Evolution of mobile ecosystem for the Internet of things

Alexandr Vesselkov
Evolution of mobile ecosystem for the Internet of things

Alexandr Vesselkov

A doctoral dissertation completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Electrical Engineering, at a public examination held at the lecture hall T2 of the school on 11 June 2019 at 12.

Aalto University
School of Electrical Engineering
Department of Communications and Networking
Network Economics
Supervising professor
Professor Heikki Hämmäinen, Aalto University, Finland

Thesis advisors
Professor Heikki Hämmäinen, Aalto University, Finland
Professor Juuso Töyli, Aalto University, Finland

Preliminary examiners
Professor Hitoshi Mitomo, Waseda University, Japan
Associate Professor Morten Falch, Aalborg University, Denmark

Opponent
Associate Professor Jan Markendahl, KTH Royal Institute of Technology, Sweden
Abstract
The Internet of things (IoT) offers the mobile ecosystem new growth opportunities. In particular, the main ecosystem stakeholders, mobile network operators (MNOs) and mobile platform providers (MPPs; e.g., Apple and Google), can grow their customer base and product portfolio. To realize these opportunities, stakeholders must evolve their current technologies and services to suit the requirements of new IoT devices and customer groups. Such developments may cause considerable and uncertain changes to the mobile ecosystem. Ecosystem stakeholders must understand and prepare for such changes to ensure future growth.

This thesis investigates the evolution of the mobile ecosystem for IoT. To gain a more comprehensive understanding, the thesis considers ecosystem changes relevant from the perspective of two key stakeholders – MNOs and MPPs. First, the main changes from the viewpoint of MNOs are analyzed. Namely, the use of mobile IoT across industries is explored to understand the new customer types of MNOs. Then, changes that Embedded SIM (eSIM), a potentially disruptive IoT technology for remote SIM management, may cause to the ecosystem are scrutinized.

Further, the main ecosystem changes from the viewpoint of MPPs are examined. First, the thesis considers a new sub-ecosystem emerging around platforms for sharing data in the consumer IoT domain. Specifically, the governance of collaboration and competition in such sub-ecosystems is studied on the example of mobile health field. Next, given the interest of large MPPs in mobile health, the thesis analyzes the feasibility of MPPs expanding their services to the highly regulated healthcare industry.

Several diverse methods are adopted in the research. For example, exploratory data analysis is utilized to examine the use of mobile IoT, and value network analysis is used to investigate structural ecosystem changes due to eSIM. Data is drawn from diverse sources, including interviews, web sources, patents, press releases, and traffic measurements in a mobile network.

In terms of the manifold results, a few are highlighted. The analysis demonstrates that mobile IoT traffic patterns significantly differ from handsets and across industries. Further, the study shows that the extent of ecosystem changes brought by eSIM could range from insignificant to disruptive depending on the value network of the eSIM service and its diffusion. In particular, if eSIM is also used in smartphones and dynamic multihoming is broadly adopted, competition and service provisioning will fundamentally transform. Furthermore, the analysis determines the key design and governance decisions that MPPs can use as mechanisms for managing competition with new complementors in mobile health platforms. Finally, the study shows that MPPs can act as health data aggregators that connect unregulated consumer and regulated medical domains of the healthcare ecosystem thereby taking a central ecosystem position.

Keywords Mobile IoT, embedded SIM, data sharing, wearables, mobile health, consumer IoT

ISSN (printed) 1799-4934 ISSN (pdf) 1799-4942
Location of publisher Helsinki Location of printing Helsinki Year 2019
Pages 199

Preface

I want to express my gratitude to a number of people who supported me along this long journey. First of all, I would like to thank my supervisor Professor Heikki Hämmäinen for sharing his vast knowledge and experience, and for his belief in my abilities. Without Heikki’s guidance and encouragement, the completion of this thesis would not have been possible. I am also extremely grateful to Professor Juuso Töyli for actively advising my thesis, giving practical suggestions, and providing very detailed feedback.

I owe special gratitude to the preliminary examiners of my thesis, Professor Hitoshi Mitomo and Associate Professor Morten Falch, for their insightful comments and suggestions to improve this work. Further, I would like to thank Associate Professor Jan Markendahl for the honor of accepting to be my opponent.

Apart from my supervisor and advisor, I have been lucky to work together with other excellent researchers, particularly, Pertti Ikäläinen, Arturo Basaure, and Benjamin Finley, who I want to thank for our fruitful collaborations that have resulted in foundational for this thesis publications. Furthermore, I would like to extend my gratitude to other so far unmentioned current and former members of our Network Economics team. Jaspreet Walia, Jaume Benseny, Kalevi Kilkki, Manohar Reddy, Oliver Landertshamer, Pekka Kekolahti, Antti Riiokonen, Michail Katsigiannis, Nan Zhang, Tapio Soikkeli, Saimanoj Katta, Levent Kartal, and Joonas Lindh – our lunch and coffee break discussions made the thesis process so much more enjoyable!

This thesis has been funded by the Internet of Things and Digital Disruption of Industry projects. I want to thank all colleagues and funders of these projects. Also, I very much appreciate the financial support that I received from the Doctoral School of ELEC and HPY Research Foundation. I further wish to thank all the people of Comnet for creating a positive work environment. I must also thank all interviewed experts for contributing to this thesis with their valuable insights.

Furthermore, I am extremely grateful to my friends. Arsen and Anya, Anar, Abir, Faraz, Prashant, Rashmi, and Tanya – I am thankful for all the great time we spent together that gave me the energy to complete this project.

Last but not least, I wish to thank my family, particularly, my parents, Sergey and Yelena, as well as my brother, grandparents, and aunts. Your support, which I have always felt despite the thousands of kilometers that separate us, helped me to reach this milestone.

Espoo, May 3rd, 2019,

Alexandr Vesselkov
Contents

Preface ........................................................................................................ 1
List of abbreviations .................................................................................. 5
List of publications .................................................................................... 7
Author’s contribution ................................................................................ 9
1. Introduction .................................................................................. 11
   1.1 Background ................................................................................ 11
   1.2 Research questions .................................................................... 13
   1.3 Research scope .......................................................................... 14
   1.4 Definitions ................................................................................. 14
   1.5 Thesis structure ......................................................................... 15
2. Background ................................................................................... 16
   2.1 Business ecosystem ................................................................... 16
   2.1.1 Ecosystem and value network ................................................... 16
   2.1.2 Evolution of business ecosystem ............................................... 17
   2.2 Past evolution of the mobile ecosystem .................................... 18
   2.3 The evolution of mobile network operators for IoT .................. 19
   2.3.1 New customers and traffic patterns ....................................... 19
   2.3.2 New radio technologies and embedded SIM ......................... 21
   2.4 The evolution of mobile platform providers for IoT ............... 22
   2.4.1 Data platforms: design and governance .............................. 22
   2.4.2 Mobile health and consumer IoT in healthcare .................. 24
3. Research design and methods ..................................................... 27
   3.1 Research approach ................................................................... 27
   3.2 Research data ........................................................................... 29
   3.3 Research methods ..................................................................... 30
   3.3.1 Methods for understanding the past and present ............... 30
   3.3.2 Methods for uncovering the future ...................................... 34
4. Evolution of mobile network operators for IoT ......................... 37
   4.1 New customer base and usage patterns ................................. 37
List of abbreviations

2G 2nd Generation
3GPP 3rd Generation Partnership Project
5G 5th Generation
ABM Agent-based modeling
AI Artificial intelligence
API Application programming interface
AS Administrative and support industry
B2B Business-to-business
B2C Business-to-consumer
CDR Call detail records
CP Content provider
DEV Developer
DWT Discrete wavelet transform
ECDF Empirical cumulative distribution function
EC-GSM-IoT Extended coverage GSM IoT
EG Electricity and gas industry
EHR Electronic health record
eSIM Embedded SIM
eUICC Embedded UICC
GSM Global System for Mobile Communications
GSMA GSM Association
HW Hardware
IC Information and communication industry
ICT Information and communications technology
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSI</td>
<td>International mobile subscriber identity</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of things</td>
</tr>
<tr>
<td>LTE</td>
<td>Long term evolution</td>
</tr>
<tr>
<td>LTE-M</td>
<td>Long term evolution - machine type communications</td>
</tr>
<tr>
<td>M(V)NO</td>
<td>Mobile (virtual) network operator, includes MNO and MVNO</td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile device manufacturer</td>
</tr>
<tr>
<td>MF</td>
<td>Manufacturing industry</td>
</tr>
<tr>
<td>mHealth</td>
<td>Mobile health</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile network operator</td>
</tr>
<tr>
<td>MPP</td>
<td>Mobile platform provider</td>
</tr>
<tr>
<td>NACE</td>
<td>Nomenclature generale des Activites economiques dans les Communautes europeennes (Statistical Classification of Economic Activities in the European Community)</td>
</tr>
<tr>
<td>NB-IoT</td>
<td>Narrowband IoT</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OEM</td>
<td>Original equipment manufacturer</td>
</tr>
<tr>
<td>OS</td>
<td>Operating system</td>
</tr>
<tr>
<td>PA</td>
<td>Professional activities industry</td>
</tr>
<tr>
<td>PP</td>
<td>Platform providers</td>
</tr>
<tr>
<td>RQ</td>
<td>Research question</td>
</tr>
<tr>
<td>RSM</td>
<td>Remote subscription management, Remote SIM management</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber identity module</td>
</tr>
<tr>
<td>SM</td>
<td>Subscription manager</td>
</tr>
<tr>
<td>SM-DP</td>
<td>Subscription manager for data preparation</td>
</tr>
<tr>
<td>SM-SR</td>
<td>Subscription manager for secure routing</td>
</tr>
<tr>
<td>SP</td>
<td>Service provider</td>
</tr>
<tr>
<td>TAC</td>
<td>Type allocation code</td>
</tr>
<tr>
<td>TR</td>
<td>Transportation industry</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal integrated circuit card</td>
</tr>
<tr>
<td>VNC</td>
<td>Value network configuration</td>
</tr>
<tr>
<td>WR</td>
<td>Wholesale and retail trade industry</td>
</tr>
</tbody>
</table>
List of publications

This doctoral dissertation consists of an overview and of the following publications, which are referred to in the text by their Roman numerals


Author’s contribution

**Publication I:** “Cellular IoT Traffic Characterization and Evolution”

Finley prepared data for the analysis. Finley and Vesselkov formed the idea, performed the analysis, and wrote the paper.

**Publication II:** “Value networks of embedded SIM-based remote subscription management”

Vesselkov, Hämmäinen, and Ikäläinen formed the idea for the paper. Vesselkov constructed the value networks and wrote the paper. Hämmäinen and Ikäläinen edited the text.

**Publication III:** “Multihoming with Dynamic Mobile Network Selection: Possible Scenarios and Impact on Competition”

Vesselkov, Hämmäinen, and Töyli formed the idea, constructed models and scenarios. Vesselkov conducted the interviews and wrote the paper. Hämmäinen and Töyli edited the text.

**Publication IV:** “Design and governance of mHealth data sharing”

Vesselkov formed the idea, collected the data, conducted interviews and wrote the paper. Hämmäinen and Töyli provided comments on the analysis and edited the text.

**Publication V:** “Internet of things (IoT) platform competition: consumer switching versus provider multihoming”

Basaure and Vesselkov formed the idea. Basaure designed the model, run the simulations, and wrote most of the paper. Vesselkov supported the modeling, wrote Sections 2.5 and 2.6, commented other sections, and edited the text. Töyli provided comments on the analysis and edited the text.

**Publication VI:** “Technology and Value Network Evolution in Telehealth”

Vesselkov, Hämmäinen, and Töyli formed the idea. Vesselkov collected the data and wrote the paper. Hämmäinen and Töyli provided comments on the analysis and edited the text.
1. Introduction

1.1 Background

The Internet of things (IoT) will bring connectivity to billions of devices, enabling the ubiquitous sensing of the physical world and thereby facilitating new products and services, improving efficiency, and cutting costs. IoT has the potential to change virtually every industry, from healthcare and education to manufacturing and logistics. The potential economic impact of IoT may reach $11 trillion by 2025 (Manyika et al., 2015), whereas the market for IoT devices and services is expected to grow to $520 billion by 2021 (Bosche et al., 2018). Therefore, the increasing activity of major ICT companies in the IoT domain is not surprising. Particularly in the mobile ecosystem, IoT is viewed as a critical factor for future growth (Deloitte, 2018) and the next stage of evolution, which will require extending primarily smartphone and human-centric services to various industrial devices and markets.

The main stakeholders of the mobile ecosystem, namely, mobile network operators (MNOs) and mobile platform providers (MPPs; e.g., Apple and Google), already operate in the IoT field. For example, in OECD countries, MNOs already serve on average about 16 mobile IoT devices per 100 inhabitants (OECD, 2017). Furthermore, the operating systems of Apple and Google, the two largest MPPs, run on about 27% of 124.9 million wearable IoT devices shipped in 2018 (IDC, 2018). Although existing assets have allowed MNOs and MPPs to enter the IoT market, in order to efficiently address emerging customer and industry requirements, they must improve their technologies and products. Technological developments, in turn, can change the business ecosystem by creating new business roles, which can attract new actors and require new business relations between stakeholders. Furthermore, such evolution of the ecosystem may also change the nature of collaboration and competition between stakeholders. Understanding potential changes in the mobile ecosystem is, then, essential for the sustainability and growth of the stakeholders and the ecosystem as a whole. However, while technological developments in IoT are well addressed by researchers, little academic attention has been paid to the business ecosystem evolution that inevitably accompanies such developments.

This thesis analyzes the evolution of the mobile ecosystem for IoT by adopting the perspectives of two main ecosystem stakeholders – MNOs and MPPs, who follow different paths toward IoT. Namely, while MNOs mainly address industrial IoT applications, such as asset tracking and fleet management, MPPs mostly target consumer IoT applications, such as mobile health and smart home. Therefore, taking these two complementary viewpoints allows the uncovering of different aspects of the mobile ecosystem evolution and thus enables a more comprehensive understanding.
Main aspects of ecosystem evolution from the perspective of mobile network operators

From the perspective of MNOs, one of the main changes in the mobile ecosystem expanding toward IoT is an evolving customer base. Indeed, while in 2010 the share of machine-type devices among mobile subscriptions globally was 1.4% (Kechiche et al., 2014), by 2025 it is expected to grow to 26% (GSMA, 2018). Such growth shows that cellular networks will have to accommodate an increasing number of devices used for various purposes in various industries, which may have different requirements, and generate new types of traffic patterns. Despite the pressing need to prepare for this change, only a few studies have empirically analyzed IoT traffic to better understand the use of mobile IoT communications (Marjamaa, 2012; Romirer-Maierhofer et al., 2015; Shafiq et al., 2012). These studies, however, did not investigate the differences in service usage between various customer groups or industries, which indicates the need for further research.

Although the lack of empirical research hinders the understanding of mobile IoT customer requirements, IoT devices have common constraints that are well understood and addressed by emerging mobile technologies. Some such technologies do not affect the mobile ecosystem significantly. For example, the recently developed narrowband cellular IoT technologies (3GPP, 2016) that are being rolled out by MNOs around the world (GSMA, 2019), assume that the mobile service provisioning will continue as usual. On the other hand, the business impact of embedded SIM (eSIM), a technology developed for remote SIM provisioning for IoT devices, may be more significant (Meukel et al., 2016). Specifically, eSIM may deprive MNOs of SIM ownership, decrease consumer switching costs, and lead to a change in power distribution in the ecosystem. Furthermore, eSIM introduces several new technological components and business roles, which could be distributed between existing and new actors in different ways, creating uncertainty. Hence, eSIM is a potentially disruptive technology, which could considerably change the mobile ecosystem, with consequences for competition. Despite this potential, the possible implementation scenarios and impacts of eSIM have not been analyzed, which may be one of the reasons for the relatively slow adoption of this technology.

Main aspects of ecosystem evolution from the perspective of mobile platform providers

For MPPs, a move into the IoT domain implies bringing new products, namely, wearable and smart home devices along with the related operating systems, to the established customer groups. However, this development does not in itself change the mobile ecosystem, because the stakeholders and relationships between them remain the same. On the other hand, MPPs can develop a platform connecting consumer IoT devices and data from different producers, laying a foundation for a new sub-ecosystem of device producers, service providers, and app developers, which would signify a more considerable change in the broader mobile ecosystem. Indeed, consumer IoT data is typically stored in vendor-specific silos, which prevents exploiting data complementarities. Maximizing the value of IoT requires creating a platform that would enable data exchange between devices of different producers as well as data sharing with third-party complementors, facilitating device interoperability and enabling the development of data-based apps and services. MPPs are well-positioned to develop such a platform and become leaders of a sub-ecosystem around it. In fact, in 2014, two such platforms for data sharing were introduced by the two largest MPPs Apple and Google in the mobile health (mHealth) domain.

Growing and sustaining a new ecosystem around IoT data platforms is challenging and requires correct design and governance decisions (Schreieck et al., 2016). These decisions, on the
one hand, must motivate complementors to join the platform by providing the means and freedom to innovate, but on the other hand, must dictate rules to ensure efficient value creation and capture. Apart from the governance of platform complementors, the governance or regulation of inter-platform relationships is of utmost importance in consumer IoT data sharing because it affects competition and may in some cases lead to monopoly. However, the governance of relationships with complementors and competitors in data platforms in general, and in consumer IoT data sharing platforms in particular, has not been sufficiently addressed in the literature likely due to the novelty of such platforms.

Although initially MPPs addressed consumer IoT domains, namely, wearables and smart home, later they may move to adjacent industries, such as healthcare and smart city. Thus, the attempts of MPPs to establish a platform for mHealth data and a sub-ecosystem around it can be viewed as the first steps of MPPs toward participating in the healthcare industry. In fact, Apple and Google are already actively developing their healthcare-related capabilities and products (Comstock, 2018; Muoio, 2018). However, the future acceptance of such technologies and products by the heavily regulated healthcare industry remains uncertain. Thus, academic business literature largely considers mobile health and traditional healthcare domains separately. Hence, the potential position of MPPs and other companies from the consumer domain in the ecosystem of regulated healthcare remain unclear, complicating the strategic planning of such companies, and making the future evolution of the industry uncertain.

1.2 Research questions

To address the identified research gaps and facilitate the evolution of the mobile ecosystem for the IoT this study examines the following high-level research problem:

How might the advent of IoT change service provisioning, collaboration, and competition in the mobile ecosystem?

This thesis focuses on the two main stakeholders of the mobile ecosystem – MNOs and MPPs and addresses the issues most relevant for them in the evolution of service provisioning, collaboration, and competition. The research problem is addressed by answering the four individual research questions listed below. The first two questions concern the ecosystem changes that are primarily relevant for MNOs, whereas the last two questions are mainly relevant for MPPs. The evolution of MPPs for IoT (RQ3, RQ4) is studied on the example of mobile health (mHealth) because it is one of the earliest and most advanced IoT verticals in terms of, e.g., the penetration of wearable and digital health devices (Cisco, 2017) and the number of application developers (research2guidance, 2017).

**RQ1.** How do mobile IoT usage patterns differ from consumer devices and across industries?

**RQ2.** How could embedded SIM technology affect the mobile ecosystem?

**RQ3.** How could collaboration and competition be governed in emerging consumer IoT data platforms and particularly mobile health data platforms?

**RQ4.** How could mobile platform providers acting as mobile health data platform providers position themselves in the ecosystem of the healthcare industry?

The research publications partially address different aspects of the research questions as Table 1.1 shows.
Table 1.1. Relationship between publications and research questions

<table>
<thead>
<tr>
<th>Pub.</th>
<th>Pub. Title</th>
<th>RQ1</th>
<th>RQ2</th>
<th>RQ3</th>
<th>RQ4</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Cellular IoT Traffic Characterization and Evolution</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>II</td>
<td>Value networks of embedded SIM-based remote subscription management</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III</td>
<td>Multihoming with Dynamic Mobile Network Selection: Possible Scenarios and Impact on Competition</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>Design and governance of mHealth data sharing</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>V</td>
<td>Internet of things (IoT) platform competition: consumer switching versus provider multihoming</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VI</td>
<td>Technology and value network evolution in telehealth</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

1.3 Research scope

The scope of this thesis is limited to profound changes in the mobile ecosystem that will arise in short to medium term due to the proliferation of IoT and key ecosystem stakeholders, namely, MNOs and MPPs, extending their operations to IoT. Therefore, answering the stated research questions will help to fill the gaps identified in Section 1.1, whereas other less significant and more distant in time ecosystem changes related to IoT are left beyond the scope of this thesis. For example, as mentioned, although the introduction of low-power narrowband 3GPP IoT technologies is a significant change from a technology viewpoint, their business ecosystem impact will likely be minimal, thus excluding them from the thesis scope. Furthermore, this thesis does not consider some potentially important ecosystem changes facilitated by technologies that have been developed after the commencement of the research (e.g., 5G).

