point of view.
4.	Methods and approaches for economic-legal analysis	DONE	Joint architecture defined	D7.1	Can be adapted, if required.
5.	Models, architecture for stakeholders (operator, application provider, end-user)	DONE	Refined and studied in value networks	D7.1	Inter-relations between stakeholders studied as part of Value Networks in D7.1. Future year will see this work as part of validation mechanism.
6.	Integration of cost, incentive, business policies and legal/regulative frameworks	DONE	Value Networks and Tussle Analysis is used to define, evaluate, and validate the scenarios from these perspectives. Also, regulative constraints for various fields of network and service management have been studied.	Section 4, Section 5	Can be re-used, if needed.
7.	Operational costs for Internet Service Provider and telecommunication system providers	FUTURE	To be defined in Y4	-	Cost models to be investigated for stakeholders.
8.	Evaluate mechanisms under scenarios determined and derive guidelines for stakeholder defined.	IN PROGRESS	Validation work of all scenarios has been done with external partners, value networks, and tussle analysis.	Section 4, Section 6	To identify and complete guidelines, keeping economic, legal and regulative constraints in consideration.

8.2 Project (S.M.A.R.T) Objectives

Progress on two Specific, Measurable, Achievable, Relevant, Timely (S.M.A.R.T) Objectives, which WP7 focuses on, are defined in the DoW and their respective achievement degrees after third project year in total reads as follows:

1. **Writing of joint scientific papers:** The Description of Work (Section B.1.1.5) states that "after 18 month at least 20 scientific papers will be submitted / published". In the first two years the project had exceeded the expected number of publications. In the third year the research work packages published 73 papers at major conferences as well as in journals, and with this exceed the expected number of papers. The complete list of published papers, is listed in D8.3. Partners also targeted top conferences and journals in the network management field and high-end conferences and journals in the field of networking and measurements as suggested by the reviewers during the last evaluation. To address this, papers have been published at IEEE INFOCOM 2015, Communications and Network Security (CNS) 2015, International Symposium on Cyberspace Safety and Security (CSS 2015) and ACM Multimedia Conference (ACM MM) 2015.

   In addition FLAMINGO has participated in writing internet-drafts and RFCs, and contributed in standardization forums like ITU-T, IETF. The complete list of such participation is listed in D4.2.

2. **Integration of Ph.D. students:** *The Description of Work (Section B.1.1.5) states that after 9 months each research WP will have identified at least two fully integrated Ph.D. students, which means that these students will be jointly supervised and financially paid by FLAMINGO* Collaborations are a cornerstone of research within FLAMINGO. It is important that collaborations are not only taking place between fully integrated PhD students, but also among students that are not financially paid by FLAMINGO but jointly supervised. In the first two years of the project 14 PhD students have joined FLAMINGO. In the third year, three more PhD students have joined the NoE. These students, their affiliations and the co-supervising institutions are listed in D8.3.

9 Abbreviations

AS	Autonomous System
CC	Cloud Computing
CDN	Content Distribution Network
CP	Content Provider/Producer
CSP	Cloud Service Provider
CSC	Cloud Service Customer
$D7.1$	Deliverable 7.1
$D7.2$	Deliverable 7.2
DPI	Deep Packet Inspection
$DWDM$	DenseWavelength-Division Multiplexing
$ETSI$	European Telecommunications Standards Institute
EU	European Union
DPD	Data Protection Directive 95/46/EC
$GDPR$	General Data Protection Regulation
$ETSI$	European Telecommunications Standards Institute
EU	European Union
FP	Flamingo Partners
$GLSBA$	Gramma-Leach-Biley Act
GRL	Goal Requirement Language
$HIPAA$	Health Information Technology for Economic and Clinical Health
$ICMP$	Internet Control Message Protocol
InP	Infrastructure Provider
IP	Internet Protocol
$IPTV$	Internet Protocal TeleVision
$IPVPN$	Internet Protocol Virtual Private Network
ISP	Internet Service Provider
$MPLS$	MultiProtocol Label Switching
NDA	Non-disclosure Agreements
NFV	Network Function Virtualization
NFR	Non Functional Requirement
NN	Network Neutrality
NO	Network Operator
NPV	Net Present Value
NSA	National Security Agency
NVE	Network Virtualisation Environment
$OECD$	Organization for Economic Co-operation and Development
OTT	Over the Top
QoE	Quality-of-Experience
QoS	Quality-of-Service
$RIPE$	Réseaux IP Européens
REG	Regulator
SLA	Service Level Agreement
SN	Substrate Network
SP	Service Provider
$SURFnet$	Dutch National Research and Education Network
TCP	Transmission Control Protocol
$TFEU$	Treaty on the Functioning of the European Union

TS	Tabu Search
UDP	User Datagram Protocol
$UniBwM$	Universität der Bundeswehr München
UCL	University College London
UPC	University Politecnicà de Catalunia
UT	University of Twente
UZH	University of Zürich
VOD	Video on Demand
VN	Virtual Network
VNE	Virtual Network Embedding
VNF	Virtual Network Function
VPN	Virtual Private Network
WDM	Wavelength-Division Multiplexing

10 References

[1] V. Allee. Reconfiguring the Value Network. *Journal of Business Strategy, MCB UP Ltd*, 21(4):36–39, 2000.

