The interplay of risks on digital platform openness – a case study

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Management of Technology**

Faculty of Technology, Policy and Management

by

Noah Brandwijk

Student number: 4958411

Date: 29-06-2020

To be defended in public on July 13 2020

Graduation committee

Chair/First Supervisor: Dr.ir. G.A. de Reuver, Information and Communication Technology
Second Supervisor: Prof.dr.ir. I.R. van de Poel, Ethics/Philosophy of Technology
External Supervisor: ir. K. V. M. Meeuwisse, Deloitte

Preface

This thesis demarks the end of my time at Delft University of Technology and the Master programme Management of Technology. Writing this thesis was a mind-broadening experience. For that I am thankful. Moreover, the topic of digital platforms never failed to spark my curiosity. Therefore I enjoyed writing this thesis. It is a topic that is highly relevant and one that affects society as a whole. Besides, I hope to have provided a meaningful contribution to both theory and practice. Nonetheless, this thesis would not have been achieved without the support of some people. I want to use this preface to thank them.

First, I want to thank Dr.ir. Mark de Reuver, chair and first supervisor of this thesis. I really enjoyed our discussions on the more conceptual topics of doing research and debating the findings. In addition, I am thankful for your critical view that motivated me to do better. Secondly, I want to thank Prof. Ibo van de Poel for the interest shown in the study since our first meeting and the helpful feedback during the writing of the thesis. Thirdly, I want to thank ir. Kirsten Meeuwisse, for your support in tackling the challenges of this thesis while also inspiring me to improve my work. Fourthly, I want to thank the case informant for his support of this research and helping me gather useful data. In addition, I want to thank the interviewees of the case for providing me with their time and a very interesting case.

Finally, I want to thank my family, friends and girlfriend for their continued support these past years and particularly these past months. Without your support I would not have achieved this!

Noah Brandwijk

29-06-2020, Rotterdam

Executive summary

A platform needs to have sufficient market potential, represented by the number of users who can join a platform. Platform openness affects the ease of actors joining the platform. Hence, in order to increase the chances of platform success, platforms want to maximize market potential and consequently also platform openness. This is problematic because architectural configurations with the highest market potential do not necessarily represent the most favourable configurations for societal values. Although there is anecdotal evidence of safety and privacy risks resulting in adjusted platform openness, there is little literature explaining the drivers and the process of adjusting due to risks posed to societal values. Hence, this thesis aims to build an initial theory on the process of how digital platforms adjust their platform openness upon learning about risks for societal values. Accordingly this research aims to answer the following research question: *How does a digital platform sponsor adjust openness upon learning about safety and privacy risks?*

To develop an answer to the research question a case study was performed at a digital platform sponsor. Specifically, the case investigates a Dutch digital payment provider. The case was selected on account of having adjusted their openness upon learning about risks in their platform ecosystem. First, existent literature was used to develop a conceptual model. The model explains the process of how and why the platform sponsor adjusts its openness due to risks. Accordingly the case study described the empirical process. Using pattern-matching, the conceptual model and empirical model were compared. Based on this comparison, conclusions were made on the validity of using the selected theories to predict the process. Any new findings were added to the conceptual model.

An interdisciplinary selection of literature was combined to construct a conceptual model on how platform openness changes. Theory on legitimacy provides an explanation for why a platform would want to change their practices due to societal risks. Legitimacy theory conceptualizes that an organization's actions are desirable within a system of public norms, values and beliefs. Furthermore, descriptive theories on organizational learning explain the process of organizational change (i.e. learning). Whereas the concept of double-loop learning describes the process of organizational change.

In contrast to legitimacy theory, theory on responsible innovation explains why an organization changes without a threat to legitimacy. Legitimacy theory suggests that a risk that is not known to the public, might not motivate an organization to act. Hence, theory on responsible innovation fills this gap by providing an alternative understanding of this process. Whereas the values and beliefs of agents can motivate change without a risk present. Analogous to real-life an agent might be motivated to show certain behaviour due to an extrinsic reward (e.g. threat to legitimacy). Yet, behaviour can also be triggered by an intrinsic motivator (e.g. values/beliefs). Moreover, the concept of second order learning also explains how these values and beliefs can change.

Based on interviews and documents it was found that the empirical process starts with risk identification. Whereas risks are primarily first identified due to a form of interaction with the public. Moreover, it was found that societal risks do negatively affect the legitimacy of a platform. A threat to legitimacy can form a threat to an organization's continuity. Hence, an organizational crisis or questioning can occur. In addition, instead of only safety and privacy risks, a broader spectrum of risks was uncovered. Due to the exploratory nature of this research these risks were also analysed.