The thesis focuses on mobile health (mHealth) as a case IoT domain for analyzing the move of MPPs into consumer IoT and related changes in the mobile ecosystem. Mobile health was selected over other consumer IoT verticals, such as smart home and connected cars, because mHealth is an early and advanced industry (Cisco, 2017; research2guidance, 2017). Moreover, the largest MPPs Apple and Google showed their interest in mHealth vertical already in the early stages of their IoT journey by introducing operating systems for wearable devices and platforms for integrating and sharing mHealth data.

Finally, the thesis analyzes a potential move of MPPs into the healthcare industry, which may further expand the mobile ecosystem. As discussed in Section 1.1, this direction of development is challenging but already actively explored by MPPs, which motivated its research in this thesis.

1.4 Definitions

The main terms used in this thesis are defined as follows:

*Business ecosystem* is an economic community formed around a product or service that consists of simultaneously collaborating and competing interconnected stakeholders – suppliers, producers, complementors, end users, competitors, and other actors (Peltoniemi and Vuori, 2004) (see Section 2.1).

*Embedded SIM* is a specification for remotely and locally reprogrammable SIM (subscriber identification module) card, which enables changing a mobile operator without changing a hardware element (SIM).

*Evolution* is a gradual development of a technology, product, or value network from simple to a more advanced state.
Internet of things (IoT) is a network of Internet-connected physical objects, which can interact with each other, humans, systems, and environment without active human involvement.

Mobile ecosystem is a business ecosystem that delivers mobile products and services. The mobile ecosystem includes mobile network operators, mobile platform providers, mobile device manufacturers and other stakeholders (see Section 2.2).

Mobile platform is a software development and marketplace environment enabling the design and distribution of third-party applications for mobile devices, namely, smartphones and tablets. A mobile platform is a multi-sided platform, which connects end users with third-party developers and potentially other stakeholders (device manufacturers, advertisers).

Mobile platform provider is a stakeholder (an actor) of the mobile ecosystem that provides a mobile platform and potentially takes other business roles.

Mobile IoT relates to IoT devices, networks, and services that use cellular 3GPP radio access networks.

Mobile health (mHealth) is a field that makes use of mobile applications (including IoT applications) and devices for achieving health targets (Olla and Shimskey, 2015).

Platform in this study refers to a multi-sided platform, an intermediary that enables direct interactions between several types of users, which provide each other with network benefits (Hagiu and Wright, 2015).

Telehealth is a remote healthcare delivery mode that makes use of ICT technologies (World Health Organization, 2010).

Value network is as a set of interconnected business actors that collaborate for creating the economic value in the form of products or services (Casey et al., 2010) (see Section 2.1).

1.5 Thesis structure

The remaining thesis is structured as follows. Chapter 2 provides background information, reviews the related literature, and articulates research gaps. Chapter 3 presents the research approach, data, and methods used. Chapter 4 and 5 report the research results on the evolution of MNOs and MPPs for IoT. Finally, Chapter 6 summarizes and discusses the results, presents limitations and directions for future work.
2. Background

This chapter presents background information to provide the context for the results discussed further in this thesis. First, the concept of a business ecosystem is defined. Then, the historical evolution of the mobile ecosystem is shortly described. After that, literature related to the evolution of MNOs and MPPs for IoT is reviewed to indicate the gaps that motivated the research questions presented in Section 1.2.

2.1 Business ecosystem

2.1.1 Ecosystem and value network

A business ecosystem was first defined as an economic community of suppliers, producers, competitors, customers, and other stakeholders, which coevolve in roles and capabilities and align themselves with the directions set by dominant ecosystem companies (Moore, 1996), which are also referred to as keystones (Iansiti and Levien, 2004). Definitions of a business ecosystem typically highlight the interconnectedness of stakeholders and their interdependence for survival and success (Iansiti and Levien, 2004; Peltoniemi and Vuori, 2004). Business ecosystems often emerge around multi-sided platforms – an intermediary that enables direct interactions between several types of users, which provide each other with network benefits (Hagiu and Wright, 2015). Such ecosystems, sometimes referred to as “platform ecosystems,” typically include a platform provider, which acts as the ecosystem keystone, end users, complementors - application developers or service providers, and a platform sponsor, which is often combined with the platform provider role (Eisenmann et al., 2008).

The idea of a business ecosystem is closely related to the concept of a value network, which can be defined as a set of interconnected business actors that collaborate for creating the economic value in the form of products or services (Casey et al., 2010). While business ecosystems include both collaborators and competitors, value networks typically focus on collaboration (Peltoniemi, 2004). Moreover, unlike value networks, which are geographically bounded, business ecosystems reject the role of geography due to their digital nature. Furthermore, the decision-making in value networks is more centralized than in business ecosystems, where keystone players often cannot fully dictate the terms of collaboration (Peltoniemi, 2004). Finally, the two terms differ in their application domains: while business ecosystems are usually discussed in the context of digital economy and Internet (Kandiah and Gossain, 1998), value networks are often viewed in the context of traditional industries.

In this thesis, both the business ecosystem and value network terms are used. Relying on the definition of Casey et al. (2010) that relates value networks to particular products or services, and given the view of a business ecosystem as a combination of value networks (Rong et al.,
2018), a business ecosystem is considered as a broader concept describing an industry where stakeholders collaborate and compete. In turn, value networks are used to describe the subset of a business ecosystem, where actors collaborate on a particular product or service.

2.1.2 Evolution of business ecosystem

On a high level, the evolution of a business ecosystem can be viewed through the stages of its lifecycle - birth, expansion, leadership, and self-renewal (Moore, 1993). External factors, such as socio-economic environment and technological progress, significantly influence the evolution of an ecosystem. However, sometimes ecosystem development is viewed as primarily driven by internal factors, particularly, co-evolution of stakeholders (Mäkinen and Dedehayir, 2012). Such co-evolution is mostly steered by keystone players, who, for example, can change the platform around which the ecosystem is organized, thereby affecting other stakeholders (Iansiti and Levien, 2004). Due to such a critical role of a platform, the ecosystem evolution can be discussed in terms of platform evolution.

Based on the literature review, Staykova and Damsgaard (2017) identified the views taken on platform evolution research and divided them into two groups: platform evolution as a continuum and as standalone issues. In the first group, particular attention is often paid to the expansion stage of the platform ecosystem lifecycle (e.g., Casey and Töyli, 2012; Zhu and Iansiti, 2012), when platforms’ survival depends on the ability to reach a critical mass of different types of users (Evans and Schmalensee, 2010). Platform evolution has also been viewed as the transformation from one-sided to the multi-sided platform (e.g., Tan et al., 2015) through attracting new stakeholder types. Furthermore, platform evolution has been broadly examined as the reconfiguration of various platform attributes, such as architecture, governance, environment (Tiwana et al., 2010), and underlying technologies (Tan et al., 2016). The views on platform evolution as standalone issues (Staykova and Damsgaard, 2017) include the evolution of the platform boundary, which is typically related to the introduction of new features (Um and Yoo, 2016) or platform envelopment (Eisenmann et al., 2011).

Based on Staykova and Damsgaard (2017), four main interrelated ways of business ecosystem evolution can be distinguished. First, ecosystem boundaries may change, for example, due to the introduction of new features or removal of old ones; or due to business growth – providing a new product or entering a new market, which can be viewed as product and market development strategies, respectively (Ansoff, 1957). With this kind of evolution, new business roles can emerge, or existing ones disappear, potentially attracting new groups of stakeholders to the ecosystem or causing the exit of existing ones. Second, the ecosystem may change structurally within old boundaries. For example, new business interfaces can appear between stakeholders, or business roles can be redistributed between stakeholders. Third, the business ecosystem can evolve through the reconfiguration of platform and ecosystem attributes, for example, new platform governance policies or a new technology creating novel affordances. This type of evolution can lead, for instance, to the redistribution of roles between stakeholders, that is, to structural ecosystem evolution. Finally, the ecosystem can change in size, that is, in the number of participants. This type of development often follows other types of evolution and therefore can be viewed as the evolution outcome (Staykova and Damsgaard, 2017).
2.2 Past evolution of the mobile ecosystem

To understand the boundaries of the mobile ecosystem, existing studies were examined to identify actors that researchers viewed as the ecosystem stakeholders. The related existing studies were defined using the “mobile ecosystem” term in a keyword search on titles, abstracts, and keywords in the Scopus database. Out of 167 results, 50 most cited papers were reviewed, along with 45 recent papers that were published in 2017-2018. Due to the overlap, 92 papers were considered. Out of these studies, most did not define the ecosystem stakeholders because, for example, they viewed the ecosystem as a context rather than an object of study, or used the term in other than business meaning. Table 2.1 shows the stakeholders that were acknowledged in 12 most relevant studies on the mobile business ecosystem. The most commonly considered by researchers stakeholders are a (mobile) platform provider (MPP, 12 studies), a mobile device manufacturer (MDM, 10 studies), a mobile network operator (MNO, 10 studies), an application developer (DEV, 10 studies), and a content provider (CP, 8 studies).

Table 2.1. Stakeholders considered in mobile ecosystem studies

<table>
<thead>
<tr>
<th>Paper</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Basole, 2009)</td>
<td>CP, DEV, MDM, MNO, MPP; system integrators, service &amp; billing providers, network &amp; infrastructure providers, silicon vendors &amp; other component providers, media &amp; entertainment providers, photography &amp; digital imaging, cable providers, gaming providers, internet service providers</td>
</tr>
<tr>
<td>(Xia et al., 2010)</td>
<td>CP, DEV, MDM, MNO, MPP</td>
</tr>
<tr>
<td>(Basole and Karla, 2011)</td>
<td>DEV, MDM, MNO, MPP</td>
</tr>
<tr>
<td>(Müller et al., 2011)</td>
<td>CP, DEV, MDM, MNO, MPP; end users, payment broker, ad broker, marketplace engineer, testing &amp; verification party, signing party</td>
</tr>
<tr>
<td>(Gueguen and Isckia, 2011)</td>
<td>CP, DEV, MDM, MNO</td>
</tr>
<tr>
<td>(Hyrünsalmi et al., 2014)</td>
<td>DEV, MPP</td>
</tr>
<tr>
<td>(Karhu et al., 2014)</td>
<td>CP, DEV, MDM, MNO, MPP; ad service provider</td>
</tr>
<tr>
<td>(Oh et al., 2015)</td>
<td>DEV, MPP (MNO and MDM)</td>
</tr>
<tr>
<td>(Gao and Krogstie, 2015)</td>
<td>CP, DEV, MDM, MNO, MPP; regulators, end users</td>
</tr>
<tr>
<td>(Lee et al., 2016)</td>
<td>DEV, MDM, MNO, MPP; network &amp; infrastructure providers, internet service providers</td>
</tr>
<tr>
<td>(Suh and Lee, 2017)</td>
<td>CP, DEV, MDM, MNO, MPP; silicon vendors &amp; component providers, media service providers, internet service providers</td>
</tr>
<tr>
<td>(Nieborg and Helmond, 2018)</td>
<td>CP, MPP; end users, advertisers, and “others”</td>
</tr>
</tbody>
</table>

Surprisingly, the main stakeholders of the mobile ecosystem have not significantly changed since the early mobile ecosystem studies1 (Basole and Karla, 2011; Xia et al., 2010). However, the function and ownership of mobile platforms have considerably evolved. Namely, in the early stages of the mobile ecosystem development, platforms (or portals) were provided by MNOs and acted as a gateway to mobile content and services (Oh et al., 2015; Yamakami, 2010), with NTT DoCoMo’s i-mode being a prominent example. However, with the evolution of mobile devices and the diffusion of Apple’s iOS and Google’s Android in the early 2010s, the mobile ecosystem platform started to refer to an operating system, usually combined with a related application store (Gueguen and Isckia, 2011; Xia et al., 2010). Consequently, the role of MNOs in the mobile ecosystem has significantly decreased (Basole and Karla, 2011), while OS providers started to lead the ecosystem (Oh et al., 2015).

1 Basole (2009) was the first to bring the term “mobile ecosystem” into wide use, therefore it can be viewed as the first mobile ecosystem study.
Figure 2.1 and 2.2 respectively show the simplified architecture of the mobile ecosystem in the MNO-led and mobile OS provider-led periods. Given that the largest mobile OS providers Apple and Google also produce mobile devices, Figure 2.2 shows that the roles of MPP and MDM can be combined. However, not all MDMs provide platforms as Figure 2.2 suggests by a connection (a business relationship) between the MPP and MDM.

**Figure 2.1.** MNO-led mobile ecosystem

**Figure 2.2.** Mobile OS provider-led mobile ecosystem

### 2.3 The evolution of mobile network operators for IoT

For MNOs, a move into the IoT domain primarily means bringing an existing product, mobile connectivity, to new markets, various industries, rather than the traditional consumer domain. Therefore, from the viewpoint of MNOs, the main evolving part in the mobile ecosystem is *customers*, as MNOs will increasingly serve “things” rather than humans and operate in B2B rather than B2C mode. New customers will further set new requirements for the service, which is currently optimized for human traffic (Palattella et al., 2016; Pötsch et al., 2013). This will demand MNOs to engage in the development of new technologies. While some of such required technological developments are incremental from the ecosystem evolution viewpoint, some are significant, because they involve new business roles, which may attract new stakeholders and compromise a dominant position of MNOs as connectivity providers.

#### 2.3.1 New customers and traffic patterns

The share of IoT will increase to 26% of total mobile connections by 2025 (GSMA, 2018). Due to the global coverage and high reliability of 3GPP mobile networks, cellular mobile connectiv-
ity is adopted across different IoT applications and industries (Shafiq et al., 2013). Such a diversity of use cases and verticals leads to the generation of heterogeneous IoT traffic differing in the volume, regularity of transmission, and mobility (Maeder et al., 2011; Shafiq et al., 2013). MNOs need to understand these differences to efficiently meet the requirements of new customers. Surprisingly, despite the significant penetration of mobile IoT in many developed countries (OECD, 2017), only a few studies have analyzed the use of mobile IoT empirically based on the data from an operating mobile network.

Real traffic generated by cellular IoT devices was first investigated by Shafiq et al. (2013)\(^2\), who analyzed a week-long data captured in August 2010 in a tier-1 US mobile network. They divided all IoT devices into six groups based on the application and compared their generated traffic along different parameters, including temporal patterns, composition (uplink vs. downlink), and periodicity of communications. They further contrasted the IoT traffic with smartphone traffic. The results showed the heterogeneity of IoT device traffic patterns and significant difference between IoT and smartphones. For example, IoT devices appeared to be less mobile and exhibit more synchronized traffic patterns than smartphones, and unlike smartphones generate more uplink than downlink traffic. IoT traffic composition was further studied by Romirer-Maierhofer et al. (2015), who confirmed the prevalence of uplink traffic. They also analyzed the patterns of the signaling traffic of IoT devices and found that it is burstier than the traffic that smartphones generate.

Furthermore, Andrade et al. (2017) analyzed traffic patterns of a million connected cars in a cellular network in the US and found that such traffic differs both from smartphones and other IoT devices, particularly, in high mobility and short data sessions. They further concluded that the large-scale over-the-air updates of car firmware could seriously harm network performance. Moreover, Kolamunna et al. (2018) took the first look on SIM-enabled wearable devices, namely smartwatches, and analyzed their traffic and usage patterns based on seven-month-long data from a large European MNO. The authors found that only 34% users of SIM-enabled wearables generate any network traffic, although such users are more active in terms of mobility, data consumption, and app usage than users that do not own a SIM-enabled wearable device.

Finally, mobile IoT device traffic was analyzed by the group of Austrian researchers (Baer et al., 2016, 2015; Laner et al., 2014), who, however, did not explore traffic profiles, but proposed methods for the detection of IoT devices that are more efficient than TAC-based (type allocation code) approach commonly used by MNOs.

Although several studies have examined mobile IoT traffic, they relied on relatively short data, which prevented the analysis of temporal trends on a longer timescale, and focused on particular types of IoT devices, such as connected cars or smartwatches. Furthermore, some of the results may have become outdated due to the fast development of IoT, with new applications and devices emerging rapidly. Finally, although Shafiq et al. (2013) compared the traffic patterns of different IoT applications, no previous studies have analyzed the use of mobile IoT across industries, although MNOs can benefit from such knowledge because it improves the understanding of the requirements and challenges posed by new IoT customers. These research gaps motivated RQ1 that have been addressed by the empirical study of the mobile IoT use across industries presented in Pub. I and summarized in Section 4.1.

\(^2\) Authors referred to IoT as machine-to-machine (M2M)
2.3.2 New radio technologies and embedded SIM

The proliferation of mobile IoT requires MNOs to develop new technologies and services that would address the challenges of serving IoT devices in the networks historically optimized for human traffic (Palattella et al., 2016; Pötsch et al., 2013). Indeed, existing cellular technologies were designed for high-data speed, while common requirements for IoT communications are low rate, low power consumption, low cost, and support for a massive number of devices (e.g., Guibene et al., 2015; Ratasuk et al., 2015). To satisfy these requirements, 3GPP (The 3rd Generation Partnership Project) developed several low-power wide-area radio technology standards (3GPP, 2016) - Narrowband IoT (NB-IoT), LTE-M (LTE for machine type communication), and EC-GSM-IoT (Extended coverage GSM IoT), with the first two technologies being actively deployed around the world (GSMA, 2019). Both NB-IoT and LTE-M are designed for low bandwidth, low power, and low-cost devices. However, unlike LTE-M, which is an enhancement of LTE, NB-IoT is a new technology that relies on the subset of the LTE standard and therefore may require higher deployment investments. Furthermore, NB-IoT can provide higher coverage and support more connections per cell than LTE-M, whereas LTE-M allows higher data rates and better mobility support (Chen et al., 2017). Future 5G networks can further expand the support for IoT communications, as they are expected to provide not only enhanced broadband rates but also ultra-reliable, low latency, and massive machine type communications (Li et al., 2018). However, unlike NB-IoT and LTE-M, as of the beginning of 2019, 5G networks have not yet been deployed.

Although new radio technologies may be viewed as the most important technical development of MNOs for IoT, they do not change the business aspects of the service provisioning and mobile ecosystem in general. On the other hand, embedded SIM (eSIM) technology for remote SIM management (RSM) may introduce significant business and ecosystem-related changes. RSM is one of the components of the “low cost” requirement for efficient mobile IoT communications. Indeed, IoT devices need a SIM card for obtaining access to the network, and due to the wide and remote device deployment, changing an MNO can constitute a significant cost because it traditionally requires a physical switch of SIM cards. Embedded SIM specifications developed by GSMA (GSMA, 2016) are expected to address this issue by enabling RSM. However, although the specifications have long been available, the deployment of eSIM has remained relatively low, with non-removable SIM shipments estimated at only 108.9 million in 2016, around 2% of total SIM shipments (Tait, 2017). This can be due to the uncertainties related to the value networks of eSIM-based RSM provisioning and MNOs’ concerns about potential negative business impacts of eSIM (EY, 2015). Surprisingly, although a potentially significant impact of eSIM on the mobile ecosystem has been recognized (Dhall and Jha, 2018; Meukel et al., 2016), it seems that only one academic study, namely, Bender and Lehmann (2012), has investigated the business aspects of eSIM. The authors presented business processes for eSIM-based RSM. They defined eight main actors participating in RSM: service provider, OEM, communication module manufacturer, eSIM supplier, subscription manager, MNO (including an initial home MNO), retailer, and end customer. Although the authors described potential business processes in detail, they focused on one out of many possible implementation scenarios. Furthermore, they did not examine the potential impacts of eSIM on competition in the mobile ecosystem. Such a lack of studies on potentially disruptive eSIM motivated the research of its possible value networks and competitive implications (RQ2) presented in Pub. II and III and summarized in Section 4.2.
2.4 The evolution of mobile platform providers for IoT

Unlike MNOs, which moved into the IoT domain through a new market development, MPPs entered IoT using a product development strategy. Thus, they offered to the existing customer groups (consumers and developers) new IoT products, namely, wearable and smart home devices, along with the related OSs. This study will focus on the wearables track of the IoT evolution of MPPs because wearables can pave the way to the healthcare industry (Feiner, 2019), and thereby offer considerable market opportunities. Furthermore, mHealth is the early and advanced IoT vertical, which guarantees the availability of research data.