[2] M. A. Alsudiari and T. Vasista. Cloud Computing and Privacy Regulations: An Exploratory Study on Issues and Implications. *Advanced Computing: An International Journal (ACIJ), AIRCC Publishing Corporation*, 3(2):159–169, 2012.

[3] M. Ananny, J. Askin, P. Aufderheide, J. B. Baker, C. Y. Baldwin, J. Balkin, et al. Attachment to ex parte letter in the matter of protecting and promoting the open internet submitted february 2, 2015 to federal communications commission. gn dkt. no. 14-28. february 2, 2015.

[4] C. Baartmans, R. V. Rijswijk Deij, E. Jeunink, and A. V. Wynsberghe. SURFnet Data Sharing Policy (DRAFT)- Legal and Ethical Guidelines Relating to Data Sharing for Research Purposes. `http://www.mymanagementguide.com/`, Accessed in September, 2015.

[5] M. Bedner. *Cloud Computing: Technik, Sicherheit und Rechtliche Gestaltung*. Forum Wirtschaftsrecht. Kassel University Press, 2013.

[6] BorsenNEWS.de. Roaming-Gebühren in Europa Fallen Weg. `http://www.boersennews.de/nachrichten/top-news/roaming-gebuehren-in-europa-fallen-weg/917292?utm_source=newsletter&utm_medium=email&utm_campaign=AdRom_51_pri_2015-MaA_Aktive_271015`. Accessed in July, 2015.

[7] Boundary Map Definition. `http://www.mymanagementguide.com/`, Accessed in September, 2014.

[8] G. Buttarelli. Security and Privacy Regulatory Challenges in the Cloud. In *Proceeding of 2012 European Cloud Computing Conference, Brussels, Belgium*, March 2012.

[9] T. Casey, T. Smura, and A. Sorri. Value Network Configurations in Wireless Local Area Access. In *IEEE 9th Conference on Telecommunications Internet and Media Techno Economics (CTTE)*, pages 1–9, Ghent, Belgium, November, 2010.

[10] H. Chang. Data Protection Regulation and Cloud Computing, A.S.Y. Cheung and R. H. Weber (eds.). In *Privacy and Legal Issues in Cloud Computing*, pages 26–42. Edward Elgar Publishing, 2015.

[11] D. Clark, J. Wroclawski, K. Sollins, and R. Braden. Tussle in Cyberspace: Defining Tomorrow's Internet. *IEEE/ACM Transactions on Networking*, 13(3):462–475, June 2005.

[12] J. E. Cohen, S. Dietrich, A. Pras, L. D. Zuck, and H. Mireille. Ethics in Data Sharing (Dagstuhl Seminar 14052). *Dagstuhl Reports*, 4(1):170–183, 2014.

[13] Computerwoche:. Internet-Verband ECO Beklagt Scheindiskussion um Schengen-Routing. `http://www.computerwoche.de/a/internet-verband-eco-beklagt-scheindiskussion-um-schengen-routing,2556658`. Accessed in July, 2015.

[14] A. Daniel, G. Sepideh, H. Jennifer, M. Gunter, P. Liam, and Y. Eric. Evaluating Goal Models Within the Goal-oriented Requirement Language. *International Journal of Intelligent Systems*, 25(8):841–877, 2010.

[15] Der Bundesrat, Schweiz. Fernmeldegesetz. https://www.admin.ch/opc/de/classified-compilation/19970160/index.html, Accessed in September, 2015.

[16] S. Dietrich, J. Van Der Ham, A. Pras, R. V. Rijswijk Deij, D. Shou, A. Sperotto, A. V. Wynsberghe, and L. D. Zuck. Ethics in Data Sharing: Developing a Model for Best Practice. In *2014 IEEE Security and Privacy Workshops (SPW)*, pages 5–9. IEEE, 2014.

[17] D. Dönni, G. S. Machado, C. Tsiaras, and B. Stiller. Schengen Routing: A Compliance Analysis. In *Intelligent Mechanisms for Network Configuration and Security, L.Steven, M. Charalambides, J. François, C. Schmitt, B.Stiller (eds.)*, volume 9122 of *Lecture Notes in Computer Science*, pages 100–112. Springer International Publishing, 2015.

[18] D. Dönni and G. S. Machado. chkroute - A Tool to Analyze Schengen Routing Compliance. http://www.csg.uzh.ch/publications/software/chkroute.html. Accessed in September, 2015.

[19] European Commission. The Open Internet and Net Neutrality in Europe, 2011.

[20] European Parliament, Council of the European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995.

[21] European Parliament, Council of the European Union. Proposal for 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), January 2012.

[22] European Union Commission. European Commission - Press Release Bringing Down Barriers in the Digital Single Market: No Roaming Charges As of June 2017. http://europa.eu/rapid/press-release_IP-15-5927_en.htm. Accessed in July, 2015.

[23] European Union Commission. The Schengen Area. http://biblio.ucv.ro/bib_web/bib_pdf/EU_books/0056.pdf. Accessed in July, 2015.

[24] European Union Commission. Consolidated Version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union*, 55(55), October 2012.