If the threat to the current way of working outweighs the benefits/hinderances will the organization change. As the threat outweighs inhibitors of change, a crisis might result in changed norms, strategies and even assumptions. Regardless, it was inconclusively found whether societal risks affect the values of the organization. Nonetheless, it could be observed that a platform's responsibility and duty of care are

affected as a result of organizational learning. In addition, it was found that theories-in-use of the platform did change and resulted in an adjusted openness.

Interesting additions to theory include the finding that organizational maturity seems to grow alongside a platform's legitimacy. As a result of this, risks that might threaten an older organization's legitimacy, might not threaten the legitimacy of a start-up. Another relationship found tied to the legitimacy of the organization is responsibility.

Moreover, it was observed that privacy risks were better anticipated on than other risks. Two possible reasons were found. Firstly, responsibility of a privacy risk is clearer than external risks. Secondly, privacy risks are more recognizable than risks such as misleading consumers. Both reasons have support from interviews gathered in the case. A third contextual factor might also be the increasing attention to privacy over the years. Ultimately also coinciding with the introduction of the GDPR.

Ultimately, the propositions derived from the conceptual model aligned mostly with empirical findings. Nonetheless, some nuance was necessary to the propositions to see whether the propositions were met in practice. The propositions of legitimacy were indeed met from a theoretical perspective. Similarly survival and learning tensions were observed. This concept described the mechanism that explains why theories-in-use changed. Regardless, upon further inspection changed background theories were complex to measure. Hence, there remain alternative explanations that explain behaviour of the organization as motived by financial gains instead of changed values.

An alternative explanation is that instead of values, financial gains moderated platform openness. Due to the effect of social desirability, it remains questionable whether certain actions were performed due to moral reasons. For example, a decision might be made due to moral reasons or to increase ones reputation. However, there were also instances where the platform forewent financial benefits in the face of values such as privacy. Thus, future research such as longitudinal case studies is necessary to better capture potential changes in values.

To answer the main research question this research developed an initial theory. This theory describes how a digital platform sponsor adjusts openness upon learning about societal risks. Whereas this process is characterized by the interaction between the platform and its ecosystem. this critical case suggests that threats to societal values do affect openness. As described in theory on organizational learning a threat of a crisis or realized crisis might incur change in an organization. Yet, it remains questionable whether a platform's value system actually changed. Nonetheless, changes to theories-in-use of the organization were observed. As result of this, different norms, assumptions and strategies led to an adjusted platform openness.

This research also has several theoretical implications. First, the study provides an initial theory on how a platform sponsor adjusts openness upon learning about certain risks. More specifically, the theory builds upon prominent theories from the fields of organizational learning, legitimacy theory and responsible innovation. Secondly, this research provides a new perspective on how platforms evolve over time by connecting previously unconnected literature streams. Hence, this research provides a first account on how endogenous drivers drive platform evolution.

Finally, this research also has practical implications. Whereas this research highlights the need for responsible platforms. As digital platforms such as in the Internet of Things domain become increasingly pervasive in society, these platforms also have access to increasingly more physical parts of life and data. This research highlights that open platform have negative externalities too. Hence, this research can be used by platforms to understand how openness can also have negative consequences.

Contents

1. Introduction

1.1 Problem definition

In recent years there has been an ongoing trend in how organizations compete against each other. Instead of product and service competition, organizations are increasingly moving towards platform-based forms of competition (Tiwana, 2014). Examples of such digital platforms are Facebook, Amazon, Apple and Microsoft, among many others. A digital platform is a software-based product or service that can be a host to complementary products or services (Tiwana, 2014). For example, Apple iOS is a software-based service offered to operate its mobile devices. Complementary services for iOS are the more than two million apps offered for its users via the App Store. Such platforms do not only compete on services but also on how widely used their platform is. Third party developers are more interested in developing apps for a platform that has many users. On the other hand, users are more interested in using the platform with the most complementary products such as apps. Hence, platforms are competing with each other based on their own ecosystems. This example characterizes platforms as mediating different groups of users, such as buyers and sellers (Boudreau & Hagiu, 2009).

Platforms have become increasingly common in society. Tiwana (2014) argues that this is happening due to the increasing packetization of products, services, activities and need for specialization in different markets. In contrast to the product and service based model of competition, Tiwana states that platforms are better suited to deal with these forces and thus more competitive than product and service based models. Furthermore, the increasing embeddedness of technology in previously nontechnological industries denote another trend. Whereas this trend results in platforms becoming so-called digital platforms.