The introduction of wearable OSs has not significantly affected the mobile ecosystem because the MPPs Apple and Google extended their smartphone strategies to wearable devices, with Apple offering integrated hardware and OS, and Google focusing on the OS. Therefore, all customers of new platforms – end users, application developers, and device manufacturers – remained nearly the same. However, a new “sub-system” (Valkokari, 2015) or “sub-ecosystem” (Heikkilä and Kuivaniemi, 2012) started to emerge around the data that wearables generate. Most wearables are continuously worn on the skin surface, and therefore can be used for measuring physiological parameters (Metcalf et al., 2016) and generating fitness, wellness, health, and disease-related data, also referred to as mobile health (mHealth) data (Shaw et al., 2016). However, such mHealth data is often generated by different devices and applications and managed by different service providers. Such fragmentation prevents benefiting from data complementarities, therefore reducing the value of that data (Chen et al., 2012; Dimitrov, 2016). Hence, data sharing platforms started to emerge that enable consented sharing of end users’ mHealth data with third-party developers (Grundy et al., 2017). In 2014, Apple and Google entered the mHealth data sharing domain by introducing Health³ and Fit⁴ platforms respectively. The platforms are intended to facilitate data sharing and gather fragmented mHealth data in a single hub. Such a new type of platforms marks a change in the mobile ecosystem by creating a “sub-ecosystem” of a new type of complementors - data-based app developers and service providers.

Establishing an ecosystem of mHealth data sharing and becoming a hub for mHealth data can be viewed as the first step of MPPs toward participating in the healthcare industry. Thus, they can start targeting doctors as a new type of platform users and establish technical interfaces between the platform and medical information systems (Comstock, 2014). This development can be considered as diversification to the healthcare industry through the market development strategy. From the mobile ecosystem perspective, the move of MPPs to the healthcare can be viewed as the expansion of ecosystem boundaries.

2.4.1 Data platforms: design and governance

Sharing wearable device data enables customers to use the applications of third-party developers with the data generated by their wearable devices. Such data sharing is potentially beneficial for data consumers (third-party developers), providers (wearable producers), and their joint end users. In mHealth, data is often shared by providing to third parties a web application programming interface (API) to the data repository (research2guidance, 2016). External APIs drive the product “platformization” (Helmond, 2015) – the process of turning a non-platform

---

3 https://developer.apple.com/healthkit/

4 https://developers.google.com/fit/
good into a platform (Patel, 2015). However, for the platform to generate value for end users, platform providers must create and sustain the network of third-party complementors (e.g., Eisenmann et al., 2006) – data-based application developers and service providers. This, in turn, requires making careful platform design and governance decisions (Schreieck et al., 2016) that would attract complementors and manage their use of the platform.

Therefore, platform design, on the one hand, should motivate complementors to join the platform by providing means and freedom to innovate. In other words, platform providers must facilitate platform generativity, which defines how easily complementors can leverage a platform for application development (Zittrain, 2008). On the other hand, platform design must impose rules to ensure the efficient value creation and capture. Therefore, platform providers must maintain a tradeoff between the platform generativity and control, which represents one of the key challenges of the platform design and governance (Constantinides et al., 2018; Eaton et al., 2011; Förderer et al., 2014; Tiwana et al., 2010; Yoo et al., 2012). Recently, boundary resources were formalized as the means of addressing this tradeoff (Ghazawneh and Henfridsson, 2013) and maintaining relations with complementors. Boundary resources are defined as “the software tools and regulations that serve as the interface for the arm’s-length relationship between the platform owner and the application developer” (Ghazawneh and Henfridsson, 2013, p. 175). They play a two-fold role of platform resourcing and securing (Ghazawneh and Henfridsson, 2013), and mainly include APIs and developer support documentation (Dal Bianco et al., 2014).

Despite the importance of platform design and governance for managing the complementors’ use of the platform, related literature is scarce and fragmented (Manner et al., 2013; Tiwana et al., 2010). Ghazawneh and Henfridsson (2013) applied their developed boundary resource model for analyzing how Apple governed its application platform at different stages of ecosystem evolution. Eaton et al. (2015) similarly focused on the case of the Apple platform for analyzing the impact of complementors on the change of platform boundary resources and therefore on the platform governance. Hein et al. (2016) examined the governance of four different types of platforms – social network (Facebook), merchant (Alibaba), service platform (Uber and Airbnb) and application platform (Google Play Store and Apple App Store). They analyzed the cases along seven dimensions of platform governance defined from the literature, including governance structure, accessibility and control, and business models. However, despite the attempt to correct the researchers’ bias toward Apple’s and Google’s mobile application platforms, Hein et al. (2016) did not examine an increasingly pervasive data sharing platform type. Therefore, seemingly no previous studies have analyzed the design and governance of data sharing platforms, which are different from previously studied types of platforms in the kind of shared resource and platform architecture (“Access API” platforms in data sharing vs. “Runtime Environment API” in mobile application development, following the classification of Andreessen (2007)). Furthermore, data sharing platforms in mHealth also differ from the commonly analyzed platforms in the sensitivity of shared data, and a higher risk of platform providers competing with complementors because providers often act as application developers. The last factor further complicates the maintenance of generativity and control. The research gap in the design and governance of data platforms and particularly mHealth data platforms partially motivated RQ3, which is addressed in Pub. IV and summarized in Section 5.1.1.

The governance of platform complementors is essential for separate platforms; however, on a market level, the governance (or regulation) of inter-platform relations is of utmost importance. Because of the lack of interoperability, which can be achieved by coopetition - the
collaboration of competitors (e.g., Ritala, 2012), IoT data is often locked in vertical silos (Chen et al., 2014; Desai et al., 2015) hindering the development of applications based on cross-industry data. Moreover, often there is also no interoperability within separate IoT vertical markets (e.g., de Arriba-Pérez et al., 2016), because device producers use proprietary standards and data formats. The lack of interoperability may lead to end users’ lock-in to the platform, which in turn can reduce competition (Klemperer, 1987). On the other hand, in markets with network effects, under some circumstances, high switching costs can increase competition (Chen, 2016; Lam, 2017; Suleymanova and Wey, 2011). Therefore, in the presence of network effects, the competitive impact of interoperability and consequent reduction in switching costs remains unclear. However, despite this controversy, just a few studies have analyzed the collective impact of network effects and switching costs on competition (Chen, 2016). Furthermore, only one study (Ruutu et al., 2017) has addressed the impact of interoperability on the competition between data platforms. The authors simulated the competitive impact of two policies related to the interoperability. Namely, they analyzed the effect of data transferability (portability), which decreases end users’ switching cost, and open interfaces, which enable easier service providers’ multihoming. However, they did not consider the switching cost of service providers, as well as device-related switching costs of end users. Moreover, when analyzing the impact of open interfaces, they did not test various extents of interface harmonization. Therefore, to fill these gaps and contribute to the limited literature on the interoperability in data platforms, and particularly in consumer IoT data platforms, an agent-based simulation was conducted. Results of the simulation are reported in Pub. V and summarized in Section 5.1.2.

2.4.2 Mobile health and consumer IoT in healthcare

There is a growing body of literature related to the role of mHealth and consumer IoT in healthcare. However, most of the studies are published in the medical domain, where the usefulness, effectiveness, and safety of wearables and mHealth apps are analyzed (Lupton, 2014; North and Chaudhry, 2016). Furthermore, the research on technical aspects of mHealth use in healthcare is extensive, focusing on, e.g., platform design (Gay and Leijddekkers, 2015) and integration to medical information systems (Electronic Health Records - EHR) (e.g., Genes et al., 2018; Kumar et al., 2016). However, business literature on the position of mHealth in healthcare is scarce. Particularly, despite the ambitions of Apple to become a major player in healthcare (Feiner, 2019), no studies seem to have examined a possible impact of mHealth service providers on the architecture of healthcare industry and their potential role in the heavily regulated healthcare industry.

Laya et al. (2018) analyzed four IoT-based wellness and social care services to identify the impact of IoT on their network-level business models. They sketched the value networks of the case services but did not explain the position of IoT providers in the broader ecosystem of healthcare. Value network patterns of mHealth services were further analyzed by Huq (2016) and Farshchian & Vilarinho (2017), who similarly did not examine the role of mHealth providers in traditional healthcare. On the contrary, Acheampong and Vimarlund (2015) in their analysis of business models in telemedicine took the viewpoint of the regulated healthcare domain and did not acknowledge the impact of proliferating IoT and mHealth. Thus, business literature often seems to consider consumer-side mHealth and traditional healthcare industries separately, despite the recognized benefits that mHealth can bring to healthcare (e.g., Piwek et al., 2016).
The potential impact of large IoT and mHealth players on healthcare could be better understood by analyzing their activities in the industry. Thus, in 2014, Apple tested sharing mHealth data from their Health platform with healthcare providers who used medical information systems produced by Epic. However, mHealth data was transferred to Epic’s patient portal rather than EHR, the data transmission could be initiated only by healthcare providers, and it was further unidirectional, without a possibility to pull the data from the medical systems (Olschesky, 2014). In 2018, Apple launched a personal health record (PHR) feature for iPhones, which enabled the aggregation of patient-generated health data from the Health platform with the data pulled from medical EHR systems of selected hospitals (Comstock, 2018). Furthermore, in 2017-2018, Apple acquired several companies in the digital health domain, hired healthcare experts and doctors, participated in medical studies (Comstock, 2017), and added a medically certified ECG (Electrocardiography) function to its smartwatch (Comstock, 2018).

Google has been similarly active in the healthcare domain. However, unlike Apple, which seemingly intends to become a health data hub, Google mainly focuses on artificial intelligence, wearable devices, and non-invasive medical sensors (Lovett, 2019; Muoio, 2018), while its data platform Fit seems to retain its initial fitness focus.

Overall, no studies seem to have clarified whether and how traditionally operating in consumer domain MPPs can position themselves in the regulated healthcare domain. Such lack of research complicates strategic planning and may slow the industry development. Therefore, this research gap motivated RQ4 that is addressed in Pub. VI and summarized in Section 5.2.
3. Research design and methods

This thesis uses a combination of multiple research approaches and methods based on the suitability for a concrete research question. This chapter introduces the research approaches, data, and methods used in this thesis.

3.1 Research approach

March and Smith (1995) broadly divide research approaches in Information Technology into two groups: natural and design science. Natural science approaches focus on studying natural phenomena and understanding the reality, whereas design science, first defined by Simon (1997), addresses human-made (as opposed to natural) artifacts. Design science includes two main research activities: building new artifacts to serve certain purposes and evaluating existing artifacts. Similarly, two natural science activities are distinguished: the discovery and formulation of new theories (theorizing) and justification of existing scientific claims, which can be roughly mapped to inductive and deductive research, respectively.

![Figure 3.1. Taxonomy of research approaches (Järvinen, 2000). Modified by highlighting approaches used in this research.](image-url)
The framework of March and Smith (1995) was extended by Järvinen (2000), who developed a research taxonomy that defines six research approaches (Figure 3.1). The taxonomy, designed in a top-down manner, first divides all approaches into mathematical (focusing on proving theorems) and the ones studying reality. The latter group of approaches is further divided into the ones stressing what is reality and the ones stressing the utility of artifacts, roughly corresponding respectively to the natural and design science of March and Smith (1995). The approaches stressing what is reality are divided into conceptual-analytical that build a theory, model, or framework for explaining the reality based on the assumptions or previous studies, and approaches for data-driven empirical studies that are further split into theory-testing and theory-creating. Finally, approaches stressing the utility of artifacts are divided into artifact-building and artifact-evaluating.

Table 3.1 summarizes research approaches taken in the research publications of this thesis. Pub. I stresses what is reality and follows a theory-creating approach, empirically studying the traffic of IoT devices in a Finnish mobile network and making observations on the difference in the IoT use across industries. The analysis in Pub. II-IV and VI can be described as artifact-building, with artifacts being value networks in Pub. II, system dynamics models in Pub. III, a framework for the design and governance of mHealth data sharing in Pub. IV, and trends along with value networks in Pub. VI. On the other hand, Pub. II, III, and VI can also be categorized as artifact-evaluating. Particularly, Pub. II and III evaluate the impact of eSIM technology on the mobile ecosystem, and Pub. VI analyzes the historical evolution of the telehealth industry and the position of IoT within it. Finally, Pub. V evaluates the impact of different regulatory policies on competition among consumer IoT data platforms, and therefore its research approach can be categorized as artifact-evaluating.

**Table 3.1. Summary of research approaches, methods, and data used in publications**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Analyze the use of mobile IoT over time and across industries to understand the needs of IoT customers</td>
<td>Theory-creating</td>
<td>Descriptive statistics; clustering</td>
<td>CDR (call detail records) from the network of a major Finnish MNO</td>
</tr>
<tr>
<td>II</td>
<td>Construct value network configurations (VNCs) of eSIM-based remote subscription management service to clarify possible futures and ecosystem impact of eSIM</td>
<td>Artifact-building, artifact-evaluating</td>
<td>Value network configuration (VNC) analysis</td>
<td>GSMA eSIM specifications</td>
</tr>
<tr>
<td>III</td>
<td>Construct scenarios for potential competitive impacts of eSIM multihoming to clarify possible futures</td>
<td>Artifact-building, artifact-evaluating</td>
<td>Qualitative system dynamics</td>
<td>Transcripts of 13 expert interviews</td>
</tr>
<tr>
<td>IV</td>
<td>Analyze data sharing in mHealth. Construct a framework to facilitate the design and governance of data sharing platforms in consumer IoT</td>
<td>Artifact-building</td>
<td>Analysis of qualitative web-based data (content analysis)</td>
<td>Boundary resource docs; app usage experiments; transcripts of 5 expert interviews</td>
</tr>
<tr>
<td>V</td>
<td>Evaluate a competitive impact of various interoperability policies on the ecosystem of consumer IoT data platforms to inform policymaking</td>
<td>Artifact-evaluating</td>
<td>Agent-based modelling</td>
<td>Literature</td>
</tr>
<tr>
<td>VI</td>
<td>Analyze the past and potential future evolution of technology and value network in telehealth to understand the role of IoT and mHealth and to clarify possible futures</td>
<td>Artifact-building, artifact-evaluating</td>
<td>Multi-layer quantitative literature analysis; literature review; VNC analysis</td>
<td>Research publications, patents, press releases</td>
</tr>
</tbody>
</table>
3.2 Research data

Variety of research data that could be divided into qualitative and quantitative were used in this study (Table 3.1). Pub. I analyzed quantitative data, Pub. II, III, and V relied on qualitative data, whereas Pub. IV and VI used mixed data, i.e., both qualitative and quantitative. Academic and industry literature has been a foundation for all research publications, and therefore it is not explicitly mentioned in Table 3.1, except for the cases when literature was the only source, as in Pub. V, where the model assumptions were formulated based on the existing studies.

Pub. I used two-year long data (September 2016 – August 2018) of all call detail records (CDR) of IoT devices from the network of a large Finnish mobile operator to analyze the use of mobile IoT. IoT devices were selected for the dataset based on the subscription type, and therefore, IoT devices that use non-IoT subscriptions were not included. Each data record contained the following information: anonymized IMSI (international mobile subscriber identity), device TAC (type allocation code), anonymized cell ID, customer company ID, uplink and downlink traffic volumes aggregated for each hour. In case if a device moved from one cell to another during an hour, additional records were created for each new cell ID. Furthermore, two other datasets were used: the one mapping company ID to an industry according to Finnish TOL2008 classification, which is based on European classification NACE Rev. 2 (Eurostat, 2008), and the one mapping TACs to device models and features. The main dataset contained tens of millions of records, which covered hundreds of companies and hundreds of thousands of IoT devices.

Pub. II extensively used eSIM specifications of GSMA (GSMA, 2016, 2017) for building a technical architecture of remote subscription management.

Pub. IV primarily relied on the analysis of web-based data (Romano Jr. et al., 2003). First, 37 most actively participating in mHealth data sharing apps and services were identified based on the previous study of Grundy et al. (2017) and app usage experiments. After that, boundary resource documentation of 21 apps and services\(^5\) that provided a platform were analyzed. The data selection is detailed in Section 3 of Pub. IV.

Pub. VI analyzed three different types of literature – research publications, patents, and press releases in quantitative (e.g., keywords frequency analysis) and qualitative (i.e., literature survey) manners. Research publications and press releases for the analysis were selected using iterative keyword search in Scopus and ABI/INFORM databases, respectively, whereas patents were derived from the database of United States Patent and Trademark Office (USPTO) by selecting all patents belonging to two relevant patent classes (subgroups). Detailed description of data collection is found in Section 2 of Pub. VI.

Pub. III and IV relied on the data from expert interviews, which were mostly conducted in a semi-structured manner, transcribed, and checked with interviewees for ensuring a common understanding. In Pub. III, 13 experts from different stakeholder groups were interviewed. Four of the interviewed experts worked for a communications regulatory authority, two – for an MNO, broadcaster, and research institution (six in total), one – for a SIM manufacturer, device manufacturer, and ministry of transport and communications (three in total). Experts representing MPPs, and other SIM and mobile device manufacturers were not interviewed because of their unavailability in Finland. The number of interviews was not pre-set. Instead, interviews were arranged while they still generated sufficient new knowledge. The lack of MPPs, SIM producers, and mobile device manufacturers among the interviewed experts was

\(^5\) One of the selected apps had two APIs; therefore, 22 sets of boundary resource documentation were analyzed
partially compensated by examining publicly available web documents (e.g., press releases and white papers) to gain the understanding of these stakeholders’ vision on the future of eSIM.

InPub. IV, five expert interviews were conducted to support the study, namely, to verify general research setup and refine the analysis results of boundary resource documents collected on the web. Two of the interviewees were API and platform experts from wearable device manufacturing companies, whereas three others did not work in the mHealth domain, but had expertise in consumer and medical devices, as well as APIs. The interviewees were selected among accessible experts with the relevant background using convenience sampling. The role of the interviews in the study was not central but supporting, and therefore only five experts were interviewed, which did not include representatives of MPPs and some other potentially relevant stakeholder groups (e.g., mHealth app developers).

3.3 Research methods

This thesis analyzes the evolution of the mobile ecosystem for IoT, with a particular focus on main ecosystem stakeholders – mobile network operators (MNOs) and mobile platform providers (MPPs). Uncovering and preparing for the future is an essential task of a strategic planner. However, foreseeing the future requires a clear understanding and the analysis of the past developments and the present state. Therefore, the methods employed in this research can be broadly divided into the ones for understanding the past and present and the ones for uncovering the future (Table 3.2), although some of them are suitable for both purposes. The methods used are further described in Sections 3.3.1 and 3.3.2.

Table 3.2. Research methods used

<table>
<thead>
<tr>
<th>Ecosystem stakeholder</th>
<th>Aspect of ecosystem evolution</th>
<th>Methods used for understanding the past and present</th>
<th>Methods used for uncovering the future</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNOs</td>
<td>New customers and traffic patterns</td>
<td>Quantitative data analysis (descriptive, clustering; Pub. I)</td>
<td>/Left for future studies: e.g., forecasting based on traffic profiles from Pub. I/</td>
</tr>
<tr>
<td></td>
<td>Emergence and diffusion of eSIM</td>
<td>Literature</td>
<td>Value network configuration (VNC) (Pub. II); Qualitative system dynamics (Pub. III)</td>
</tr>
<tr>
<td>MPPs</td>
<td>Emergence of consumer IoT data sharing sub-ecosystem</td>
<td>Analysis of web-based qualitative data (Pub. IV)</td>
<td>Agent-based modelling (Pub. V)</td>
</tr>
<tr>
<td>Entering regulated healthcare industry</td>
<td>Multi-layer quantitative and qualitative analysis of literature (Pub. VI)</td>
<td>VNC (Pub. VI)</td>
<td></td>
</tr>
</tbody>
</table>

3.3.1 Methods for understanding the past and present

Quantitative data analysis

Pub. I uses quantitative data analysis to characterize the usage of mobile IoT across industries and thereby address RQ1. The choice of quantitative methods was in part motivated by the availability of a dataset suitable for the analysis. Although the scope and depth of quantitative research are limited by the coverage and quality of the dataset, the quantitative analysis of pre-collected data is faster and often provides wider research space coverage, which make it more suitable for exploratory studies compared with qualitative approaches that typically involve unscalable manual data collection. Furthermore, since RQ1 aims to study mobile IoT usage patterns to gain an understanding of new customers that MNOs will serve in the IoT age, the
analysis of the dataset collected from an operating mobile network in Finland, an advanced in mobile services country, is well-suited for addressing RQ1.

Apart from descriptive data analysis, the methodology for which is self-evident, a temporal analysis of IoT traffic was conducted in Pub. I using periodograms and temporal clustering. Periodogram is a common method of finding periodic patterns in time series. Apart from its ubiquity, the use of periodograms was also motivated by the previous related study (Shafiq et al., 2013). Periodograms provide an estimate of the spectral density of a time series as the square of the modulus of the discrete Fourier transform. In practice, periodograms were computed using the \textit{periodogram} function in \texttt{scipy.signal} Python library.