[25] European Union Court of Justice. Judgment of the Court - 6 October 2015 Schrems Case C-362/14. http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=, Last accessed in October 2015.

[26] R. Garg, B. Naudts, S. Verbrugge, and B. Stiller. Modeling Legal and Regulative Requirements for Ranking Alternatives of Cloud-based Services. In *In the Proceedings of 8th International Workshop on Requirements Engineering and Law*, pages 25–32, Ottawa, Canada, September 2015. IEEE.

[27] J. N. Hoover. Compliance in the Ether: Cloud Computing, Data Security and Business Regulation. *Journal of Business and Technology Law, HeinOnline*, 8(1):255–273, 2013.

[28] International Telecommunications Union. *Socio-economic Assessment of Future Networks by Tussle Analysis (ITU-T Recommendation Y.3013, M. Waldburger, P. Poullie, C. Schmitt, and B. Stiller (Eds.))*, August, 2014.

[29] ITU-T. Recommendation Z.151 (09/08). User Requirements Notation (URN)–Language Definition, Geneva, Switzerland, 2008.

[30] Jean-Paul Martoz. Germany Scores Against the Surveillance State. `https://cpj.org/blog/2015/08/germany-scores-against-the-surveillance-state.php`. Accessed in September, 2015.

[31] C. Kalogiros, C. Courcoubetis, G. Stamoulis, M. Dramitinos, and O. Dugeon. Socioeconomic Tussles Analysis of the ETICS Approach for Providing QoS-enabled Inter-domain Services. In *Future Network & Mobile Summit (FutureNetw), IEEE*, pages 1–8, Berlin, Germany, 2012.

[32] B. Kandukuri, V. Paturi, and A. Rakshit. Cloud Security Issues. In *Proceeding of IEEE International Conference on Services Computing (SCC '09), Bangalore, India*, pages 517–520, September 2009.

[33] J. Kerr and K. Teng. Cloud Computing: Legal and Privacy Issues. In *Proceedings of 12th Annual Academy of Business Disciplines Conference, Ft. Myers Beach, Florida, USA*, 2010.

[34] A. Kertesz and S. Varadi. Legal Aspects of Data Protection in Cloud Federations. In *Security, Privacy and Trust in Cloud Systems*, pages 433–455. Springer, 2014.

[35] J. B. Kirkwood and R. H. Lande. The Fundamental Goal of Antitrust: Protecting Consumers, Not Increasing Efficiency. *Notre Dame Law Review*, 84(1):191–244, November 2008.

[36] R. Koch, M. Golling, L. Stiemert, and G. Rodosek. Using Geolocation for the Strategic Preincident Preparation of an IT Forensics Analysis. *IEEE Systems Journal*, PP(99):1–12, February, 2015.

[37] A. Kostopoulos, I. Papafili, C. Kalogiros, T. Levä, N. Zhang, and D. Trossen. A Tussle Analysis for Information-centric Networking Architectures. In *The Future Internet: From Promises to Reality (Future Internet Assembly 2012)*, pages 6–17. Springer, Lecture Notes in Computer Science (LNCS), Heidelberg, Germany, 2012.

[38] J. Krämer, L. Wiewiorra, and C. Weinhardt. Net neutrality: A progress report. *Telecommunications Policy*, 37(9):794–813, 2013.

[39] S. Landau. Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *Security Privacy, IEEE*, 11(4):54–63, July 2013.

[40] J. Marcus, P. Nooren, J. Cave, and K. Carter. Network neutrality: Challenges and responses in the eu and in the us. *European Parliament's Committee on the Internal Market and Consumer Protection*, 2011.

[41] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi. Cloud Computing - The Business Perspective. *Decision Support Systems*, 51(1):176–189, April 2011.

[42] Maxmind. GeoLite Legacy Downloadable Databases. `http://dev.maxmind.com/geoip/legacy/geolite/`. Accessed in July, 2015.

[43] Maxmind:. GeoLite Legacy Downloadable Databases. `http://dev.maxmind.com/geoip/legacy/geolite`. Accessed in December 2014.

[44] M. Meinshausen, N. Meinshausen, W. Hare, S. C. Raper, K. Frieler, R. Knutti, D. J. Frame, and M. R. Allen. Greenhouse-Gas Emission Targets for Limiting Global Warming to 2 C. *Nature*, 458(7242):1158–1162, 2009.

[45] R. Mijumbi, J.-L. Gorricho, J. Serrat, M. Claeys, F. De Turck, and S. Latre. Design and evaluation of learning algorithms for dynamic resource management in virtual networks. In *Network Operations and Management Symposium (NOMS), 2014 IEEE*, pages 1–9, Krakow, Poland, May 2014.

[46] R. Mijumbi, J. Serrat, J. Gorricho, and R. Boutaba. A Path Generation Approach to Embedding of Virtual Networks. *IEEE Transactions on Network and Service Management*, 12(3):334–348, September 2015.

[47] R. Mijumbi, J. Serrat, J. Gorricho, N. Bouten, F. De Turck, and R. Boutaba. Network Function Virtualization: State-of-the-art and Research Challenges. *Communications Surveys Tutorials, IEEE*, PP(99):1–1, 2015.

[48] R. Mijumbi, J. Serrat, and J.-L. Gorricho. Self-managed resources in network virtualisation environments. In *IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 1099–1106, Ottawa, Canada, May 2015.

[49] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and S. Davy. Design and Evaluation of Algorithms for Mapping and Scheduling of Virtual Network Functions. In *1st IEEE Conference on Network Softwarization (NetSoft)*, pages 1–9, London, UK, April 2015.

[50] R. Mijumbi, J. Serrat, J.-L. Gorricho, J. Rubio-Loyola, and S. Davy. Server Placement and Assignment in Virtualized Radio Access Networks. In *Conference on Network and Service Management (CNSM)*, Barcelona, Spain, November 2015.

[51] R. Mijumbi, J. Serrat, J. Rubio-Loyola, N. Bouten, F. De Turck, and S. Latre. Dynamic resource management in sdn-based virtualized networks. In *10th International Conference on Network and Service Management (CNSM)*, pages 412–417, Rio De Janerio, Brazil, November 2014.

[52] J. P. Moiny. Cloud and Jurisdiction: Mind the Borders, A.S.Y. Cheung and R.H.Weber (eds.). In *Privacy And Legal Issues In Cloud Computing*, pages 118–138. Edward Elgar, 2015.

[53] Organization for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*. OECD Publishing, 2002.

[54] Rainer Hörbe. Options for Schengen Net architectures. `http://mappingtheinternet.eu/node/86`. Accessed in September 2015.

[55] F. Rambach, B. Konrad, L. Dembeck, U. Gebhard, M. Gunkel, M. Quagliotti, L. Serra, and V. López. A multilayer cost model for metro/core networks. *Journal of Optical Communications and Networking*, 5(3):210–225, 2013.

[56] Report on Stakeholders Characterization and Traffic Characteristics; SmartenIT Deliverable D1.1. I. Papafili and G. D. Stamoulis (eds.). `http://tinyurl.com/delieverableD1-1`, August 2011.

[57] RIPE Network Coordination Center. RIPE ATLAS. `http://atlas.ripe.net`. Accessed in July, 2015.

[58] J. P. Sluijs, P. Larouche, and W. Sauter. Cloud Computing in the EU Policy Sphere. *Journal of Intellectual Property, Information Technology and e-Commerce Law*, 3(1):12–32, 2011.

[59] D. N. Staiger. Cross-Border Data Flow in the Cloud between the EU and the US, A.S.Y Cheung and R.H. Weber (eds.). In *Privacy and Legal Issues in Cloud Computing*, pages 96–117. Edward Elgar, 2015.

[60] M. Tahon. *Flexibility, competitive and cooperative interactions in telecommunication networks: a model for extended techno-economic evaluation*. PhD thesis, Ghent University, 2013.

[61] The Federal Council of Switzerland. Telecommunication Act. `https://www.admin.ch/opc/en/classified-compilation/19970160/index.html`, Accessed in September, 2015.

[62] G. Y. Tian. Cloud Computing and Copyright, A.S.Y. Cheung and R.H.Weber (eds.). In *Privacy and Legal Issues in Cloud Computing*, pages 160–179. Edward Elgar, 2015.

[63] UN General Assembly. Universal Declaration Of Human Rights. `http://www.un.org/en/documents/udhr/`, 1948.

[64] M. Van der Wee, N. Vandevelde, S. Verbrugge, and M. Pickavet. Evaluation of the impact of net neutrality on the profitability of telecom operators: a game-theoretic approach. In *26th European regional conference of the International Telecommunications Society (ITS 2015)*, pages 1–19, 2015.

[65] R. H. Weber. Legal Safeguards for Cloud Computing, A.S.Y. Cheung and R.H.Weber (eds.). In *Privacy and Legal Issues in Cloud Computing*, pages 43–68. Edward Elgar, 2015.