Temporal clustering was used for defining temporal traffic profiles. For performing a temporal clustering, time series were averaged over a month and normalized over the 24-hour series so that the value for a given hour represented the fraction of device traffic at that hour. Further, time series were transformed using a discrete wavelet transform (DWT) with a Daubechies-1 wavelet and a decomposition level of 3. DWT was selected because it allows multi-level decomposition of time series and because of the relatively fast performance of wavelet-based clustering (Chaovalit et al., 2011). Furthermore, the previous related study of Shafiq et al. (2013) similarly used DWT with a Daubechies-1 wavelet and a decomposition level of 3. After obtaining DWT coefficients, they were clustered using bisecting k-means, with the optimal number of clusters chosen based on the silhouette score. The choice of bisecting k-means was motivated by its lower computational complexity ($O(n)$) compared with other methods, such as hierarchical clustering with ward linkage ($O(n^2)$) that was used by Shafiq et al. (2013). Furthermore, unlike some other methods, bisecting k-means can be computationally distributed. Practically, \texttt{PyWavelets} library in Python was used for DWT, while the clustering was performed in Spark (\texttt{pyspark}) using \texttt{pyspark.ml.clustering} library.

\textbf{Analysis of web-based qualitative data}

Web-based materials comprise a rich and accessible data source for studying online services. Unlike other qualitative data (e.g., collected through research interviews), web-based data is more accessible, and its collection is more scalable. Therefore, data obtained from the open web sources was the primary research data in multiple ICT ecosystem studies (e.g., Eaton et al., 2015; Ghazawneh and Henfridsson, 2013; Karhu, 2016).

Web-based data can be studied using many qualitative data analysis method. Although in practice the methods used for analyzing such data in the ICT ecosystem are often tailored for particular needs research (e.g., Eaton et al., 2015; Ghazawneh and Henfridsson, 2013; Karhu, 2016), they typically follow similar steps that can be formalized using the methodology of Romano Jr. et al. (2003): elicitation, reduction, and visualization. \textit{Elicitation} step covers qualitative data collection and formatting; \textit{reduction} step consists of the \textit{selection} of initial categories or codes, followed by \textit{coding} - an iterative update of initially selected codes based on the data, leading to the generation of final code scheme and coded text, and \textit{clustering} - assigning final codes to the text. Finally, the \textit{visualization} step involves data display in, e.g., tabular or graphical formats.

Motivated by the richness and easy accessibility of web-based qualitative data, as well as its wide use in ICT ecosystem research, Pub. IV employed the above-described process for analyzing collected on the web documents on the boundary resources of mHealth data sharing platforms. Boundary resources, as discussed in Section 2.4.1, are the tools that platform providers use for governing the platform. Therefore, the analysis of boundary resources can help to partially address RQ3. Figure 3.2 details the approach used for the analysis. This approach can
also be viewed as inductive content analysis, a commonly used method for classifying written or spoken materials into categories (e.g., Cho and Lee, 2014). After the case platforms were selected and documents were collected (elicitation), the research proceeded with data reduction that started with the open coding of API references (selection), that is, attaching concepts to the observed data for developing codes that accurately describe or classify the studied phenomenon (Flock, 2009). When coding the following documents (coding), new codes were added to the coding scheme if the existing ones were not suitable. After the initial coding, codes were revised, and data was categorized using the developed codes (clustering). First, API references were coded, and after that API license agreements. Next, the cases were tabulated using code labels (API characteristics) as columns, case APIs as rows, and the values of characteristics as cells. The resulting table enabled cross-case analysis, after which only those code labels (characteristics) were selected that were different for at least two cases, which allowed formalizing them as design and governance decisions. After that, final decisions were formatted as a table (visualization), categorized, and elaborated based on the data. Finally, at different stages, the analysis was supported by expert interviews, as Figure 3.2 shows.

Figure 3.2. Web-based data analysis approach used in Pub. IV (adapted from Pub. IV)

Multi-layer quantitative analysis of literature

Review of academic literature is one of the most common ways of “analyzing the past to prepare for the future” (Webster and Watson, 2002). However, such analysis is inherently limited in scope, as it only allows understanding the scientific progress and interests of the research community, which do not necessarily coincide with the interests of business organizations that drive the industry development. To focus on the technological interests of companies, invention patents can be analyzed. Indeed, since creating and filing a patent entail costs, to be patented inventions must be viewed as potentially useful for future products, and therefore patents can be used for tracking technologies that were considered important by organizations employing the patent inventors. Following this logic, the growing amount of technology management literature analyzes patents to understand technological trends (e.g., Joung and Kim, 2017; Karvonen and Kässi, 2011). However, not all patents are eventually used in products, and
therefore understanding the industry evolution in terms of technologies that found real applications requires another data source, such as press releases of new product launches. Although press releases have been analyzed only in a few academic studies, such as Benbunan-Fich and Altschuller (2005), and Bonilla and Rao (2015), they constitute a unique source of timely industry-related information.

Technological evolution of an industry can be studied at different layers using different information sources. However, to gain a holistic understanding, several data sources must be analyzed. Therefore, inspired by the model of Kilikki et al. (2018), Pub. VI proposed a research framework that suggests uncovering a potential future industry architecture by studying the technological development of an industry on three layers – scientific research, inventions, and products, using three corresponding data sources – research publications, patents, and press releases (Figure 3.3). A large number of available documents of these types, as well as the structured format of the metadata of scientific papers and patents, facilitate their quantitative analysis. Unlike qualitative literature review, quantitative research methods are more scalable and enable covering a larger number of documents.

The multi-level literature analysis in Pub. VI addresses the evolution of telehealth, ICT-based remote mode of healthcare service delivery (World Health Organization, 2010), and helps to identify its trends that allow estimating the position of MPPs in future telehealth. Since Pub. VI in a top-down manner focuses on telehealth rather than the position of MPPs within the industry, its scope exceeds the scope of RQ4. However, only relevant to RQ4 results of Pub. VI are presented in this thesis.

![Figure 3.3. Research framework for the multi-layer analysis of technological evolution of an industry (Pub. VI)](image-url)

The evolution of telehealth was studied throughout three time periods: 2002-2006, 2007-2011, and 2012-2016. To understand the technological development of telehealth on scientific research layer, the analysis of author-supplied keywords of telehealth-related publications was conducted, similar to the previous studies that used keywords as indicators of publication content (Cunningham and Kwakkel, 2011; Ferreira et al., 2014; Li et al., 2009). The development of telehealth on the invention layer was studied using patent co-classification analysis, relying on patents typically belonging to multiple classes, representing invention areas. Telehealth-related patents were first selected, after which their classification to other invention areas was
analyzed, which was viewed as an indication of patent content. A similar method was applied in previous studies (Caviggioli, 2016; Curran and Leker, 2011). Finally, to understand the evolution of telehealth products, relevant press releases were first selected, after which keywords were derived from their texts and analyzed. To deepen the understanding of the technological development of telehealth, the analysis on all three layers was supplemented by a review of studied literature – scientific publications, patents, and press releases. After that, trends were formulated based on the analyzed literature, which guided further analysis of a future industry architecture using the value network configuration method described in the next section.

### 3.3.2 Methods for uncovering the future

**Value network configuration analysis**

A value network is a set of business actors that work together to create economic value through a product or service by fulfilling functional roles enabled by technical resources (Casey et al., 2010). When developing a new service or product, a technical architecture – a set of required technical components and interfaces between them – is often defined by standards. However, uncertainty can exist around the business architecture of a service, that is, actors involved in the service provision, and the distribution of business roles, defined as an indivisible set of activities and technical components. To reduce this uncertainty, value network configuration (VNC) method (Casey et al., 2010) can be used to analyze different arrangements of role distributions among actors as well as business interfaces between them. VNC analysis can be viewed as a method of representing both the business and technical architecture of a service through interconnected actors, roles, and technical components. An actor can take one or several roles, and each role is enabled by one or several technical components. The method has been recently used in many studies that aimed to clarify potential industry architectures of a new technology or service (e.g., Walia et al., 2017; Zhang et al., 2015). The VNC method has an advantage over other value network analysis methods in showing both technical and business architecture of a service in the same figure. Pub. II uses the VNC method to partially address RQ2 by analyzing different potential ways of the distribution of new and old roles in eSIM-based RSM between the stakeholders of the mobile ecosystem. Furthermore, the VNC method together with multi-level literature analysis is used in Pub. VI for addressing RQ4.

**Qualitative system dynamics**

In Pub. III, RQ3 is partially addressed by analyzing potential competition implications of eSIM and eSIM-based multihoming with dynamic network selection using qualitative system dynamics. System dynamics is a method for analyzing the structure and dynamics of complex systems (Sterman, 2000), such as an industry or ecosystem. The method focuses on a system’s internal feedback structure that consists of variables and relations between them that can be of a positive or negative polarity. A relation of a positive polarity means that the change in one variable prompts another variable to change in the same direction, whereas a negative polarity link implies that the change in one variable makes another variable change in the opposite direction. The relationships between variables form feedback loops when the change in one variable alters other variables, eventually affecting the initial one and making it change again. Feedback loops generate dynamics in the system and can be reinforcing and balancing, with the former having an even and the latter an odd number of negative polarity links. Reinforcing loops lead to an exponential increase or decrease, whereas balancing loops result in a goal-seeking behavior.
System dynamics modeling starts with the conceptualization, that is, the definition of a qualitative model, consisting of variables, relationships, and loops. After that, the model is typically quantified: causal relationships between variables are formalized, and numerical inputs are entered so that the model can be simulated. However, system dynamics can also be used qualitatively, that is, as an influence model illustrating complex relationships between variables and feedback loops of a system. Especially when the problem under investigation is futuristic, and no reliable inputs can be found, the quantification of assumption-based models may involve too many uncertainties and lead to misleading results. In this case, a qualitative system dynamics model can provide insights without the danger of producing wrong numerical outputs (Coyle, 2000). Recent examples of using qualitative system dynamics can be found, for example, in public health (Macmillan et al., 2018) and electric power fields (Riva et al., 2018).

Pub. III adopted qualitative system dynamics over other alternatives (e.g., scenario planning or agent-based modelling) because it produces an influence map that in turn indicates variables that can be used as levers for changing the industry dynamics. Therefore, system dynamics models can help MNOs, regulators, and other stakeholders to gain a better understanding of the mechanisms that can be used for altering the ecosystem evolution.

Agent-based modeling

Pub. V used agent-based modeling (ABM) for simulating competition among IoT data platforms and partially addressing RQ3. ABM is a method for simulating the interacting autonomous micro-level agents that allows evaluating the emergent macro-level system behavior (Macal and North, 2010). Agent-based models consist of a set of agents – self-contained, autonomous, social, adaptive, and goal-directed components (e.g., an individual, a company, or software), the behavior of which is governed by rules; a set of relationships defining with whom and how actors interact; and the environment, where actors exist and which imposes constraints on actor’s behavior and interactions (Macal and North, 2010).

Agent-based modeling is well-suited for problems that can naturally be represented in terms of interacting, adaptive, and learning agents (Macal and North, 2005). Therefore, the method has been used in a broad range of applications from modeling human behavior on stock markets to the spread of epidemics and mobile communication service usage (Basaure et al., 2016). At the same time, ABM has some disadvantages, including computational intensity and poor generalizability beyond the analyzed cases (Rand and Rust, 2011).

ABM was chosen as a research method for Pub. V because it allows decision-making to happen at a micro level (agents select a platform), whereas some rules can be imposed centrally (interoperability between platforms that affects switching costs and multihoming). As a top-down alternative, quantitative system dynamics would require market-level models that cannot be reliably developed given the future-oriented nature of research. In turn, in the bottom-up ABM, modeling the ecosystem evolution requires setting the parameters governing the behavior of individual actors e.g., by relying on previous studies. This could be done more accurately than developing a market-level model.
4. Evolution of mobile network operators for IoT

This chapter analyzes the evolution of mobile network operators (MNOs) for IoT. Section 4.1 examines new traffic patterns that mobile IoT devices from different industries generate, focusing on the differences across industries as well as between IoT and consumer devices. Therefore, Section 4.1 addresses RQ1 and helps to understand the new customers that MNOs will increasingly serve in IoT.

After that, Section 4.2 analyzes potential impacts of Embedded SIM (eSIM) technology on the mobile ecosystem in general and the position of MNOs in particular and thereby addresses RQ2. Embedded SIM can become one of the most disruptive developments in the mobile telecom industry, with a significant impact on the mobile ecosystem. First, potential value networks of eSIM in IoT are studied to understand the possible distribution of new business roles related to eSIM among the ecosystem stakeholders. Then, the potential competitive impacts of eSIM are analyzed.

4.1 New customer base and usage patterns

To characterize the use of mobile IoT devices, two-year-long CDR (call data record) data from a major Finnish MNO was analyzed. The results of the analysis are presented in Pub. I and summarized in this section.

Table 4.1. Definition of industries based on NACE Rev. 2 (Eurostat, 2008) (Pub. I © 2019 IEEE)

<table>
<thead>
<tr>
<th>Industry (abbr.)</th>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative and support</td>
<td>AS</td>
<td>Activities supporting general business operations, except professional activities; e.g., rental and leasing, recruitment, security and investigation</td>
</tr>
<tr>
<td>Electricity and gas</td>
<td>EG</td>
<td>Providing electric power, natural gas, steam, hot water and the like through a permanent infrastructure</td>
</tr>
<tr>
<td>Information and communication</td>
<td>IC</td>
<td>Publishing activities, including SW; broadcasting; telecommunications and IT activities</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>MF</td>
<td>Physical or chemical transformation of materials or components into new products, e.g., food, textiles, computers, and electronics</td>
</tr>
<tr>
<td>Professional activities</td>
<td>PA</td>
<td>Activities making specialized knowledge available to users, e.g., consultancy and engineering</td>
</tr>
<tr>
<td>Transportation</td>
<td>TR</td>
<td>Provision of passenger or freight transport, and associated activities, such as terminal and parking facilities, cargo handling, and storage</td>
</tr>
<tr>
<td>Wholesale and retail trade</td>
<td>WR</td>
<td>Wholesale and retail sale of any goods, including associated operations, such as assembling and packing; repair of motor vehicles and motorcycles</td>
</tr>
</tbody>
</table>
4.1.1 Traffic patterns

First, the evolution of IoT device traffic over the two years was examined. Figure 4.1 shows a four-week moving average of the traffic per device. Both received and sent traffic increased over the two years from September 2016, the former one nearly by six times to 50MB, and the latter one by three times to 100MB. Although there are some fluctuations in traffic evolution, Figure 4.1 does not show any clear seasonal patterns. Expectedly, IoT devices generate considerably lower data traffic than consumer devices, which in Finland consume on average 14200 MB of data (tefficient AB, 2018).

Further, traffic evolution in different industries was analyzed. For generalizability, only industries with a sufficient number of companies and devices were selected. Table 4.1 describes the analyzed industries. Figure 4.2 demonstrates considerable differences in the traffic across industries, with Administrative and support industry generating the most traffic – more than 1GB per device, likely because of a large number of security cameras, and devices in Manufacturing industry on average generating the least traffic – less than 1MB. Traffic volume increased in almost all industries, with the most significant growth in the Electricity and gas industry - from 1.5 to 20 MB over two years.
After that, to observe weekday traffic patterns, traffic per device per day across industries was examined for the latest available month (August 2018). As Figure 4.3 shows, weekday-weekend patterns can be observed in Professional activities, Manufacturing, and to a lesser degree in Wholesale and Retail trade industries, with traffic decreasing significantly on weekends. Smartphone traffic typically does not exhibit weekday-weekend patterns (e.g., Shafiq et al., 2013).

![Figure 4.3. Data per device per day for industries (August 2018)](Pub. I © 2019 IEEE)

Finally, to understand the composition of IoT traffic, similarly to Shafiq et al. (2013) the empirical cumulative distribution function (ECDF) of the logarithm of uplink to downlink traffic ratio was plotted for different industries. Figure 4.4 shows that the logarithm of uplink to downlink ratio is mostly positive, meaning that IoT devices in all industries generate more uplink than downlink traffic. Namely, about 92% of IoT devices generated more uplink than downlink traffic, which agrees with the findings of Shafiq et al. (2013) although exceeds by 30% the share observed by Romirer-Maierhofer et al. (2015). At the same time, in some industries, such as Transportation, the share of devices with prevailing uplink traffic is lower – about 54%. Nevertheless, such a composition of IoT traffic contrasts with smartphone traffic, which is dominated by downlink for 75% of devices (Shafiq et al., 2013).

![Figure 4.4. ECDF of the log of uplink to downlink traffic ratio for August 2018](Pub. I © 2019 IEEE)
4.1.2 Mobility patterns

To gain a better understanding of the use of mobile IoT devices across industries, device mobility was analyzed. Figure 4.5 shows the ECDF of the number of distinct cells visited per device per month in August 2018. About 40% of IoT devices visited only a single cell, which is close to 30% discovered by Shafiq et al. (2013). The actual share of stationary devices can be even larger because devices can connect to different cells with overlapping coverage depending on the signal quality. As Figure 4.5 shows, the least mobile devices are in Electricity and gas, Wholesale and retail trade, and Administrative and support industries, whereas the most mobile – in Transportation and Manufacturing. Thus, half of the IoT devices in the Transportation industry visited more than 40 distinct cells per month. Therefore, IoT devices in Transportation seem to be more mobile than smartphones, half of which visit about seven cells per week (Shafiq et al., 2013).

Figure 4.5. ECDF of IoT device mobility for August 2018 (Pub. I © 2019 IEEE)

4.1.3 Traffic and device distribution over cells

Figure 4.6 shows the distribution of traffic and devices over all cells IoT devices visited at least once during the two years of data coverage. As Figure 4.6 indicates, IoT traffic is spatially concentrated, with about 40% of all data being generated in 0.01% of the cells, and 10% of the cells carrying 93% of all IoT traffic. This is larger than the concentration of human device traffic observed by Paul et al. (2011), who found that 55% such traffic was generated in 10% of the cells in a nation-wide network in 2007. At the same time, 50% of the cells served about 90% of all IoT devices, which indicates that some cells contain only a few IoT devices. Such a high concentration of IoT devices can be explained by the higher centralization of company campuses, where IoT devices are typically deployed, compared with consumer customers.

Figure 4.6. Distribution of traffic and devices among cells for August 2018 (Pub. I © 2019 IEEE)
4.1.4 Device base statistics

Furthermore, using the device feature dataset, the IoT device base was examined. First, the mean age of the device population was analyzed defined based on the device model introduction year (Figure 4.7). Since the dataset does not contain information on the month of device model introduction, all devices were assumed to be introduced on the January 1st, meaning that the device population age on Figure 4.7 is overestimated, which, however, does not prevent comparing the mean age across industries and tracking the dynamics. As the figure shows, the IoT device population age was more than 8 years as of August 2018. Furthermore, the trend is increasing, which indicates the slow pace of device substitution to new device models. Electricity and gas industry appeared to use the oldest IoT device models, with the mean age exceeding 10 years. This is likely due to the early deployment of smart electricity meters in Finland and long lifecycle of such devices.

Figure 4.7. Mean age of device population (months) based on the device model introduction year (Pub. I © 2019 IEEE)

Moreover, the diffusion of 3GPP connectivity standards among the IoT device population was analyzed, which showed that the diffusion of LTE was only around 2% as of August 2018. This is sufficiently lower than the diffusion of 41% among non-machine devices estimated by GSMA for European countries (GSMA, 2018). At the same time, nearly 100% of mobile IoT devices are equipped with GPRS and EDGE connectivity, and about 70% have UMTS and HSDPA features. This indicates that about 30% of all IoT devices are 2G-only, which may slow the shutdown of 2G networks planned in some countries.

4.1.5 Temporal analysis

Furthermore, the temporal activity of IoT devices was analyzed. First, similarly to Shafiq et al. (2013), the periodicity of device communications was explored. For that, the periodogram of the traffic series of every device for received data for August 2018 was plotted. Figure 4.8 shows peaks at 6, 12, and 24 hours for devices with small and large traffic volumes (power), indicating that the communication of many IoT devices is periodic, likely triggered by a timer. Also, an unexplained peak at 13 hours can be observed, which is due to two companies with a large number of devices of the same model.
Finally, temporal clustering of data time series for all devices for August 2018 was conducted. Figure 4.9 shows the results of clustering, which divided IoT devices into three groups that account for 25%, 41%, and 34% of the devices. As Figure 4.9 illustrates, Cluster 1 peaks at 2:00, whereas Cluster 3 at midnight. In turn, Cluster 2 transmits data more steadily throughout the day.

Further, the representation of different industries in clusters was checked. Cluster 1 is dominated by one large company that accounts for 88% of devices, while Cluster 2 contains devices from different companies and industries, including Wholesale and retail trade (40%), Electricity and gas (22%), and Information and communication (14%). For Cluster 3, the main industries are Wholesale and retail trade (51%), Electricity and gas (30%), Administrative and support services (11%). Interestingly, devices from the same industry (Wholesale and retail trade, Electricity and gas) belong to different clusters, potentially indicating different IoT device use cases within the industry.
4.2 Provision of embedded SIM-based subscription management

4.2.1 Value network configurations

Remote subscription management or remote SIM management (RSM) is a driver for the diffusion of mobile IoT. Embedded SIM specifications have emerged as a de-facto standard for RSM in IoT. While the specifications define the main technical components and roles, they do not clarify potential business implementations of eSIM. Given the importance of RSM for future mobile IoT, many actors are interested in leading its value network, therefore, creating uncertainty about the future of RSM service. To reduce this uncertainty, Pub. II examined value networks that can emerge around eSIM-based RSM using the value network configurations (VNC) method of Casey et al. (2010) (see Section 3.3.2). The notations of the method are presented in the upper left side of Figure 4.10. The technical architecture of eSIM RSM was assumed to comply with GSMA specifications. Furthermore, for the clarity of figures, VNCs omitted some technical interfaces between the roles of the same actor.