11 Acknowledgements

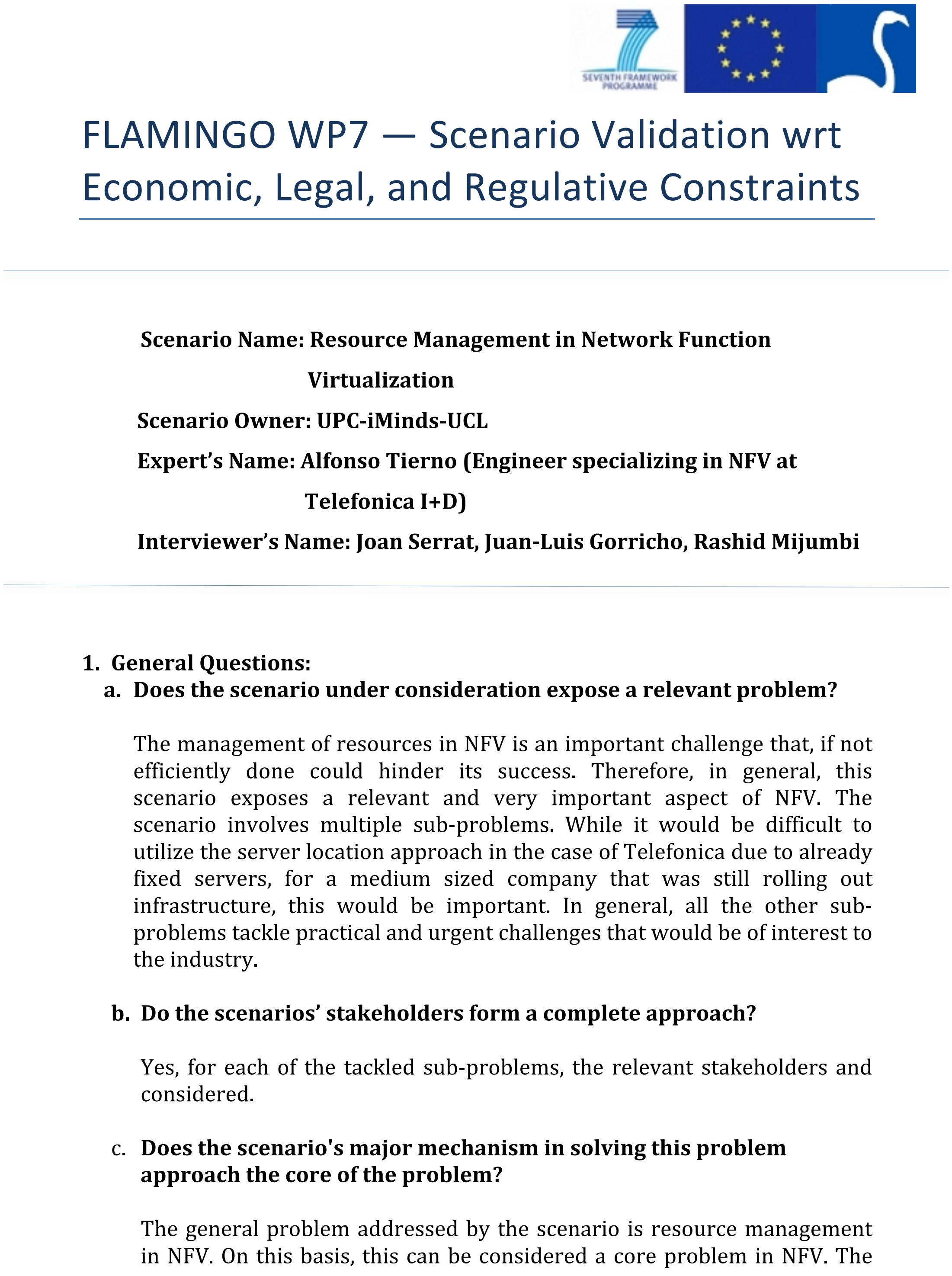
This deliverable was made possible due to the large and open help of the WP7 Partners of the FLAMINGO consortium. Also, feedback and comments from reviewers were highly valuable and enriching for the quality of deliverable. Many thanks to all of them.

12 Appendices

The interview-based validation approach was based on a general template of questionnaires, prepared by WP7 of FLAMINGO. This template consisted of four major categories of questions- (1) General Questions to identify the validity of assumptions, problem, and approach followed, (2) Scenario Specific Questions to perform in-depth analysis of scenarios with experts in terms of implementation and practicality, (3) General Recommendations to identify areas of changes and/or improvements for the scenarios, and (4) Applicability and Limitations Questions, where there relevance of scenario in real world is being discussed.

As a result, these questionnaires were used in the interview and were consequently filled off by scenario owners. This section presents all these questionnaires for the scenarios within WP7.

12.1 Resource Management in Network Function Virtualization



FLAMINGO WP7 — Scenario Validation wrt Economic, Legal, and Regulative Constraints

Scenario Name: Resource Management in Network Function Virtualization

Scenario Owner: UPC-iMinds-UCL

Expert's Name: Alfonso Tierno (Engineer specializing in NFV at Telefonica I+D)

Interviewer's Name: Joan Serrat, Juan-Luis Gorricho, Rashid Mijumbi

1. **General Questions:**
   a. **Does the scenario under consideration expose a relevant problem?**

      The management of resources in NFV is an important challenge that, if not efficiently done could hinder its success. Therefore, in general, this scenario exposes a relevant and very important aspect of NFV. The scenario involves multiple sub-problems. While it would be difficult to utilize the server location approach in the case of Telefonica due to already fixed servers, for a medium sized company that was still rolling out infrastructure, this would be important. In general, all the other sub-problems tackle practical and urgent challenges that would be of interest to the industry.

   b. **Do the scenarios' stakeholders form a complete approach?**

      Yes, for each of the tackled sub-problems, the relevant stakeholders and considered.

   c. **Does the scenario's major mechanism in solving this problem approach the core of the problem?**

      The general problem addressed by the scenario is resource management in NFV. On this basis, this can be considered a core problem in NFV. The approach taken is to divide the problem into multiple relevant sub-problems which are solved independently. As already explained, each of the sub-problems can be evaluated on its own, by as a whole, the approach is complete.

d. **Which areas impact this scenario?**

☑ Economic constraints
□ Legal constraints
☑ Regulative constraints

e. **Are the key assumptions made for this scenario realistic?**

Many of the assumptions are valid. For example, the assumption that all operators would have the flexibility to choose locations of the servers may not be valid for large operators. In addition, some considerations like being able to move functions from one virtual machine to another are, while interesting, not currently in the practice. However, the possibility to dynamically allocate resources to functions, to deploy light functions in containers rather than dedicated virtual machines are realistic.