Seven key roles were determined in the value network of eSIM: subscription manager-data preparation (SM-DP), subscription manager-secure routing (SM-SR), provisioning of bootstrap subscription, provisioning of operational subscription, IoT service provision, IoT module production, and eUICC\(^6\) production. The first three roles are new and defined by GSMA Embedded SIM specifications (GSMA, 2016). SM-DP is responsible for the operator’s profile preparation; the function of SM-SR is to deliver a profile from a remote server to an eUICC, and a bootstrap subscription is required for providing initial connectivity to an eUICC for downloading an operational subscription. IoT service providers rather than end users were assumed to make technical and business decisions relevant for the analysis, and therefore, an end user is not among the main roles of the value network.

After the roles were defined, five VNCs were constructed that could be divided into three groups: driven by hardware vendors, connectivity providers, and IoT service providers. Although more than five feasible implementations (configurations) exist, only the ones that are the most different from each other were examined.

Unlike in Pub. II, VNCs in this section do not assume SM-DP role to be served exclusively by UICC vendors. Indeed, although UICC vendors have the expertise and secure production sites required for acting as SM-DP, some other actors, such as MNOs (Telenor, 2017), have shown their interest and readiness to provide SM-DP services. Additionally, in this section, all VNCs assume that SM-DP and SM-SR roles are taken by one actor because such a configuration decreases the costs and complexity of establishing interfaces between the two subscription manager roles. Moreover, this represents the plan of GSMA to combine SM-DP and SM-SR functions into a single subscription manager role, similarly to eSIM specifications for consumer devices (GSMA, 2017). However, other implementations are possible where SM-DP and SM-SR roles are taken by different actors.

Hardware vendor-driven VNCs

The first two VNCs, UICC vendor-driven and IoT module vendor-driven, constitute hardware vendor-driven VNCs. UICC (SIM card) vendors are well positioned to lead a VNC since they already serve the functions of SM-DP in a conventional SIM architecture and collaborate with

\(^6\) Hereinafter, GSMA specifications for RSM will be referred to as “eSIM,” whereas a hardware element (a SIM card) compliant with eSIM specs will be referred to as “eUICC.” Further, for consistency, SIM vendors will be referred to as “UICC vendors”
MNOs around the world. Therefore, this VNC is beneficial for IoT Service providers (SP) operating globally. The role of a UICC vendor in the VNC in Figure 4.10 is two-fold. First, it produces eUICCs loaded with an initial bootstrap profile of its own in-house virtual mobile operator and delivers them to IoT module vendors. Second, a UICC vendor also acts as a subscription manager (SM) for IoT SPs.

![Figure 4.10. UICC vendor-driven VNC (Adapted from Pub. II © 2015 IEEE)](image)

IoT SPs can either contract mobile operators in different countries independently or manage cellular contracts centrally through the SM (UICC vendor) if the latter provides such an opportunity. This is shown by dashed red arrows in Figure 4.10. Further, this VNC requires IoT SPs to select operational M(V)NOs that are integrated with the contracted SM (fulfilled by UICC vendor). However, given that UICC manufacturing is a concentrated market with five producers accounting for around 70% of total shipments (Sultania et al., 2017), mobile operators may be interested in maintaining integrations with the SM systems of the largest UICC vendors. Depending on the country of the first device use, a subscription manager, fulfilled by a UICC vendor, downloads an operational profile of an MNO selected and contracted by an IoT SP to the defined eUICC. For streamlining the process, ordering and preparation of profiles can be done in bulk before IoT devices are activated. An operator switch can be initiated by an IoT SP through SM-SR if the mobile subscription contract allows that.

This configuration is likely to bring UICC vendors new sources of revenue, which are important to offset the potential revenue drop caused by the decrease in sales due to the programmability of eUICC. MNOs in this VNC are only responsible for providing the actual connectivity. Moreover, MNOs will likely have to invest more in customer retention, because the switch between operators in this configuration may be easy. However, long-term contracts that will protect the position of MNOs are likely to be common. The advantage of this VNC is the global reach of UICC vendors, which collaborate with MNOs around the world. Compliance with
GSMA specifications should further guarantee the interoperability of eUICCs of a manufacturer with the SM system of another UICC vendor. To illustrate that, VNC in Figure 4.10 shows that IoT module vendor and IoT service provider have business relationships with different UICC vendors.

The second VNC shown in Figure 4.11 is IoT module vendor-driven, which illustrates the willingness of IoT module producers to move from HW to service business. Thus, some IoT module vendors, such as Sierra Wireless and Telit, already provide IoT platforms as a service for device management and application development, and the addition of SM functions would complement the functionality of such platforms. Moreover, IoT module vendors can move upstream in the supply chain and start producing eUICCs, although Figure 4.11 assumes that a UICC vendor takes the roles of eUICC production and its loading with a bootstrap profile through in-house SM-DP. The benefit of IoT module vendor-driven VNC is the reach of MNOs around the world.

**Figure 4.11. IoT module vendor-driven VNC**

**Connectivity provider-driven VNCs**

The next group of VNCs is driven by connectivity providers. The third VNC is managed by an MNO. In this VNC, eUICCs are produced by the order of an MNO and loaded with its operational profile on the stage of manufacturing, unlike in the previous VNCs, where newly produced eUICCs are not associated with any operational MNO. This, in turn, removes the need in a separate bootstrap subscription. IoT SPs can order IoT modules either directly from the manufacturer, or an operational M(V)NO may act as a reseller of IoT modules equipped with eUICC provisioned with its subscription profile. These options are illustrated by dashed red arrows (business interfaces) in Figure 4.12.

In the mobile operator-driven VNC, MNOs from different countries may form alliances, illustrated by the dashed business interface between the two Operational M(V)NOs in Figure 4.12. If an IoT SP decides to use the services of such an alliance, it will be able to use the networks of partner operators in the countries of their presence. Thus, if a connected car (an IoT device) roams from the network of the initial operator to a partner operator’s network, the car’s
eUICC can automatically receive a profile of a local partner operator thereby helping to avoid roaming charges. At the same time, IoT SPs will keep a contractual relationship with the initial MNO. In the VNC driven by an MNO alliance, IoT SPs cannot select separate preferable operators in different counties, but instead have to choose a desirable mobile operator alliance, which cannot be changed thereby forming a “walled garden,” meaning that IoT SPs will be locked-in to the operator alliance. On the other hand, Operational M(V)NOs may operate independently without an alliance, allowing the switch to any other operator at the end of the subscription period. However, MNOs may try to avoid such a service configuration as they may be concerned about a potential increase in churn that such a configuration may cause.

The fourth VNC is driven by a new actor – IoT connectivity provider, fulfilling the roles of operational and bootstrap connectivity provision, along with SM-DP and SM-SR (Figure 4.13). IoT connectivity provider may act as a global virtual operator buying network access in bulk and reselling it to IoT SPs, allowing eUICCs to be provisioned with a local profile from the pool of a connectivity provider’s profiles. In the local scenario of this VNC, a connectivity provider collaborates with several local operators, and if the network connection fails, devices of customer IoT SPs automatically switch to a fallback (bootstrap) profile and download a new profile of another MNO. This is especially critical for some applications requiring high connection reliability, such as remote healthcare or emergency, and therefore, a regulator can support the idea of establishing a local or regional IoT connectivity provider. On the other hand, such a VNC is hard to implement, because it deprives MNOs of contractual relations with IoT SPs, which operators would like to avoid. Therefore, an IoT connectivity provider must be an influential actor, potentially with existing relations with mobile operators. Large mobile device manufacturers, such as Apple or Gemalto (a producer of IoT modules) may act as IoT connectivity providers for their IoT devices.
Finally, the fifth VNC is an IoT service provider-driven (Figure 4.14). In this VNC, IoT SP serves SP-SR and SP-DP functions in-house. This VNC is hard to implement, as it requires IoT SP to establish and maintain integrations with MNOs, set up and run network elements for SM functionality, as well as go through GSMA certification for SM, which is a requirement for participating in the global eSIM ecosystem. Therefore, this VNC can be only feasible for large IoT SPs, such as manufacturers of connected cars.
Comparison of VNCs

The comparison of the five analyzed VNCs is presented in Table 4.2. The core difference between the VNCs is the party providing subscription management service. Moreover, the fourth VNC differs from others in the connectivity provider, which may come from a non-MNO family (e.g., Google or Apple). A separate subscription for each operator is required in the first, second, and fifth VNCs, whereas in the third and fourth VNCs one subscription may be enough for using the networks of partner operators. Further, customer lock-in is possible in all cases, at least for the duration of a subscription contract, or permanently in the mobile operator-driven and IoT connectivity provider-driven VNCs. Finally, although it is difficult to estimate which of the analyzed VNCs will become a dominant design of the business architecture of RSM, the IoT connectivity provider-driven VNC is less likely to become a standard in the short term since this VNC is the most disruptive to MNOs. On the contrary, UICC vendor and MNO-driven VNCs are more probable because they involve fewer changes to the current mobile ecosystem, and because both actors have some of the capabilities and assets required for serving SM-SR and SM-DP roles.

<table>
<thead>
<tr>
<th>Table 4.2. Comparison of analyzed VNCs (Adapted from Pub. II © 2015 IEEE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) UICC vendor-driven VNC</td>
</tr>
<tr>
<td>SM provider</td>
</tr>
<tr>
<td>Contracting party providing connect. to IoT SP</td>
</tr>
<tr>
<td>Coverage of the connectivity provider’s subscr. without roaming</td>
</tr>
<tr>
<td>Customer lock-in to the connectivity provider</td>
</tr>
<tr>
<td>Probability of becoming a dominant design</td>
</tr>
</tbody>
</table>

4.2.2 Evolution scenarios and impacts

Although originally embedded SIM was promoted for IoT devices, in 2016 the specification was extended to consumer devices. Currently, the specification imposes certain restrictions, which seem to be set up artificially for protecting the business interests of mobile operators. Thus, only one profile can be active at a time, and the profile switch requires explicit end user’s intent and cannot be automated. However, since there are no technical grounds for these limitations, they can be lifted, and embedded SIM can lead to even more sufficient changes in the mobile ecosystem and further challenge the position of MNOs. These potential changes were modeled using a qualitative system dynamics method based on the input from 13 interviewees. The results of this analysis are presented in Pub. III and summarized in this section.
The starting point for the study was the adoption of remote subscription management (RSM) for IoT devices, meaning that the main HW elements required for the RSM are in place. The next step on the way of eSIM evolution is the diffusion of eSIM handsets, which is affected by forces depicted in Figure 4.15. The main requirements for the diffusion of eSIM handsets, as the figure shows, are the availability of such handsets on a market (Diffusion of eSIM among handset models) and technical support of eSIM by a sufficient number of MNOs (Diffusion of eSIM support among MNOs), which are connected through the combination of loops R1.1 “Demand-supply synergy” and R1.2 “Indirect network effect.” Furthermore, the bandwagon effect (loop R1.3) may increase the Adoption of eSIM support among MNOs, because operators not supporting eSIM will be at a competitive disadvantage compared with adopters. Since eSIM can reduce the cost of switching between MNOs, which typically leads to higher competition, the regulator may be interested in promoting the adoption of eSIM support for handsets among MNOs (loop B1.1a) if the market is not competitive enough. At the same time, if eSIM for handsets is already supported, MNOs may try to complicate the process of switching between profiles (loop B1.2). For example, they can try to lock customers contractually, in which case the regulator may intervene and relax such restrictive practices (loop B1.1b).

Depending on the relationships between variables and the strength of feedback loops, the ecosystem can follow different scenarios presented in Table 4.3.

If the dynamics of the system presented in Figure 4.15 result in medium to high diffusion of eSIM among end users, it can prompt the diffusion of eSIM multihoming with dynamic network selection - the situation when end users have subscriptions of several operators, and can dynamically and automatically select the one providing the best price or quality. The diffusion of eSIM multihoming is affected by benefits that such a mechanism can bring to the customers, which can be divided into capacity, coverage, and reliability-related. However, the first two of

---

7 The architecture and HW elements of GSMA eSIM specifications for IoT and consumer devices are different but overlapping. However, some elements deployed for IoT eSIM can be reused.
8 Text in italics in Section 4.2.2 corresponds to the names of variables in qualitative system dynamics models
9 Hereinafter referred to as eSIM multihoming for brevity
these benefits only exist if the networks of operators are different in the mentioned quality metrics, as illustrated by negative links to the Customer benefit of eSIM multihoming in Figure 4.16. For example, if operators’ networks completely overlap in coverage, multihoming does not bring a coverage advantage. Further, as eSIM multihoming penetrates the market, competing networks become more similar in terms of capacity that they provide to customers, which decreases users’ intention to switch from single-homing (loop B2.1). This happens due to a load and congestion balancing capability of eSIM multihoming.

Table 4.3. Scenarios for the diffusion of eSIM among handsets

<table>
<thead>
<tr>
<th>Diffusion of eSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Zero:</strong> MNOs refuse to support eSIM for handsets (R1.2), no compatible devices produced (R1.1). “Chicken and egg” problem.</td>
</tr>
<tr>
<td><strong>Low:</strong> Limited number of eSIM handsets available, limited support among MNOs (R1.1, R1.2). Subscription management process is restricted (B1.2).</td>
</tr>
<tr>
<td><strong>Medium to high:</strong> eSIM handsets are introduced by major producers, eSIM is supported by large MNOs (R1.1, R1.2); the bandwagon pressure drives eSIM support (R1.3). Regulators promote eSIM support (B1.1a, B1.1b). eSIM multihoming is in demand.</td>
</tr>
</tbody>
</table>

Multihoming increases service quality compared with single-homing (Finley and Basaure, 2018). However, not all customers will switch to multihoming, because of, for example, the inconvenience of maintaining several active subscriptions. Further, depending on pricing models, keeping several mobile subscriptions may be expensive, although with metered data pricing a price difference between single-homing and multihoming will be small. Another reason for possible limited uptake of multihoming is the sufficiently good performance of individual networks. As Figure 4.16 shows, if customers are satisfied with the service quality of single-homing, they will not adopt multihoming. Moreover, MNOs may try to increase customer satisfaction and loyalty in order to decrease the relative advantage of multihoming (loops B2.2a,

---

Note that Finley and Basaure (2018) define “multihoming” as the ability of simultaneously transferring data over multiple networks, whereas our definition of multihoming relies on the ability of changing dynamically between networks. In the terminology of Finley and Basaure (2018), this is referred to as “end user network switching.”
B2.2b, B2.3). Furthermore, the diffusion of multihoming will increase the competition and put pressure on MNOs to increase investments to sustain in the market, which can decrease the Adoption of eSIM multihoming (loop B2.4). On the other hand, due to the increased competition and reduced profits, MNOs may be unable to continue investing in the network, further increasing the popularity of multihoming (loops R2.1a, R2.1b). These dynamics can lead to different diffusion scenarios of eSIM multihoming, which are summarized in Table 4.4.

Table 4.4. Scenarios for the diffusion of eSIM multihoming

<table>
<thead>
<tr>
<th>Diffusion of eSIM multihoming</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Zero or low:</strong> Limited benefits of combining several operators (similar capacities and footprints). High satisfaction with single-homing. MNOs invest in customer loyalty and network (B2.2.3, B2.2.4).</td>
</tr>
<tr>
<td><strong>Special use cases:</strong> Ordinal users are satisfied with single-homing or perceive its benefits as insufficient for adoption. Multihoming is adopted for special use cases (e.g., emergency communications).</td>
</tr>
<tr>
<td><strong>Medium to high:</strong> Quality of individual networks is not good enough to keep customers satisfied (B2.2.2a, B2.2.2b). Diffusion of eSIM multihoming imposes additional budget constraints, leading to less investment and a further decrease in the attractiveness of single-homing (R2.1a, R2.1b). The coverage and capacity of competing networks are different, therefore driving multihoming adoption.</td>
</tr>
</tbody>
</table>

Finally, if the Diffusion of eSIM multihoming achieves a medium or high level, it can lead to new competitive dynamics (Figure 4.17). At this stage, most of the customers maintain subscriptions of several operators and their devices can seamlessly change between them. Operators are not anymore competing for a market share traditionally defined in terms of subscriptions. Instead, the share of data or other communication sessions served by an MNO becomes a relevant metric of its performance and success. Customers’ devices select a network for their data sessions based on the Network availability, Average capacity per session available and Price per unit of data, which are affected by the dynamics of loops R3.3a, R3.3b “Network investments pay off”, B3.1a, B3.1b “Negative network effect”, B3.3 “Congestion pricing”, and others.

Figure 4.17. MNO’s operations in eSIM multihoming scenario (Pub. III)
Mobile operators will continue to compete based on the price and quality, but the competition will become more dynamic. Price competition-related loops B3.4 and R3.1 show that MNOs will try to provide the lowest market data price to attract more data sessions if they have underutilized network capacity. If services of different MNOs are similar in quality, which may be the case because of the load-balancing capability of multihoming, customers select the operator mainly based on their price. This can lead to a price war between MNOs that can decrease the price to a marginal cost, which can lead to the reduction of operators' Revenues and Investments in network performance.

Quality competition in the form of capacity competition is shown by loops B3.5 and R3.2. If the capacity utilization is high, and adding new capacity is potentially profitable, operators will try to provide the highest capacity in the market to attract more sessions, since the deployment of additional capacity instantly increases the number of allocated sessions, given the competitors' prices are equal. However, in unprofitable sparsely populated areas, operators may rely on competitors to serve customers and stop building infrastructure, since the service unavailability does not negatively affect their reputation as in the single-homing scenario.

Overall, eSIM, initially developed by IoT, can disrupt human communication's part of the mobile ecosystem by enabling dynamic multihoming and significantly changing the timescale of operator switching. Since MNOs are not interested in such a change, eSIM multihoming will diffuse only if strongly supported by device manufacturers or regulators. The latter can be interested in eSIM multihoming especially if separate networks cannot provide the quality that would satisfy customers' requirements. However, due to high market dynamism resulting from eSIM multihoming, cellular network planning will become difficult, which may result in network over-provisioning and consequent fierce price competition in an attempt to increase the network utilization by decreasing the price. On the other hand, under-provisioning situation is also possible, resulting in networks' congestion (Pub. III). Therefore, before mandating the support for eSIM multihoming, regulators should quantitatively evaluate the potential impacts of eSIM multihoming, perhaps using the qualitative models presented in Pub. III as a basis.
5. Evolution of mobile platform providers for IoT: case mHealth

This chapter analyzes the evolution of mobile platform providers (MPPs) for IoT using the case of the mobile health domain. The mobile health is an advanced consumer IoT domain in terms of device adoption, as well as the number of device producers and app developers. Therefore, the case study results are of immediate relevance not only to MPPs but also to multiple other mHealth companies. Furthermore, the results of the mHealth study can be partly generalized to other consumer IoT domains as they share many similarities. Namely, just like in mHealth, in the connected car and smart home domains, the data is fragmented and often kept proprietary by producers, resulting in its under-utilization that calls for the data sharing. Collaborative and competitive relationships emerging in such data sharing ecosystems need to be carefully governed by the ecosystem keystone (MPPs or other stakeholders in different domains). At the same time, consumer IoT domains have particularities that limit the generalizability of the mHealth study results to other verticals. For example, unlike in mHealth, where IoT devices are mostly sensors, in the smart home domain devices can also be actuators, potentially requiring setting up additional policies for governing the data sharing. Furthermore, whereas in mHealth the data is generated and managed by multiple producers, most of the connected car data will likely be kept by car manufacturers, implying that the governance of data sharing will be more centralized in the connected car domain than in mHealth. Nevertheless, while the results of the mHealth case study are not fully generalizable to other domains, the developed research design can be applied for studying other verticals.

This chapter is further structured as follows. On the example of mHealth, Section 5.1 examines how MPPs can govern collaboration and competition in the evolved mobile ecosystem. As Section 2.4 described, the two largest MPPs Apple and Google introduced platforms for centrally collecting and sharing wearable and mHealth data, creating a “sub-ecosystem” of new complementors – data-based application and service providers, thereby extending the boundaries of the mobile ecosystem. Creating and sustaining such an mHealth data ecosystem require careful governance of relations with complementors and other platforms. However, previous research has not examined the governance of emerging mHealth data sharing platforms, indicating a research gap addressed by Pub. IV and V and summarized in Section 5.1.