2. **Scenario Specific Questions:**

2.a Please give us specific feedback on the importance/relevance of each of the identified sub-problems to the industry and specifically to an operator like Telefonica.

Sub-problem 1: Server location problem. Server location is usually linked to the physical buildings owned by Telefonica (old central exchanges) and/or to the location of third parties (i.e. Amazon). This means that here we have a very little flexibility to decide

Sub-problem 2: The function placement problem. This is really important because the functions placement will impact the amount of traffic to be moved through the network as well as on the delays that traffic will experience. Function placement is currently done by hand applying some logical criteria (for instance, making use of the servers which are closer to the users and so forth). On the other hand is true that an automatic mechanism able to do this placement would be welcome to avoid errors

Sub-problem 3: The scheduling of functions problem. This is something already solved in the context of the NFV. That is, the vendor that is supplying the NFV is already providing a set of concrete functions with a given performance (which depends on the number of VMs used to deploy these functions). In general the processing functions cannot be moved from one VM to another VM. In this context it would be interesting to try to solve the load balancing problem. But in general this is also done manually assuming that all the VMs have the same processing capacity (the detection that a VM has stopped working would be within sub-problem 4).

The use of VMs or dockers is something that has been argued within the industry and it depends on the adopted solution. For instance, in case of the virtualization of the CPE, where functions like DHCP, NAT, Routing are moved to the network there are two options: a) Install a VNF for each individual home or CPE. Then it is advisable to use dockers because the load will be relatively low, b) Install a VNF that serves DHCP for all the houses, another serving NAT for all the houses and so forth. In this case the load of these functions is big and we will likely need VMs. Selecting between a) or b) is something done by the network providers based on the solutions and performance provided by the NFV vendors. Hence we don't see the case to have an online solution nor the translation of functions between VMs

Sub-problem 4: Dynamic allocation. This is really a key point: the management of the lifecycle of the NFVs (this is done by the NFV manager in the ETSI model). This deals about the need that NFVs can increase/decrease (adding/removing VMs) adapting themselves to the traffic demand, rebooting in case of failure, even in another server, etc. Currently this is done assuming the worst case scenario but an automatic solution would be great. As you well say, although the physical resources have to be dimensioned for the worst case, there would be a clear advantage in energy saving

3. General recommendations to the scenario owner

Telefonica is actively involved in NFV, especially at the moment in the area of management an orchestration. On this basis, there are opportunities for collaboration between Telefonica and academia.

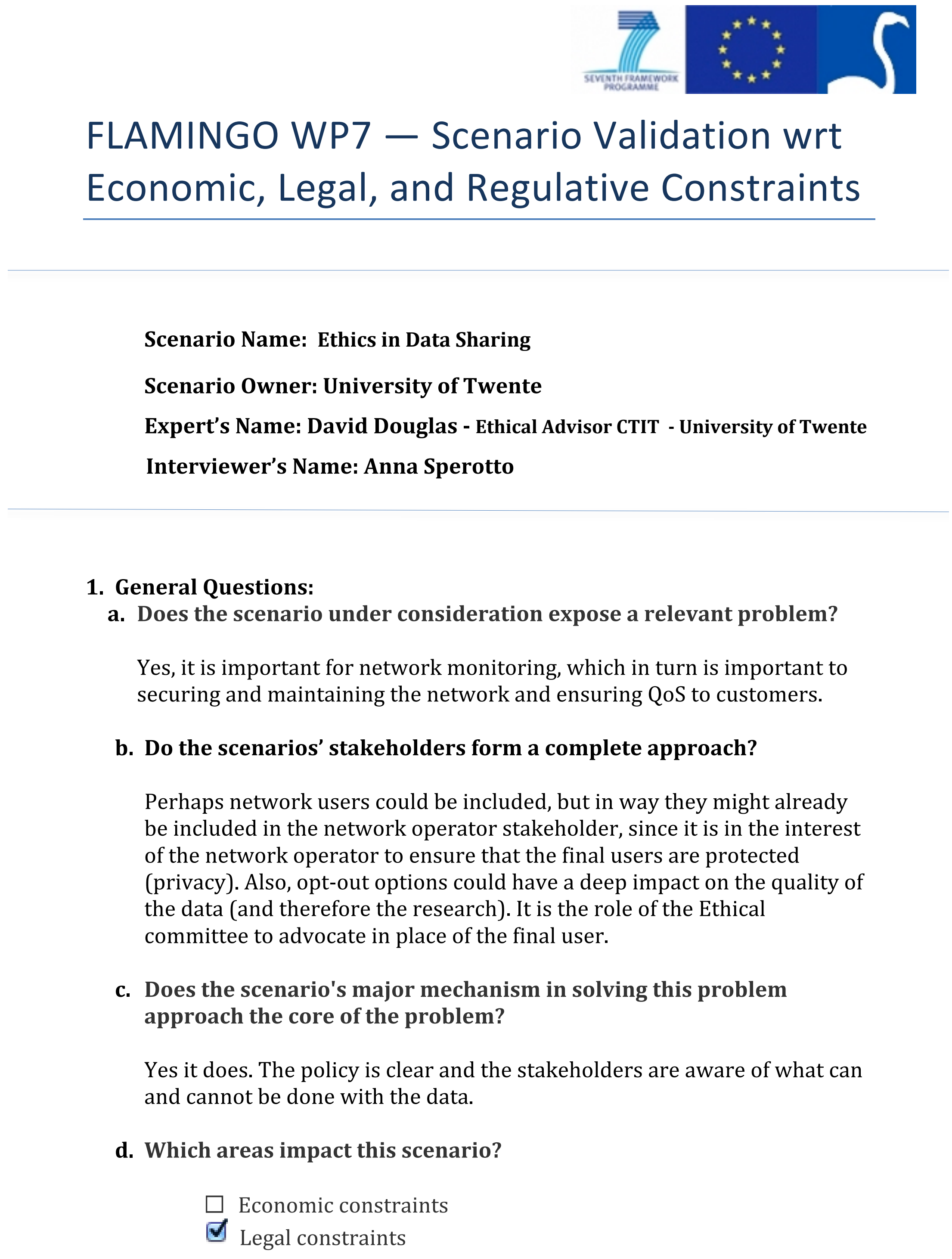
4. **Applicability of scenario in the real world**
   a. **Please tick the relevant box based on relevance**

☐ irrelevant
☐ partially irrelevant
☐ neither
☑ partially relevant
☐ relevant

b. **List of limitations (if any) with their reasons**

Some of the sub-problem formulations as described in the sub-problem specific questions.

12.2 Legal and Ethical Facets of Data Sharing



FLAMINGO WP7 — Scenario Validation wrt Economic, Legal, and Regulative Constraints

Scenario Name: Ethics in Data Sharing

Scenario Owner: University of Twente

Expert's Name: David Douglas - Ethical Advisor CTIT - University of Twente

Interviewer's Name: Anna Sperotto

1. **General Questions:**

   a. **Does the scenario under consideration expose a relevant problem?**

   Yes, it is important for network monitoring, which in turn is important to securing and maintaining the network and ensuring QoS to customers.

   b. **Do the scenarios' stakeholders form a complete approach?**

   Perhaps network users could be included, but in way they might already be included in the network operator stakeholder, since it is in the interest of the network operator to ensure that the final users are protected (privacy). Also, opt-out options could have a deep impact on the quality of the data (and therefore the research). It is the role of the Ethical committee to advocate in place of the final user.

   c. **Does the scenario's major mechanism in solving this problem approach the core of the problem?**

   Yes it does. The policy is clear and the stakeholders are aware of what can and cannot be done with the data.

   d. **Which areas impact this scenario?**

   ☐ Economic constraints
   ☑ Legal constraints

☑ Regulative constraints

e. Are the key assumptions made for this scenario realistic?

Yes, there is nothing unrealistic about it.

2. General recommendations to the scenario owner

a. Clarify how the end users interests are represented. The type of data that can be used should be better specified in the scenario description

3. Applicability of scenario in the real world

a. Please tick the relevant box based on relevance

☐ irrelevant
☐ partially irrelevant
☐ neither
☐ partially relevant
☑ relevant

b. List of limitations (if any) with their reasons

None.

12.3 Legal and Ethical Facets of Data Sharing

FLAMINGO WP7 — Scenario Validation wrt Economic, Legal, and Regulative Constraints

Scenario Name: **Legal and Ethical Facets of Data Sharing**

Scenario Owner: **Roland van Rijswijk-Dei1, Anna Sperretto,**
Burkhard Stiller

Expert's Name: **Daniel Bertolo**
(System Engineer, Team Leader Global LAN, SWITCH)
Esther Zysset
(Attorney-at-law, General Counsel, SWITCH)

Interviewers: **Burkhard Stiller, Radhika Garg**

Note: All statements made below do not bear any legal liability, neither from the interviewed nor from the interviewing persons involved. These statements made, driven by those questions prepared and originating from the constructive discussions, are documented as view points made under the current situation of network service provisioning under Swiss laws.

1. **In which sense does ethics and legal requirements (in operations) show a relevance for SWITCH as the SWISS NREN?**

   Law is considered as a codification of any such requirements, therefore, forcing the detailed discussion of ethical requirements to the back seat. There are always some discussions and considerations, but in the end it is the legal basis that is important.

2. **Did SWITCH consider ethical requirements in case of data sharing at all? If so, in which level or particular perspective?**

Policy work and guidelines, such as outlined a defined in the "SURFnet Data Sharing Policy" is an indication of an organization taking its responsibility of protecting the data seriously. This is considered very forward-looking. However, for SWITCH the board has made a decision of not sharing data with external parties. The reason for that is that SWITCH is now subject to the Telecommunication Secrecy Law owing to its status of Internet Service Provider (ISP).

3. **Which legal requirements does SWITCH have to follow in case of sharing networking data (*e.g.*, traffic management and measurement data) as of today?**

   As such the position of data collections of networking data for research purposes is not fully clear by now: If the law is interpreted in the narrowest possible way only data collections of networking data is allowed to ensure the operations, security, and efficiency of the network. If the law is applied in a broader interpretation, the efficiency term does not specify that such data can only or have to be analyzed within an ISP.
   As of today almost all customers of SWITCH are Universities or educational entities within Switzerland. Thus, all those networking data belong to the educational sector. In principle, a joint measurement effort from all networking customers can collect the same data as done within SWITCH. However, for SWITCH the decision had been taken to not share data.