First, Section 5.1.1 analyzes the governance of complementors in mHealth data platforms. After that, the viewpoint is switched from an individual platform to a broader data ecosystem view (Figure 5.1) and the governance of platform collaboration for achieving a competitive market is studied in Section 5.1.2. In this way, Section 5.1 addresses RQ3 “How could collaboration and competition be governed in emerging consumer IoT data platforms and particularly mobile health data platforms?”
After investigating the governance of consumer IoT data platforms on the example of mHealth platforms, the scope is broadened to consider the position of the mHealth data ecosystem in healthcare, namely, its ICT-based remote delivery mode that is referred to as telehealth (World Health Organization, 2010) (Figure 5.2). Indeed, after MPPs develop an ecosystem around mHealth data, the next step in their IoT journey will likely be a new market development. Namely, MPPs can offer their products – mHealth data platforms and wearable devices – to a new for them healthcare industry market. However, it is unclear whether and how MPPs can fit a highly regulated healthcare industry. To understand that, Section 5.2 examines the evolution of telehealth – a part of the regulated healthcare that mHealth is likely to contribute the most. Particular attention is placed on the past and current positions of wearables, IoT, and mHealth in telehealth and their role in the future telehealth ecosystem. As pattern fill on Figure 5.2B shows, the study is centered on telehealth rather than mHealth to get an unbiased understanding of the position of the mHealth data ecosystem in telehealth. The results of this analysis, which are presented in Section 5.2, answer RQ4 “How could mobile platform providers acting as mobile health data platform providers position themselves in the ecosystem of the healthcare industry?”
5.1 Governance of consumer IoT data platform ecosystems

To understand the governance of consumer IoT data platforms, the case of mHealth data sharing is examined.

5.1.1 Individual platform view

*High-level data sharing strategy*

Pub. IV took an individual platform view (Figure 5.1) for analyzing the governance of collaboration and competition with complementors of 21 web mHealth data platforms\(^{11}\). Particularly, mechanisms were identified that are used for resolving one of the main tradeoffs of platform governance – enhancing the platform generativity while maintaining control.

Companies participating in data sharing choose different roles and thereby follow different high-level sharing strategies. Namely, two decisions were found to define a high-level data sharing strategy of a company: data sharing role and data platform role. Based on these two decisions, a high-level data sharing strategy of a company can be described as one of the 15 possible combinations of the four “elementary” roles A, B, C, and D (Table 5.1).

<table>
<thead>
<tr>
<th>Data role</th>
<th>Platform role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data provider</td>
<td>Platform provider</td>
</tr>
<tr>
<td>Data consumer</td>
<td>A</td>
</tr>
<tr>
<td>Data consumer</td>
<td>C</td>
</tr>
</tbody>
</table>

Data sharing role can be a provider (A and B) and consumer (C and D). Data platform roles are similarly a platform provider (A and C) and consumer (B and D). A company can further combine the roles and become a “prosumer” (a data prosumer – e.g., AC, or a platform prosumer – e.g., AB). The strategy of a company, defined as one of the 15 possible combinations of the roles from Table 5.1, determines the extent it can govern data sharing. Thus, while data consumers – platform consumers (strategy D) typically do not have the power to manage data sharing, data providers – platform providers (strategy A) have the most power to govern data sharing: they can both set the rules of platform use and decide what data to share with complementors. However, such power comes at a high cost because platform design and support require considerable investment and involve the risk of failing to attract third-party complementors to the platform. Therefore, the analysis showed that many companies took a platform consumer role by connecting to the existing platforms of desirable complementors. However, the deployment and maintenance of multiple integrations can be expensive and risky because platform providers may change the API that third-party complementors use to access the platform, thereby breaking the integration (Rafiq et al., 2013), or discontinue access to the platform altogether. Therefore, the decision of whether to provide or consume the platform, or combine the two roles is of strategic importance in data sharing. The analysis of 192 direct data sharing links between 37 case mHealth companies most actively participating in data sharing revealed that out of the studied companies, four followed the platform provider role, including the largest MPPs Apple and Google, eleven selected the platform consumer role, and 22 were platform prosumers (Figure 5.3).

---

\(^{11}\) mHealth data sharing platforms are provided not only by MPPs but also by device manufacturers and app developers (see Figure 5.3)
Design and governance of mHealth data sharing

Out of the 37 apps and services that most actively participated in mHealth data sharing, 21 provided web data sharing platforms. The boundary resources of those 21 apps and services were analyzed to determine design and governance decisions of data sharing made by platform providers for managing the relations with complementors (see Section 3.3.1 for methodology). Sixteen such decisions were determined, which were further divided into three groups (Table 5.2). The first group of decisions – the governance of data scope – represents choices relevant to data providers and platform providers, whereas the last two groups apply to platform providers only. For each “elementary” component role of its high-level strategy (Table 5.1), a company should make separate although interrelated decisions. For example, the strategy of wearable device manufacturer Polar is AB, which means that as a data provider – platform provider (role A), Polar should make decisions on the scope of shared data and decide on the platform design and governance. On the other hand, as a data provider – platform consumer (role B), Polar must choose the scope of data shared through the platforms of third parties.

First, data providers need to decide whether to open all available data types or to keep some data proprietary (Decision 1). Data providers may choose not to share some data types to maintain a competitive advantage of its in-house application. As the examples in Table 5.2 illustrate, fitness device producer Fitbit shares all data from its platform, whereas Polar keeps sleep data proprietary. On the other hand, instead of restricting the sharing of particular data types, a provider may decide to limit the granularity of opened data (Decision 2). At the same time, although sharing the aggregates and summary statistics is safe for the data provider as it prevents replicating and substituting its service, it does not provide sufficient benefits to complementors, who, therefore, can choose not to join the platform. Finally, some data providers may artificially delay the delivery of data to complementors (Decision 3). For example, a producer of continuous glucose monitoring devices Dexcom delays the delivery of data by three hours, explaining it by the need to prevent using their medical-grade data in inaccurate health-threatening applications.
Table 5.2. Key design and governance decisions managing the use of mHealth data sharing platforms by complementors (adopted from Pub. IV)

<table>
<thead>
<tr>
<th>Decision</th>
<th>Alternatives</th>
<th>Ex.1: Fitbit (strategy: ABCD)</th>
<th>Ex.2: Polar (strategy: AB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance of data scope (platform providers)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) Data types shared</td>
<td>Limited or not limited. (Provided: all collected or some. Accepted: custom data types allowed or not)</td>
<td>Provided: not limited (all collected) Accepted: custom data not allowed</td>
<td>Provided: limited (except sleep data)</td>
</tr>
<tr>
<td>2) Granularity of provided data</td>
<td>Limited or not limited. (Provided: summaries/samples or most granular available. Accepted: granularity restricted or not)</td>
<td>Provided: limited for heart rate and activity data; not limited with special permission Accepted: limited (no time series logging)</td>
<td>Provided: limited (no granular daily activity data)</td>
</tr>
<tr>
<td>3) Timeliness of provided data</td>
<td>As soon as available or delayed</td>
<td>As soon as available</td>
<td>As soon as available</td>
</tr>
<tr>
<td>Platform design (platform providers)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4) Number of APIs to a data platform</td>
<td>One or more</td>
<td>One</td>
<td>One</td>
</tr>
<tr>
<td>5) Platform API rights</td>
<td>Read, write, or both</td>
<td>Both</td>
<td>Read</td>
</tr>
<tr>
<td>6) Architectural style of API</td>
<td>REST API or other</td>
<td>REST API</td>
<td>REST API</td>
</tr>
<tr>
<td>7) Data change detection mechanisms</td>
<td>Polling, pull notifications, subscription API (&quot;webhook&quot;)</td>
<td>Subscription API</td>
<td>Pull notifications</td>
</tr>
<tr>
<td>8) Data access authorization</td>
<td>OAuth (1 or 2: authorization code grant or other grant flow), or other</td>
<td>OAuth 2.0: Authorization code grant, Implicit grant</td>
<td>OAuth 2.0: Authorization code grant</td>
</tr>
<tr>
<td>9) Supported data format</td>
<td>JSON, XML, FIT, GPX, TCX, or other</td>
<td>Read: JSON, TCX; Write: JSON</td>
<td>Read: JSON, XML, FIT, GPX, TCX</td>
</tr>
<tr>
<td>Platform governance (platform providers)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10) Platform openness</td>
<td>Open, semi-open, moderated, or hidden</td>
<td>Semi-open, access to granular data requires special permission</td>
<td>Open</td>
</tr>
<tr>
<td>11) API usage rate limitation</td>
<td>Yes or no</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>12) Price of API usage</td>
<td>Free, paid, or freemium</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>13) Revenue sharing / affiliate program</td>
<td>Yes or no</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>14) Directory of partners using API</td>
<td>Yes or no</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>15) Secondary data sharing</td>
<td>Prohibited or not explicitly prohibited</td>
<td>Prohibited</td>
<td>Not explicitly prohibited</td>
</tr>
<tr>
<td>16) Use of historical data after the integration is terminated</td>
<td>Prohibited or not explicitly prohibited</td>
<td>Not explicitly prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

Further, data platform providers must make six decisions related to the platform design. Thus, a provider may decide to have one or several APIs to its platform (Decision 4). Having several APIs may be sensible, e.g., for separating different groups of platform users (e.g., different APIs for data providers and data consumers). Next, a platform provider must decide whether their platform can be used for reading data, writing data, or for both purposes (Decision 5). This decision is connected with the data role of a platform provider. For example, when the platform provider is also a data provider, its API must provide "Read" access rights. Further, a platform provider must select the architectural style of the platform API (Decision 6). Nowadays, REST (Representational state transfer) is a dominant design among web API architectures likely because of its comparable simplicity, although other alternatives, such as SOAP, exist. Next, data change detection mechanisms must be defined (Decision 7). In mHealth platforms, three different mechanisms were detected: polling, pull notifications and webhooks. Further, platform providers must determine how data access authorization is granted (Decision 8). This decision
is of utmost importance for data privacy and security reasons, namely, for ensuring that platform end users willfully and consciously share their data with third parties. OAuth 2.0 is a de-facto standard for web data sharing authorization. Furthermore, platform providers must decide on the data formats supported by their platform \((\text{Decision 9})\). JSON is a de-facto standard that is ubiquitously used with REST API. However, some mHealth platform providers additionally support XML and fitness-specific data formats, such as GPX, TCX, and FIT.

Finally, seven key platform governance decisions were determined. For the beginning, platform providers must choose the level of their platform openness \((\text{Decision 10})\). Some mHealth data sharing platforms are open, that is, allow self-registration of developers and provide an API key without the approval of a developer and its application. Platforms can also be semi-open, with the access to some options requiring the approval of a platform provider (e.g., access to second granularity-level data in Fitbit platform). Finally, platforms can be moderated, meaning that an API key is provided after a developer and its application are approved. Some moderated APIs can also be hidden meaning that their existence is not announced publically on the web.

Further, platform providers have to decide whether and how to limit the maximum number of API calls to the platform \((\text{Decision 11})\). Such limits are ubiquitously imposed to protect the servers of platform providers from overload, although sometimes such limits are used as a differentiator between free and premium service tiers. The next identified governance decision is whether and how to charge for the API access \((\text{Decision 12})\). Currently, APIs in mHealth are mostly provided for free, as platform providers are expected to benefit from sharing indirectly through an increase in sales and consumer base. However, some APIs are paid, and some provide freemium access, charging, for example, for exceeding the limit of API calls. On the other hand, if the services of third-party developers directly contribute to the sales of a platform provider’s service, the provider may share these additional revenues with the developers \((\text{Decision 13})\).

Further, web platform providers may decide to have the directory of integrated partner apps \((\text{Decision 14})\). Although such partner listings are inseparable from many two-sided platforms, surprisingly, they are not ubiquitous in mHealth data sharing, likely because of practical reasons (uncertainty on whether the integration works properly). Moreover, platform providers shall decide their policy on secondary data sharing, a situation when the data gets from an originating service provider (SP) to another SP through the third one \((\text{Decision 15})\). Finally, the last identified governance decision is related to the policy on the use of historical data by complementors after the termination of an integration \((\text{Decision 16})\). Thus, some platform providers in such a case require the removal of all data received from the platform, which may constitute a significant switching cost for a data-consuming complementor due to the importance of historical data for improving AI-based services.

Overall, companies that decided to share data through a web platform must make decisions related to its design and governance to maintain the tradeoff between control and generativity, which is required for creating and sustaining the ecosystem of third-party applications. In mHealth, platform control typically includes the mitigation of potential risks associated with the substitution of the data-based service of a platform provider. This explains why platform providers often prohibit the apps that are “substantially similar” to the provider’s one (e.g., Nokia, 2017). However, this risk can be mitigated by limiting the scope and amount of opened data, as Figure 5.4 shows. Interestingly, data sharing can be managed not only by platform providers (roles A and C in Table 5.1) but also by data providers even if the platform of another
party is used (role B; Decisions 1-3). However, platform providers can use a broader set of decisions unavailable to platform consumers for managing data sharing (Decisions 4-16). All identified decisions can be used as mechanisms to affect generativity and control to a greater or lesser extent. For example, platform openness (Decision 10) directly influences control and generativity by changing the platform accessibility. Unlike governance decisions, platform design decisions affect generativity indirectly. For example, the more common architectural style is used (Decision 6), the easier the platform use, and the more generative the platform. However, the impact of the identified decisions is still to be formally investigated. At the same time, Pub. IV provides an initial discussion on the issue.

**Figure 5.4.** Relationship between control, generativity, and amount of shared data (adapted from Pub. IV)

*Generalization to other consumer IoT verticals*

Data sharing is required for utilizing data complementarities, enabling the development of data-based apps, and enhancing device interoperability. Therefore, data sharing is essential for all consumer IoT domains. Key design and governance decisions managing the use of mHealth data sharing from Table 5.2 can also be used for other consumer IoT verticals. However, differences may exist between verticals in decision alternatives. For example, supported data formats (Decision 9) may be industry-specific. Furthermore, other consumer IoT verticals likely require some additional governance mechanisms or decisions.

### 5.1.2 Platform ecosystem view

Section 5.1.1 took an individual platform view (Figure 5.1) and focused on the governance of collaboration and competition with platform complementors. This section takes an ecosystem view and concentrates on the governance of the relations between platforms.

Strong network effects can lead to monopoly in data platform markets, and therefore with the proliferation of such platforms in consumer IoT, the consideration of potential competition-related issues becomes increasingly important. Namely, the impact of different regulatory and standardization schemes on platform competition should be analyzed to define policies that would effectively govern a consumer IoT data platform ecosystem and ensure sufficient competition. To inform such policies, an agent-based simulation of the competition among consumer IoT data platforms was conducted. The simulation results, which are presented in Pub. V and summarized in this section, can inform regulators about schemes that help to manage the industry efficiently and show platform providers potential development paths of different inter-platform collaboration scenarios.

*Model and simulation setup*

A detailed model description and simulation setup are presented in Pub. V. The model represents a horizontally differentiated area with three platform providers, which compete for three types of users – service providers, complementary service providers, and consumers, each of which need to be present for the successful operation of a platform. Users move in a simulation.
area during the simulation period following a random walk\textsuperscript{12}, representing the changes in supply and demand, and at each iteration evaluate the utility of every platform and make a decision whether to stay with the current platform or switch to another one. The overall platform utility depends on the standalone platform utility (dependent on platform quality and the distance between a user and a platform in a horizontally differentiated simulation space), utility due to indirect network effects (dependent on the number of users of other two types on the platform), switching cost, and price:

\[
V = U_{sa} + U_{ne} - sc - p = U_{q} - c_d + U_{ne} - sc - p, \quad (1)
\]

where \(V\) is the overall platform utility; \(U_{sa}\) is standalone platform utility; \(U_{ne}\) is the utility due to network effects; \(sc\) is a switching cost; \(p\) is the service price (assumed to be equal for all platforms); \(U_{q}\) is the utility due to platform quality (assumed to be equal for all platforms); and \(c_d\) is the cost due to horizontal differentiation, i.e., the cost assigned to the distance between a platform and a user, representing the difference in customers’ preferences and tastes (individual demands). In contrast to our model, a related study of Ruutu et al. (2017) assumed that the platform quality changes depending on the competitive effort of a platform provider, which, in turn, depends on the number of end users: the more the end users, the less the competitive pressure, and the less the effort. The absence of vertical differentiation in our model is a reasonable assumption for mature developed markets. On the other hand, unlike Ruutu et al. (2017), our model assumes that platforms are horizontally differentiated (represented by variable \(c_d\) in formula (1)), accounting for the diversity of agents’ tastes and demands.

Users have two types of switching costs: related to accumulated data and initial investment. Namely, SPs invest in platform application development, whereas consumers invest in IoT devices. The switching cost related to data gradually increases over time eventually reaching a maximum\textsuperscript{13}, showing that consumers and SPs value the accumulated historical data due to data network effects (Mitomo, 2017). The initial investment-related switching cost gradually decreases over time. For comparison, the related study of Ruutu et al. (2017) considered only the end users’ switching cost related to the accumulated data.

The model assumes that service providers can multihome, that is, provide their services on several platforms at the same time. The budgets of service providers are uniformly distributed \(~U(a, 2a)\), where \(a\) is the investment required for entering a platform. The extent of multihoming depends on the level of interoperability between platforms, namely, on the share of investment that can be reused when developing an application for a new platform. Thus, if platforms are not interoperable, the minimum investment of \(2a\) is required for multihoming, meaning that almost all service providers will single-home. On the other hand, if 50% of development investments can be reused, the cost of multihoming on two platforms will become \(1.5a\), meaning that 50% of service providers will multihome.

The time horizon of the simulation was chosen to be 20 years, and a single iteration represents one month. Each simulation was repeated 100 times to calculate average values and standard errors. At each iteration, the total number of users was counted for each platform. After each simulation (20 years, \(20 \times 12 = 240\) iterations) the number of users was averaged for every platform and concentration index HHI (Herfindahl–Hirschman Index) was calculated

\textsuperscript{12} Consumers move 4 times faster than service providers
\textsuperscript{13} It is assumed that recent data is more valuable than old data, and as data gets older, it becomes less relevant for end users. For the modeled mHealth case, the data switching cost is assumed to reach the maximum after about two years.
based on the average number of consumers and services providers for the whole simulation period.

Five different scenarios were defined to represent different market conditions. The scenarios differ in the presence of switching costs, as Table 5.3 summarizes. In the first (base) scenario, switching costs are high: platforms are vertically integrated with devices, and data portability is not possible. This scenario roughly represents the current situation in mHealth: Google Fit and Apple Health are only available for Android (Wear OS) and Apple (Watch OS) devices, respectively. In the second scenario, IoT devices are unbundled from platforms, and therefore can be used with any platform although historical data cannot be transferred to a new platform. In the third scenario, on the contrary, data portability is in place, but devices are bundled with the IoT data platform. In scenario 4, all consumer switching costs are removed. In scenario 5, data-related switching costs are lifted, meaning that not only consumers can keep historical data when switching the platform, but also service providers.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Presence of switching costs</th>
<th>Consumer device</th>
<th>Consumer data</th>
<th>SP investment</th>
<th>SP data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario 1 (Base)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Scenario 2</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Scenario 3</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Scenario 4</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Scenario 5</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.3. Summary of analyzed scenarios (Pub. V)

In Pub. V, several cases representing different market situations were simulated, including service provider multihoming, platform differentiation, and different strength of network effects. However, here only the multihoming case is reported. In the multihoming case, interoperability between platforms is assumed, which allows the reuse of 70% of the initial investment for the service provision on another platform. This implies that 70% of service providers will multihome on two platforms and 40% - on all three platforms.

**Effect of service provider multihoming on competition**

Figure 5.5 presents mean HHI values for the five analyzed scenarios as well as standard deviations of HHI. As the figure shows, in the no-multihoming case, consumer HHI appeared to be higher in Scenarios 2-5 than in the base Scenario 1, meaning that lowering switching costs can counter-intuitively result in decreasing competition. At the same time, the variation of the consumer HHI is also higher in Scenarios 2-5 compared with the base scenario showing that with high switching costs the industry does not significantly deviate from the initial state after 20 simulated years.

In Scenario 5, when data switching costs are lifted for all user types, the HHI significantly increases both for consumers and service providers to the level of around 0.90, showing that one winning platform may take the entire market due to strong network effects. This is different from the results of Ruutu et al. (2017), who found that a high degree of data portability in the long term makes the platform competition more dynamic and prevents the winner-takes-all situation. This disagreement in results likely arises due to the difference in model assumptions. Thus, in the model of Ruutu et al. (2017), platform providers react to the customer churn by increasing the investment in the platform quality, preventing the winner-takes-all situation, whereas in our model the quality is assumed to remain the same throughout the simulation. Therefore, our results complement the findings of Ruutu et al. (2017) by showing that in data platform markets with little vertical differentiation removing data-related switching costs may
lead to monopoly. However, the negative competition effect of decreasing switching costs can be offset by facilitating service provider multihoming. Thus, as Figure 5.5 shows, multihoming can promote competition even in Scenario 5 and keep the HHI on both consumer and provider sides near the initial level. This result agrees with the findings of Ruutu et al. (2017), who discovered that open interfaces, which enable service provider multihoming, prevent the winner-takes-all situation.

Figure 5.5. Simulation results for multihoming versus no-multihoming cases: (A) mean HHI; (B) standard deviation of HHI (Adapted from Pub. V)

Furthermore, a sensitivity analysis with different reuse rates illustrative of various extents of platform interoperability was conducted, which showed that the positive effect of multihoming in promoting the platform competition is more pronounced when a reuse rate is 70% and more (Figure 5.6A). After that, the impact of multihoming on the initially highly concentrated market (HHI = 0.75) was tested. The analysis showed that lowering switching costs with multihoming leads to lower market concentration, whereas the opposite effect is observed in cases with no multihoming (Figure 5.6B).

Figure 5.6. Sensitivity analysis of multihoming case: (A) effect of reuse rate; (B) effect on initially concentrated market (HHI = 0.75) (Adapted from Pub. V)
Generalization to other consumer IoT verticals

Inputs to the models in Pub. V and Section 5.1.2 represent the mHealth case. Namely, the dynamics of data and device-related switching costs, detailed in Section 3.2 of Pub. V, are specific to mHealth. Indeed, while switching costs related to replacing a smartwatch (a wearable device) can be assumed to decline nearly to zero in a year, this assumption does not hold for a connected car. Therefore, results from Pub. V can be fully generalized only to consumer IoT applications with similar dynamic in terms of user switching costs and provider multihoming, such as smart home and connected cars with modular, replaceable OBD (on-board diagnostics) devices. However, the investigated impact of lowering switching costs on competition is relevant for other platform markets with high network effects. Furthermore, the developed research setup can also be used for modeling other verticals.

5.2 Extension of IoT and mHealth providers to telehealth

For understanding a potential position of MPPs acting as mHealth data platform (hub) providers as well as other players from consumer IoT in the ecosystem of a highly regulated telehealth industry, the study of multiple literature types was conducted, including scientific research, patents, and press releases over 15 years from 2002 to 2016. Further, guided by trends detected from the literature analysis, a future ecosystem of the telehealth industry was proposed using the value network configuration (VNC) notations\(^{14}\). The research framework is presented in Section 3.3.1, and the detailed description of the research design is found in Pub. VI. The study took telehealth rather than IoT and mHealth focus in order to position IoT and mHealth among other relevant developments and have an unbiased understanding of their role in the evolution of telehealth.

5.2.1 The evolving role of IoT in telehealth

The results of the analysis of multiple literature types – academic publications, patents, and product press releases are shortly presented in this section.

The analysis showed that wearable devices have been in the focus of telehealth researchers already in 2002-2006, many years before the proliferation of consumer fitness trackers and smartwatches that made the wearable device category familiar to the general public. In 2002-2006, researchers mostly focused on the use of wearables for vital sign monitoring of remote patients and physical activity monitoring of independently living seniors. In 2012-2016, new applications were proposed, including the tracking of mental diseases and facilitation of a healthy lifestyle. Furthermore, the analysis of research publications revealed the increasing importance of mobile health, which was the most frequent keyword in telehealth-related articles in 2007-2011 and 2012-2016. As wearable devices are often bundled with a mobile application, their increase also contributed to the growth of mHealth as a research direction in telehealth.

Furthermore, the analysis showed that many telehealth patents in 2012-2016 were granted to MPPs, MDMs, and other companies from the consumer electronics domain, with fitness wearable device company Fitbit being a notable example. This indicates the contribution of consumer companies to the technological development of telehealth. Moreover, some of the

\(^{14}\) Differences between “business ecosystem” and “value network” terms are discussed in Section 2.1.1. VNC notations can be also used to depict technical and business architecture of the industry ecosystem
Evolution of mobile platform providers for IoT: case mHealth

patents developed by consumer companies were found to serve medical purposes, such as blood sugar measurement using “soft sensors” – algorithms and models that are fed with user-input information or data from generic sensors to estimate parameters that are not directly measured by hardware. This indicates the growing role of data analytics in telehealth.

The analysis of press releases showed that wearables and IoT devices are not yet common in telehealth, likely because of regulatory restrictions. Indeed, consumer IoT devices are not typically approved as medical devices, which prevents their use for medical purposes. However, mobile apps played an important role in newly launched in 2012-2016 telehealth products, with almost every fourth new product release having included some mobile app. Furthermore, application-wise, telehealth products in 2012-2016 appeared to be increasingly focused on wellness management, unlike in 2002-2011, when telehealth applications primarily addressed the disease management, with a particular focus on chronic diseases.

The observed development of telehealth-related literature indicates that the role of wearable devices and mHealth will likely increase in future telehealth facilitated by the growing attention to wellness management in previously mostly disease-focused telehealth, along with the increasing penetration and expanding application scope of wearables and mHealth apps. As a consequence, large data volumes will be generated and managed by patients outside of hospital settings. Given the growing importance of wellness, and wearables increasingly focusing on medical conditions, clinicians are likely to be interested in accessing patient-generated data. In conjunction with the observed in Pub. VI increasing usage of cloud computing and storage in telehealth, we propose that cloud-based health data aggregation platform will emerge and take a central position in a future telehealth value network to facilitate data exchange between an unregulated consumer and a regulated medical domain of telehealth.

5.2.2 Ecosystem of telehealth in recent past

Guided by the trends defined based on the literature analysis and the review of industry news and reports, the ecosystem of telehealth was determined for the recent past (years 2008-2012) and the near future (around the year 2022). The main business roles in the past and future ecosystems of telehealth are presented in Table 5.4.

First, the state of the telehealth ecosystem from the recent past (2008-2012, after the emergence of Android and iOS smartphones) in a developed Western country was considered (Figure 5.7). The ecosystem is divided into two domains: a regulated healthcare provider-driven and an unregulated citizen-driven that can also be viewed as the mHealth data ecosystem (Figure 5.2B). The latter mostly concerns not critical unregulated disease self-management and wellness management tools, which in the recent past were not viewed as the part of telehealth but shown for the reason of consistency with the future industry ecosystem. The wellness management role of citizens was not sufficiently supported by healthcare providers in the past disease-focused telehealth, and this gap was addressed by a number of small lifestyle digital product providers – producers of fitness wearables and developers of apps for lifestyle tracking. Further, personal health digital products for disease self-management were provided by both medical and non-medical companies, which is why the corresponding role is located at the boundary of regulated and unregulated telehealth domains. In the healthcare provider-driven domain, telehealth services were provided in two forms: real-time consultations with a healthcare provider and remote patient monitoring of non-hospitalized patients. The latter typically included a hardware platform that could collect readings from the connected peripherals and send them to a server, where healthcare providers could access them. There was often
no interface between a medical information system (electronic health record – EHR) of a hospital and a telehealth platform.

Table 5.4. Main business roles in the ecosystem of telehealth (adapted from Pub. VI)

<table>
<thead>
<tr>
<th>Business role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disease management</td>
<td>Receiving medical treatment for a disease and monitoring the disease by tracking body and mind parameters</td>
</tr>
<tr>
<td>Wellness management</td>
<td>Taking actions to improve own health and fitness condition and minimize the risks of health problems by following a healthy lifestyle</td>
</tr>
<tr>
<td>Provision of video conferencing platform</td>
<td>Provision and management of tools enabling delivery of healthcare services to remote patients in the form of video consultation</td>
</tr>
<tr>
<td>Provision of remote patient monitoring platform</td>
<td>Provision and management of tools enabling the collection of health parameters of non-hospitalized remote patients and transmission of the data to clinicians</td>
</tr>
<tr>
<td>Patient health care</td>
<td>Diagnostic and treatment of diseases and healthy lifestyle coaching provided to patients, i.e., citizens with diseases</td>
</tr>
<tr>
<td>EHR (Electronic Health Record) usage</td>
<td>Using an electronic medical information system that contains information on patients and digital tools for supporting patient care</td>
</tr>
<tr>
<td>Provision of EHR</td>
<td>Provision and management of software and hardware required for the deployment and operation of EHR</td>
</tr>
<tr>
<td>Provision of disease self-management tools</td>
<td>Provision of tools, e.g., mobile applications or wearables that aim at tracking and measuring health parameters for helping patients to manage their disease</td>
</tr>
<tr>
<td>Provision of lifestyle tracking tools</td>
<td>Provision of tools, e.g. mobile applications or wearables that aim at tracking and measuring the lifestyle for the promotion of healthy living</td>
</tr>
<tr>
<td>Provision of healthy lifestyle coaching</td>
<td>Provision of a personalized lifestyle coaching service based on tracking and analysis of lifestyle data</td>
</tr>
<tr>
<td>Provision of disease self-management coaching</td>
<td>Provision of a personalized disease self-management coaching service based on tracking and analysis of disease data</td>
</tr>
<tr>
<td>Citizen health care</td>
<td>Diagnostic and treatment of diseases, and healthy lifestyle coaching provided to citizens, including sick and healthy people</td>
</tr>
<tr>
<td>Health data aggregation</td>
<td>Collection and harmonization of personal health data from different databases, including patient-generated lifestyle and disease data along with patient’s data generated in healthcare facilities from EHR</td>
</tr>
<tr>
<td>Development of clinical apps</td>
<td>Development of applications for enhancing the decision making of clinicians, e.g., data analytics for automated diagnosis</td>
</tr>
</tbody>
</table>

Figure 5.7. A business ecosystem of telehealth in the recent past (Pub. VI)
5.2.3 Potential future ecosystem of telehealth

The future ecosystem of telehealth will include several new and transformed roles. Accumulated data and evolving AI algorithms will enable healthy lifestyle and disease self-management coaching, which are more engaging and effective than simple tracking of lifestyle and health conditions, which were available in the recent past. The role of healthcare providers will change from patient health care to citizen health care, indicating the shift to preventive and wellness-centric telehealth. EHR providers will build a platform around their product by providing an API for the platform to the third-party developers, as Figure 5.8 shows by a business interface between an EHR vendor and a clinical app developer.

The growing volume of patient-generated lifestyle and disease-related mHealth data, which is scattered over multiple vendor-specific platforms, creates the need for the health data aggregation role that would enable clinicians to access that data. Furthermore, the liberalization of patients’ medical data promoted by regulators in some countries like the UK and US demands the means for opening the patient data stored in medical systems. Therefore, a health data aggregator will emerge that collects the data from the multitude of mHealth applications as well as from the EHR cloud, as Figure 5.8 shows. Apart from enabling sharing the data between citizen and healthcare provider-driven telehealth domains, health data aggregators may also act as data sharing platforms for lifestyle and personal health digital product providers enabling access to complementary data types and promoting the development of innovative applications. In the regulated telehealth domain, healthcare data aggregators will similarly allow new application development by bringing the patient-generated data to the EHR cloud. Furthermore, health data aggregators can enable health information exchange required for maintaining the continuity of care when the services are provided by different healthcare institutions.

Figure 5.8. A potential future business ecosystem of telehealth (Pub. VI)

The health data aggregator will take a central position in the future ecosystem of telehealth, which will motivate various actors to compete for this role. The position on the boundary of
the regulated and unregulated telehealth domains makes the role suitable for different companies, such as MPPs and consumer data companies (Apple, Google, and Facebook), EHR providers (Epic Systems), personal health record providers (Microsoft HealthVault), and governments, particularly in the countries with public healthcare systems. In particular, the largest MPPs Apple and Google that already act as mHealth data platform providers can become health data aggregators by interfacing with EHR vendors. However, establishing and taking that role requires resolving multiple challenges, primarily related to regulations and business models. Nevertheless, literature-based analysis of telehealth showed that the role of mHealth and IoT increased over time, which should urge regulators to work on the policies that would enable the use of consumer IoT devices and mHealth data in healthcare. However, the investigation of possible ways of resolving current regulatory and business model-related challenges is left for future studies.
6. Discussion and conclusions

Since the inception of mobile broadband, the mobile ecosystem has been constantly evolving. While initially the mobile ecosystem was centered around mobile network operators (MNOs) and device manufacturers (MDMs), in the late 2000s platform providers (MPPs) appeared as new stakeholders and shortly became the ecosystem keystones, bringing mobile applications into the picture. The advent of IoT further expands the mobile ecosystem by including new types of devices, applications, and customers.

As Section 4.1 (Pub. I) showed, such new types of mobile devices and customers may have opposite service requirements in terms of data traffic, mobility, and frequency of communications that MNOs need to satisfy for efficient service provisioning. Providing efficient mobile IoT services may further require establishing new collaborations between the existing and new stakeholders of the ecosystem. For example, to implement the remote subscription management service, which is essential for the diffusion of wide-scale mobile IoT, MNOs need to collaborate with UICC vendors, IoT device vendors, and potentially other parties, which can provide components and services to enable eSIM-based RSM. These stakeholders, however, may also compete with MNOs in the provision of subscription management, as Section 4.2.1 (Pub. II) describes. Moreover, for delivering end-to-end IoT service, MNOs may need to team up with IT and big data companies, such as Cisco and IBM. This kind of collaboration, however, is not considered in this thesis due to the scope and time constraints.

Similarly, MPPs need to establish new collaborations to deliver their IoT products efficiently. MPPs have entered the IoT with consumer wearable devices, which allow constant tracking of physiological parameters and therefore can be used for health monitoring. To enhance the value of such mobile health data and enable efficient data-based application development, different data sources must be combined. This, in turn, requires establishing a sub-ecosystem of mHealth data complementors. For creating and sustaining such a sub-ecosystem, as Section 5.1.1 (Pub. IV) summarizes, MPPs and other potential platform providers must take decisions defining the platform design (e.g., platform API rights), governance (e.g., platform openness), and scope of shared data (e.g., granularity). Apart from ensuring the ecosystem growth and control, these decisions must resolve competitive tensions that emerge between data providers in such platforms due to the threat of data shared by providers being used to substitute their in-house service. Furthermore, to avoid monopoly in the data sharing ecosystem, platform providers themselves must collaborate to enable sufficient interoperability that would facilitate easy multihoming for app developers and service providers (Section 5.1.2, Pub. V). Finally, if such an mHealth data sharing platform and a sub-ecosystem around it are successfully created and managed, MPPs can position their platform at the boundary between the unregulated consumer and regulated medical domains of healthcare, enabling the data flow between the two...
domains, as Section 5.2 (Pub. VI) describes. From the mobile ecosystem’s evolution viewpoint, this can be considered as further expansion of ecosystem boundaries.

Before the emergence of IoT, the main stakeholders of the mobile ecosystem – MNOs and MPPs – collaborated in serving the same group of consumer customers. In IoT, initially, the paths of MNOs and MPPs have diverged, with the former mostly having focused on serving industrial business customers and the latter initially having aimed at deepening relations with existing consumer customers and app developers by offering new products (HW – wearable devices and SW – data platforms). However, recently, MPPs started to target the industrial IoT domain, with healthcare being a prominent and perhaps the most advanced example. Similarly, MNOs are catching up with consumer IoT offering various solutions in, e.g., mHealth and smart home. Therefore, with the development of IoT, MNOs and MPPs need to reestablish their cooperative and competitive relationships in the mobile ecosystem. Such new relationships can be similar to the ones they had in the pre-IoT ecosystem, with MNOs providing connectivity and selling the devices, and MPPs producing devices and enabling application development. However, the stakeholders may also want to change the distribution of existing roles. Such changes are further facilitated by new technologies, such as eSIM. For example, delivered by MPPs wearables are increasingly cellular-connected with eSIM. To ensure these devices are supported, MPPs have to collaborate with MNOs and agree on the terms of remote SIM provision for their wearables. At the same time, MPPs may want to provide mobile connectivity to such devices, thereby starting to compete with MNOs. Such connectivity provision of MPPs can further extend to handsets and trigger market dynamics presented in Section 4.2.2 (Pub. III). Therefore, IoT does not only extend the mobile ecosystem, but it may also change the traditional human communications part of the ecosystem.

Overall, with the advent of IoT, new devices, customers, and applications will be included in the mobile ecosystem, thereby prompting significant changes in service provisioning, collaboration, and competition, which this thesis analyzed. To adapt to these changes and take new roles in the ecosystem, MNOs and MPPs have to develop new knowledge and competencies, potentially utilizing the results of this thesis. Apart from MNOs and MPPs, the results can also be useful for other stakeholders of a broader mobile ecosystem, such as policymakers (Table 6.1).
<table>
<thead>
<tr>
<th>Research question</th>
<th>Pub</th>
<th>Main results</th>
<th>Main implications</th>
</tr>
</thead>
</table>
| RQ1. How do mobile IoT usage patterns differ from consumer devices and across industries? | I   | - In average, mobile IoT devices generate about 150 MB of traffic per four weeks.  
- 92% of IoT devices generate more uplink traffic than downlink.  
- The IoT traffic is highly periodic: devices often transmit every 6, 12, or 24 h.  
- IoT devices can be divided into three clusters based on temporal traffic profiles.  
- Mobile IoT usage patterns differ from consumer devices and across industries in the average traffic, traffic composition (uplink vs. downlink), and device mobility. | - MNOs get a better understanding of the differences in IoT usage patterns across industries that can help to define and provide virtual network slices that are optimized for industry/use case.  
- Defined temporal trends can be used for the forecasting of IoT traffic and device feature diffusion.  
- Researchers can refine IoT traffic models using empirical observations provided in Pub. I. |
| RQ2. How could embedded SIM technology affect the mobile ecosystem?                  | II, III | - Several VNCs of eSIM-based RSM are feasible that may bring to power different ecosystem actors: HW vendors (producers of IoT modules and UICC), connectivity providers (MNO and MVNO – IoT connectivity provider), or IoT SPs.  
- eSIM can enable the dynamic multihoming of consumer devices. Depending on the actions of stakeholders and market development, multihoming may reach high market diffusion or fail to take off.  
- If eSIM multihoming diffuses, the competition between operators will become more intense, with operators competing for communication sessions rather than subscriptions. | - Defined VNCs can be used for evaluating RSM solutions and designing regulatory policies.  
- Regulators, MNOs, and MDMs can use the models to better understand potential eSIM implementations, diffusion of eSIM multihoming, factors that are affecting this diffusion, and its possible consequences. This understanding can improve strategic planning and suggest mechanisms that can be used to drive the ecosystem evolution in desirable directions. |
| RQ3. How could collaboration and competition be governed in emerging consumer IoT data platforms and particularly mobile health data platforms? | IV, V | - Key design and governance decisions are defined that can affect generativity and control of mHealth (and more generally consumer IoT) data sharing platforms and can be used for managing relations with complementors.  
- Not only platform providers, but also data providers that use the platforms of third parties can govern data sharing by defining the scope of shared data.  
- To promote competition, consumer IoT data platforms must be interoperable and enable both data portability and service provider multihoming, whereas data portability alone may result in monopoly. | - MPPs can use the identified decisions as mechanisms for affecting platform generativity and control.  
- Consumer IoT stakeholders willing to establish a data platform can rely on the identified decisions for defining the design and governance of the platform.  
- Regulators and platform providers can make more informed decisions based on the investigated potential competitive impacts of different extents of interoperability in consumer IoT data platforms. |
| RQ4. How could mobile platform providers acting as mobile health data platform providers position themselves in the ecosystem of the healthcare industry? | VI | - The role of consumer wearable IoT devices and mHealth is likely to increase in future telehealth due to their enhanced capabilities, along with the growing attention to wellness paid in healthcare.  
- A health data aggregation role may emerge in the telehealth ecosystem to enable data exchange between the unregulated consumer and regulated medical domains, creating a business opportunity for MPPs. | - Regulatory bodies and governments can make more informed decisions when formulating policies for enabling the use of consumer IoT devices and mHealth data in telehealth.  
- MPPs and other stakeholders can better position themselves in the telehealth industry knowing its evolution and trends. |
6.1 Summary and implications

The thesis makes several contributions, which answer the four research questions presented in Section 1.2:

1) The study characterized the usage patterns of mobile IoT and indicated their differences from consumer devices and across industries.
2) The study showed how eSIM-based remote subscription management could change the mobile ecosystem by constructing potential value network configurations of eSIM and further demonstrated potential competitive impacts of eSIM.
3) The study defined the design and governance decisions as well as interoperability-related policies that could be used for governing collaboration and competition in data platforms in mobile health and other consumer IoT domains.
4) Based on the identified trends of the evolution of telehealth, the study determined roles that MPPs can take in the ecosystem of traditional healthcare.

Table 6.1 details the main results of the thesis and their implications, which are further discussed in sections below.