4. **What are technical concerns that have to be taken care of when network data is shared with external partners?**

   Not discussed in detail. But in addition to question 3: If the data collected by all customers attached to the SWITCH network, the interactions with other Autonomous Systems (AS) can be derived.
   Furthermore, SWITCH does measure data based on the NetFlow technology for the primary purpose of security investigations and incident discovery.

5. **Which dedicated technology or functionality does SWITCH operate to (1) achieve a stable and secure network operations and (2) collect additional data (if any) on top of operational goals (*e.g.,* for longer-term traffic estimations or even research goals)?**

   For operating the network, SWITCH has internally two bifurcations in terms of responsible teams:
   1. Security Team: They store the data collected for analysis purposes. The analysis involves generating security reports, which for example

includes information such as that of malware detected or security incidents. Security analysis had also included third-parties in the past (mostly as part of research projects), who were given access to data on local premises to analyze the network behavior, for example, measures after a big link fails to function.

2. Network Team: This team is responsible for generating and collecting unsampled flow data. These data are basically used for accounting purposes, for example, maintaining data about which university generates which amounts of data sent to or received from the network. These volume information form the input to the charging approach SWITCH uses for years by now to determine network usage charges for universities and educational units throughout Switzerland.

6. **How is a privacy risk level of such networking data determined and differentiated? In which sense do current legal laws and acts apply to this case (*e.g.*, local/regional laws (Kt. Zürich), federal laws (Switzerland), and wider-range, such as data security and privacy acts (EU)? Does a risk assessment provide the right means to be adopted for a decision finding on such a sharing request?**

   As being an ISP, SWITCH has to safeguard the privacy of the user. If SWITCH does not follow the Telecommunication Secrecy Law of Switzerland the consequences can be determined in terms of "sanctions", as defined in the law. A violation of these telecommunications secrecy laws can result in the telecommunications service provider having its license suspended or revoked. It is, therefore, of utmost importance to take the necessary technical, legal, and organizational measures to preserve the secrecy as required.

7. **What are the implications of storing the respective source data, *e.g.*, size-wise, storage management-wise, access control-wise? Are aggregation and consolidation mechanisms applied on the data collected, before they are archived?**

   This question was not discussed.

8. **If the source data is allowed to be stored, (1) how is the permissible duration determined, (2) how is the potential use determined, and (3) how are possible data evaluators/interpreters selected?**

   This question was not discussed.

9. **How does the cross-border transfer of network measurement data adds to the complication of protecting the data?**
   - **d.1 In terms of sharing, storing**
   - **d.2 In terms of using and processing**
   - **d.3 In terms of destroying the data**

As far as the cross-border transfer is concerned, every measurement is done within the network of SWITCH itself and is static, since SWITCH is fully aware of how the network is connected to other ASes. As these ingress an egress points of the network are very stable over time, there is no interaction with networking peers with respect to measurement data in order to exchange that information.

The pure generation of measurement data is not considered to be a large load in this setup, however, the export of such measurement data for the highest data rate wire-speed lines currently puts a very high load onto the devices CPU. Thus, new hardware from INVEATec was ordered and will be integrated into the existing network in the next months.

An off-loading of measurement processes and data measured with a combination of sampling of networking data seems to be a technological must today for wire-speeds at about 100 Gb/s.

10. **What are special legal considerations of a Swiss NREN while sharing network data? This encompasses the operations, the optimizations, and the estimation needs of an NREN as well as the research and development – as above.**

As discussed above the Telecommunication Secrecy Law paves the legal ground for data sharing.

11. **Which technical and organizational measures the party with which such data is shared should take, in case SWITCH agrees on sharing for research purposes?**
    - **11.1 Protect the data in terms of unauthorized access.**
    - **11.2 Data is used for the right and agreed purposes.**
    - **11.3 Publication of any results, based on these data.**

This question was not discussed due to SWITCH's decision to not allow for data sharing at this stage due to a legal evaluation of their current situation and standing in the Swiss ISP sector.

12. **Which technical and organizational measures the party with which such data is shared should take, in case SWITCH agrees on sharing**

for operations (inter-connection), network optimization purposes?

This question was not discussed.

13. **In which way does such a "SURFNet Data Sharing Policy" interests and effects its operations, visibility in the international research community SWITCH?**

    As the legal decision has been made of not sharing the data with external parties a view on this type of policies is not relevant anymore, since a reversing of the board's decision is not considered a case at all. Thus, there is no use of such policies at this time.
    But if this legal decision would not have been taken, SWITCH, as an open and research platform and network service provider, would have be very much interested in identifying clear and measurable means of mitigating any risk related to data sharing.

14. **In case of interest, does the set of those policies reflect SWITCH's requirements and does it match with the underlying legal Swiss grounds?**

    This question was not discussed.

15. **If such a policy would be adopted by SWITCH, which additions, updates, or changes may be required (for legal, SWITCH-operational, or other reasons)?**

    This question was not discussed.