6.1.1 New usage patterns brought by mobile IoT

Traffic and mobility patterns of IoT devices significantly differ from traditional mobile handsets. Thus, IoT devices were found to generate less traffic than smartphones – around 150 MB for IoT (Pub. I) vs. 14200 MB for consumer devices in Finland (tefficient AB, 2018). However, a widespread belief that IoT devices generate “a few kilobytes of data per day” (e.g., Guerzoni et al., 2014) proved to be inaccurate at least for mobile IoT: an average device appeared to generate several megabytes of data per day, and the trend is growing. However, the main challenge of MNOs in the IoT age will likely be not adding capacity for serving IoT devices, but accommodating diverse IoT use cases, which impose different requirements on the service. Thus, Pub. I compared the mobile IoT usage patterns across seven industries, and found that in some industries IoT uses and devices do not seem to have much in common except for being labeled as “IoT.” Thus, industries differ in generated traffic – from 10 MB to 2 GB per month, in the presence of weekday-weekend patterns, in the traffic composition – uplink vs. downlink, in mobility – with an average device visiting from 1 to 40 unique cells monthly, and in temporal traffic patterns. Furthermore, the clustering in Pub. I showed that even seemingly narrow industries, such as Electricity and gas, have different IoT use cases, further increasing the complexity of defining and serving customers’ needs. Therefore, although Pub. I provides an initial understanding of mobile IoT usage patterns across industries, further analysis may be required for defining the parameters of virtual networks optimized for addressing the diverse needs of diverse customers. Such virtual networks (network slicing) are expected to play a crucial role in future 5G networks.

At the same time, the use of mobile IoT across industries exhibits some similarities. Notably, unlike smartphones, most of the IoT devices (namely, 92%) generate more uplink traffic than downlink. Furthermore, many IoT devices are stationary, with 75% of the devices visiting not more than three unique cells in a month. Moreover, IoT traffic is spatially concentrated, with 10% of cells carrying 93% of IoT traffic. Therefore, before technologies required for network
slicing become more mature, MNOs should consider these fundamental differences between IoT and human device traffic when defining IoT service offerings.

To summarize, the results of Pub. I have implications primarily for MNOs, who can consider them when planning and dimensioning their network, and designing new IoT service offerings for various industries.

6.1.2 Value networks and impacts of Embedded SIM

Remotely programmable Embedded SIM may be the first strategically important development in the nearly 30-year history of SIM technology. With eSIM, the conventional one-to-one mapping of SIM and mobile device is likely to change, as one eUICC can contain the subscriptions of several operators. This, in turn, may deprive MNOs of customer “ownership” and increase the already high risk of the commoditization of MNOs’ services. Such a potentially disruptive effect of embedded SIM could have served as a motivation for GSMA to take control of the specifications development that would otherwise have been led by device manufacturers (e.g., Apple). Therefore, GSMA Embedded SIM specifications expectedly protect mobile operators’ interests by, e.g., imposing unnecessary restrictive rules, such as the requirements of one active profile at a time and explicit user intent for switching between profiles that effectively prohibits automatically triggered profile changes. Moreover, in 2018 the US Justice Department suspected collusion between AT&T, Verizon, and GSMA to hinder eSIM-enabled profile switch (Kang, 2018). Nevertheless, eSIM is gradually becoming a reality, and under the pressure of end users and other ecosystem stakeholders, including regulatory authorities and MDMs, the restrictions, including the ones grounded on specifications as well as the ones set up in subscription contracts, could be lifted, thereby decreasing the power of MNOs.

Section 4.2 studied possible impacts of embedded SIM on the structure of the mobile ecosystem and competition within. Two cases, namely, eSIM in IoT and consumer devices, were considered separately because of the differences in contractual terms (long-term contracts in IoT vs. non-binding contracts in consumer devices), which lead to different market dynamics. Pub. II showed that even in a less dynamic IoT segment the position of MNOs in the future mobile ecosystem could be challenged because the provision of subscription management service is of interest to many stakeholders, including UICC and IoT module vendors, non-MNO connectivity providers, and IoT service providers. Thus, while the mobile operator-driven VNC, which is similar to the solutions promoted by some operators\(^\text{15}\), lets MNOs retain customer ownership, with IoT connectivity provider-driven VNC, operators lose direct customer relationships, implying a more significant business change. However, such a VNC is hard to implement because of the need to collaborate with multiple MNOs, which requires high bargaining power of IoT connectivity providers. On the other hand, the largest MPPs Apple and Google are increasingly diversifying toward IoT, and therefore they may have interest and power to become IoT connectivity providers at least for devices produced by them. At the same time, the UICC and IoT module vendor-driven VNCs are easier to implement than the IoT connectivity provider-driven, and therefore they are more likely to become a reality. Moreover, such VNCs may look more appealing to IoT SPs than the MNO-driven VNC because they can provide wider operator reach and more likely to help to avoid lock-in.

\(^{15}\) e.g., Global M2M Alliance and Bridge Alliance
Slightly different VNCs can emerge around eSIM-based RSM service for consumer devices. However, once an eUICC is loaded with several profiles, the architecture of remote provisioning becomes irrelevant because the profile switch may happen locally on a device, reducing the power of MNOs to control the process. Although MNOs can still inhibit the seamlessness of switching by, e.g., setting a policy requiring the profile removal once it gets disabled, regulators may prohibit such restrictive practices. Provided that eSIM is technically supported by operators and handsets, eSIM multihoming can start penetrating the market. The diffusion of eSIM multihoming is more likely to progress if customers are not satisfied with the quality of a mobile connection they get with single-homing. As Pub. III showed, if eSIM multihoming penetrates the market, the competition in the mobile ecosystem may considerably change due to operator switching happening on the scale of minutes and seconds rather than years and months. The impact of such new dynamics on infrastructure competition may be negative in sparsely populated areas, meaning that regulators should impose coverage requirements to guarantee service accessibility. Overall, eSIM, initially designed for IoT devices, may disrupt a human communications’ part of the mobile ecosystem by enabling dynamic multihoming. To protect their business from the potentially negative impact of eSIM multihoming, MNOs should provide sufficiently good quality of single-homing, diminishing the benefits of combining several operators.

Overall, the impact of eSIM on the mobile ecosystem can be different depending on its implementation, as illustrated by color coding in Figure 6.1. Thus, eSIM available solely for IoT devices with the MNO-driven VNC will cause the least changes to the mobile ecosystem, whereas if eSIM is used in handsets and eSIM multihoming reaches high penetration, its competitive impacts are likely to be significant. The recent announcement of eSIM support by the largest MPPs/MDMs Apple and Google suggests that the competitive impact of eSIM will likely be at least medium. Moreover, since MDMs become the owners of eUICCs, they could act as a “gateway” for mobile subscriptions and charge MNOs for the activation of their subscriptions. Finally, MDMs can even introduce their MVNO hiding the serving MNO from end users.

![Figure 6.1. Potential implementations of eSIM and their impacts on the mobile ecosystem, from the least significant (white) to the most significant (dark green)](image)

In terms of implications, VNCs of RSM in Pub. II can help the involved stakeholders of the mobile ecosystem recognize potential business architectures of RSM and their features, which is an essential first step of implementing the service. Moreover, the comparison of potential VNCs can facilitate IoT SPs in making a more informed decision on choosing a provider of RSM service from the available alternatives. Furthermore, regulators can promote or discourage particular VNCs to prevent lock-in and facilitate efficient service provisioning. The models
Discussion and conclusions

from Pub. III help to understand the potential future evolution of the mobile ecosystem and identify levers (variables) that ecosystem stakeholders, primarily MNOs, regulators, and MDMs, can use to affect that evolution. Moreover, regulatory bodies can use the models and identified scenarios for defining whether and how to promote eSIM and multihoming with dynamic network selection. Furthermore, researchers and practitioners can build on the presented in Pub. III conceptual models and quantify the impact of eSIM with dynamic multihoming on the competition once reliable numerical input becomes available.

6.1.3 Governance of consumer IoT data platforms

MPPs extend the mobile ecosystem by providing platforms for consumer IoT data sharing, therefore creating a new “sub-ecosystem” of data complementors. IoT data sharing platforms are most mature in mobile health, although similar platforms are being established by various actors in other IoT domains, such as the connected car, smart home, and smart city. Establishing and sustaining a “sub-ecosystem” of data-based developers requires careful governance of collaboration and competition with complementors and other platforms that were analyzed in Pub. IV and V, and summarized in Section 5.1.

The governance of collaboration and competition with platform complementors involves maintaining the tradeoff between platform generativity and control. Platform providers use boundary resources to manage this tradeoff. Therefore, Pub. IV analyzed the boundary resources of mHealth data sharing platforms to understand the decisions that providers make to govern the collaboration and competition with platform complementors. Interestingly, the results showed that not only platform providers, but also data providers that use platforms of other parties could govern the terms of collaboration by defining the scope of data they open to third parties. For example, a data provider may decide to keep some data types proprietary or share only coarse aggregated data. Although such limitations can protect the provider’s in-house service from competition, the generativity of such limited data is low, and therefore, data consumers may have not enough motivation to collaborate. In general, the generativity of data is highest when all available data types are opened for sharing, the data is provided immediately and with the highest possible resolution.

Furthermore, apart from the decisions related to the governance of data scope (Table 5.2), platform providers can use other, unavailable to platform consumers, mechanisms for governing the relationships with complementors. Such mechanisms include, for example, setting platform API rights, API usage rate limitations, platform openness, and a price. Such decisions can affect generativity or control directly (e.g., platform openness) or indirectly (e.g., supported data formats). Moreover, platform providers can change the API or discontinue the complementor’s platform access altogether, which puts them in a strong position. That is why MPPs and other mHealth companies with a high customer base, and therefore market power, commonly play a platform provider role, whereas smaller companies often act as platform consumers (Figure 5.3).

Apart from collaborating with platform complementors, platform providers should cooperate with each other to ensure interoperability and market growth. Agent-based simulation of consumer IoT data ecosystem conducted in Pub. V showed that competitive, and therefore socially optimal outcome, could be achieved with a certain level of interoperability that allows end users and service providers transferring their data freely between platforms and at the same time enables easy service provider multihoming. Somewhat counterintuitively, removing data switching costs and allowing data portability alone is not enough for ensuring market
competition, and, on the contrary, results in a winner-takes-all situation due to strong network effects. Therefore, to reach a competitive market, platform providers should collaborate and pay more attention to the standardization of data models, devices, and APIs that can make service provider multihoming easier. In other words, a certain level of interoperability (collaboration between competing platforms) is required for promoting market competition, whereas mandating data portability alone is not enough for reaching an efficient market outcome.

In terms of implications, the results on the governance of collaboration and competition in consumer IoT data sharing are relevant to various stakeholders. Thus, design and governance decisions from Pub. IV can be used by MPPs and other mHealth and consumer IoT data platform providers as mechanisms for affecting generativity and control. Moreover, the identified decisions can be used in planning or evaluating data sharing platforms in other consumer IoT domains. Furthermore, Pub. IV is one of the first that provides a practical example of analyzing boundary resource documentation for understanding the mechanisms of platform design and governance. Therefore, research design developed in Pub. IV can be used by researchers for studying the design and governance of API-enabled platforms in other fields, not necessarily related to IoT. The results of Pub. V, in turn, can be used by regulatory and standardization bodies, along with platform providers for designing policies to promote the competition in the ecosystems forming around data in consumer IoT domains, such as mHealth and smart home. Finally, the results of Pub. V showing the impact of low switching costs on competition contribute to the theoretical understanding of competition in markets with network effects.

6.1.4 The role of mobile platform providers in healthcare

The healthcare industry, particularly its remote delivery mode, generally referred to as telehealth, can be the next step in the evolution of MPPs operating in the mHealth domain after they establish their mHealth data platforms. The analysis showed that telehealth researchers were already paying a lot of attention to wearable devices in 2002-2006, although, at that time, wearables were medical devices provided to patients by healthcare providers for short-term use. Nowadays, with the growing attention to wellness management in previously mostly disease-focused healthcare and with the increasing capabilities of mobile technologies, consumer-owned wearables and mHealth are increasingly often discussed in new telehealth-related scientific publications, inventions, and product releases. This indicates the growing role of wearables and mHealth for telehealth and healthcare.

As a consequence of mHealth proliferation, an increasing amount of potentially valuable health data is generated outside of clinical settings. This creates the need for a role that would establish a data flow from the mHealth ecosystem, which can be viewed as an unregulated citizen-driven domain of telehealth, to the regulated healthcare provider-driven domain. Because of the location of this role on the boundary between the two domains of telehealth, various actors can take it. Thus, MPPs, namely Apple or Google (the citizen-driven domain), which already act as mHealth data platform providers, may become health data aggregators by interfacing to medical EHR systems. In fact, in 2018, Apple integrated its Health platform with EHRs of several hospitals in the USA (Comstock, 2018), thereby taking another step to becoming a health data aggregator. On the other hand, EHR providers (the healthcare provider-driven domain) could also be interested in taking this gateway role.

However, strict regulatory requirements complicate the data flow between the two domains of telehealth. For example, entities that are processing and storing medical data must be compliant with General Data Protection Regulation (GDPR) in the EU and the Health Insurance
Portability and Accountability Act (HIPAA) in the US, both of which require deploying privacy and security protection mechanisms that could be costly to implement. Furthermore, lengthy clearance procedures of medical devices, which the manufacturers of consumer wearables must undergo to enable the use of their devices in the regulated medical field, restrict the dissemination of wearables and IoT into the healthcare industry. Nevertheless, recently, regulatory authorities in the USA made the first steps toward enabling the use of consumer technologies in healthcare by introducing the “fast track” software precertification pilot program, with Apple, Google, Samsung, Fitbit, and other five companies included in the pilot (U.S. Food and Drug Administration, 2017). Such actions may facilitate the use of wearable devices and mHealth apps and promote the extension of MPPs to the healthcare industry.

The results of this study have implications for industry stakeholders. In particular, understanding the evolution of telehealth can help MPPs and other consumer companies position themselves in the industry. Furthermore, regulatory bodies can make more informed decisions when formulating policies regulating the use of consumer IoT devices and mHealth data in telehealth. Finally, researchers can use the proposed framework and research setup for analyzing the evolution of other industries.

6.2 Limitations

This study has some limitations that need to be noted. For example, the evolution of the mobile ecosystem was analyzed by taking the viewpoint of main ecosystem stakeholders that have acted as keystones at different evolution stages – MNOs and MPPs. Therefore, the resulting view on the ecosystem evolution may miss certain aspects that arise due to other ecosystem stakeholders. Nevertheless, due to time constraints, broadening the scope would require decreasing the depth of studying the chosen evolution aspects. Therefore, by focusing on the main stakeholders, this thesis tried to reach the tradeoff between research depth and breadth.

For the same reason, this thesis did not consider some aspects of the ecosystem evolution that are relevant to MNOs and MPPs. Notably, the developments articulated at later stages of the thesis research process were not considered. For example, in 5G, industrial customers can act as micro-operators by obtaining a local mobile spectrum license from the regulator or MNOs (Ahokangas et al., 2018). Such a seemingly significant change in the mobile ecosystem was not addressed because of its recency.

Furthermore, this study analyzed the positions of MNOs and MPPs in industrial and consumer IoT domains, respectively. Although this view on the stakeholders’ focus is accurate for the initial stages of IoT development, in the future, both stakeholders can extend their operations to their currently uncovered IoT domains. For example, recently, one of the largest MPPs Apple showed its interest in industrial IoT by collaborating with GE in developing the ecosystem of apps for industrial IoT that would work with iPhone and iPad (Apple, 2017). Similarly, consumer IoT devices directly connected to a mobile network are more and more common, increasing the role of MNOs in the consumer IoT domain. These evolution aspects can be considered in future research.

Moreover, the choice of mobile health domain for studying the evolution of the mobile ecosystem toward consumer IoT imposes generalizability limitations. For example, Pub. V includes mHealth-specific assumptions on switching costs, which affect the dynamics of the model. Nevertheless, consumer IoT domains have many similarities, and therefore, the main findings of Pub. IV and V presented in Section 5.1 are relevant to other consumer IoT verticals.
However, with respect to them, the results in Section 5.1 may be incomplete, as they neglect the particularities of the domains other than mHealth. For example, unlike in mHealth, data platforms in the smart home domain must also support device actuation and therefore may require additional mechanisms for the governance of platform complements.

The methods and assumptions adopted in this research also impose certain limitations. For example, the results of the quantitative analysis in Pub. I could be limited in generalizability as they rely on the data from a single mobile operator. In addition, Finland is one of the most advanced countries in mobile IoT diffusion and mobile internet traffic volume, suggesting that the findings of Pub. I are possibly not representative of other developed markets. Moreover, the fast pace of IoT development may limit the predictive value of the analysis, as industries are continuously adopting new IoT applications, thereby changing usage profiles. Nevertheless, the results of Pub. I could serve as a benchmark for other operators, which is especially valuable considering the limited existing related studies.

The value network configuration method adopted in Pub. II and VI also has some limitations. Although the method enables a structured way of constructing potential technical and business architectures of an industry for reducing uncertainty, it does not allow evaluating the probability of VNCs becoming a dominant design. Therefore, while VNCs in Pub. II and VI provide decision-makers with initial tools for planning, they should be complemented with other knowledge for making more informed decisions.

The qualitative system dynamics method adopted in Pub. III similarly imposes some limitations. Namely, qualitative models do not produce definite numerical estimates that could be directly used for forecasting and making, e.g., investment decisions. However, when the problem under investigation is futuristic, and no reliable quantitative input is available, as in the case of eSIM, qualitative scenarios help to decrease uncertainty about the future without the risk of producing wrong numerical outputs due to multiple assumptions. Furthermore, as Pub. III relied on expert interviews in constructing and testing the models, its results could be limited because some stakeholder groups, such as SIM vendors and device manufacturers, were underrepresented among the interviewed experts, and some others, such as MPPs, were not interviewed at all due to the lack of their presence in Finland. Nevertheless, this limitation was partially compensated by the information from web sources, which express these stakeholders’ viewpoint on the development of eSIM.

In Pub. IV, the analysis of collected on the web boundary resource documentation may be limited in having studied only openly available documents, whereas API references and the terms of use of moderated platforms are only available to approved developers. Because of this, some platform governance mechanisms may have remained undiscovered. However, most mHealth data sharing platforms are open, meaning that they were included in the analysis. Furthermore, the results of boundary resource analysis were discussed with five experts only. However, the interviews in Pub. IV were conducted to refine the results and not to validate them. Further, the results of agent-based simulation in Pub. V are limited because the models relied on assumptions in the absence of real input data. However, sensitivity analysis increases the reliability of modeling results. Lastly, although adopted in Pub. VI multi-level quantitative literature analysis provided a comprehensive view on the evolution of telehealth, the reliability of results may be limited as the method is sensitive to the keywords selected for the document search. While the keywords for Pub. VI were iteratively chosen by all authors, they were not confirmed with industry experts, meaning that some aspects of telehealth evolution might have left undiscovered.
Finally, since the research in this thesis is future-oriented, uncertainties and ambiguities may limit the reliability of the results. For example, embedded SIM technology is still under development, and no wide-scale real-world implementations of remote subscription management for IoT or consumer devices exist. Nevertheless, in the face of such uncertainty, future-looking research is particularly valuable.

6.3 Future work

The scope of the thesis imposed limitations on the analyzed aspects of ecosystem evolution. However, such unaddressed aspects can be viewed as opportunities for future research. Thus, taking the viewpoint of stakeholders other than MNOs and MPPs can produce additional insights into the ecosystem evolution. For example, it would be interesting to study whether mobile infrastructure providers like Nokia and Ericsson diversify to adjacent markets along the way to IoT, and how the Internet and mobile giants like Facebook and Microsoft grasp the opportunities provided by IoT.

In addition, the models developed in this thesis would benefit from further elaboration. For example, system dynamics models from Pub. III can be quantified, and agent-based models in Pub. V can be improved based on the real data once it becomes available. Moreover, the research on data platform governance can be extended by quantitatively studying the impact of the decisions identified in Pub. IV on platform generativity, control, and overall success.

Furthermore, the analysis of the mobile IoT usage from Pub. I can be extended by using more granular data and adding the data from other operators’ networks for making more accurate inferences. However, even building on our rather high-level analysis, future studies can propose the ways of optimizing the service quality for specific industries and use cases. In addition, the identified traffic patterns can be used for developing new pricing models for mobile IoT.

Finally, future research should pay closer attention to the emerging in IoT data platforms. While this thesis analyzed the governance of consumer IoT data platforms on the example of mHealth, data platforms are also likely to play a critical role in the smart city ecosystem. Leading such an ecosystem seems to be of high interest to both MNOs and MPPs. Due to the emergent nature of smart cities, there are possible multiple directions for future studies. For example, technical implementation and ownership of data platforms in smart cities remain uncertain (Vijay, 2018). Therefore, future studies can propose and evaluate different models of such platform implementation.
References


Casey, T., Smura, T., & Sorri, A. (2010). Value Network Configurations in wireless local area access. In 2010 9th Conference of Telecommunication, Media and Internet (pp. 1–9). Gent: IEEE. https://doi.org/10.1109/CTTE.2010.5557719


References


Flock, U. (2009). *An Introduction to Qualitative Research* (Fourth). SAGE.


References


References


88


References