Practical relevance

An important decision in the governance of these platforms is openness. A digital platform can be open by making it easy for external actors to use services of the platform or build on the platform (Evans, Hagiu, & Schmalensee, 2006). These varying degrees of openness can prove beneficial to the platform in multiple ways. One of this is the fact that an increased openness can result in more potential users (i.e. market potential) (Ondrus, Gannamaneni, & Lyytinen, 2015). By making it easy for users to use services on the platform a platform can be open. In addition, a platform can also be open in the sense that it can allow for building on its platform (i.e. creating complementary products). Some research (See Boudreau, 2010) suggests that having a higher degree of openness can have a positive effect on a platform's innovativeness. If more people are allowed to build on the platform (indicating openness), then this can have a positive effect on the innovation on that platform (Boudreau, 2010). As a result openness is often a management decision to increase the competitiveness of a platform.

However, open platforms carry risks too. Digital platforms have the ability to collect large amounts of data of its users, whereas this can lead to privacy risks. As is illustrated by the Facebook and Cambridge Analytica events. Whereas large amount of data from people was utilized without consent, for purposes of political advertising. Thereby violating the privacy of millions of people. Furthermore, in opening up a platform, safety risks can be encountered too. For example, Amazon further opening up their platform for retailers (i.e. less strict requirements on sellers) resulted in thousands of unsafe products on the platform (Berzon, Shifflett, & Scheck, 2019). In this case opening up increased the total value of the platform. In contrast, the openness of the platform increased the threat to the safety of many consumers on the platform.

Recently several platforms have faced outcry over certain risks and as a result sometimes also adjusted their openness. While the privacy risks of many digital platforms are widely highlighted by the news, there are also various cases of safety risks posed by digital platforms. Examples other than the Amazon case are Tinder, Uber and Jeep vehicles. Recently the popular dating app, Tinder, announced plans to add a 'panic button' to their services to alert local authorities if a date is deemed unsafe by the user (Valinsky, 2020). Similarly ridesharing platforms such as Uber and Lyft, among others, faced allegations of badly handling reports of sexual assault or dangerous driving. After which the platforms added increased screenings of new drivers and an anonymous reporting functionality to their app (Garcia & O'Brien, 2019). This highlights platforms like Uber closing their platform openness towards new drivers and Tinder taking responsibility for risks in their ecosystem by adding safety measures to their platform.

Besides these conventional examples of digital platforms, digital platforms are also becoming increasingly pervasive in other industries such as the automotive industry. As cars are becoming increasingly digitized and connected, cars themselves are becoming digital platforms (Yoo, Henfridsson, & Lyytinen, 2010). Consequently, third parties can develop apps and services for cars (Henfridsson & Lindgren, 2010). Yet, as cars become more digitized, new safety risks are also introduced to the domain. In 2015 hackers managed to remotely hack a Jeep Cherokee driving on the road, rendering the vehicle out of control from the driver (Greenberg, 2015). This example highlights that while other sectors seek to follow the trend of digital platforms, they may also face new risks.

Some risk can be anticipated and dealt with, while other risks are unforeseeable. Especially in a digital context, increasing complexity might give rise to additional risks (Hanseth & Ciborra, 2007). Above cases can be seen to suggest that digital platforms let financial gains guide platforms openness, instead of societal values. Sometimes only after public outcry do societal values also have an effect on this openness and vice-versa. This leads to believe that there may be a disregard for societal values as a guide in designing platform openness.

The societal relevance of this issue is that platform openness is often optimized for financial gains, or in other words, to increase competitiveness. However, this approach of thinking about platform openness does not take into account societal values such as the safety and privacy of users. Consequently, digital platforms might proliferate at the cost of societal values such as privacy and safety.

Academic relevance

One condition for platform success is to reach a critical mass of users (Evans & Schmalensee, 2010). The growth and attractiveness of platforms are subject to the positive same-side and cross-side network effects a market provides (Ondrus et al., 2015; Rysman, 2009). Therefore a platform needs to have sufficient market potential, represented by the number of users who can join a platform. Whereas, the architectural configuration of platform access, interoperability and ownership rights (i.e. openness) is theorized to influence this market potential (Ondrus et al., 2015). Hence, in order to increase the chances of platform success, platforms want to maximize market potential. This is problematic because architectural configurations with the highest market potential do not necessarily represent favourable configurations for societal values. Consequently, platform openness can allow for profound risks to materialize on societal values such as safety and privacy. Yet, current theory on platform openness does not capture the drivers and consequences of evolving platform openness (Gawer, 2014). Additionally, literature does not incorporate safety and privacy risks as guiding platform openness.

As is illustrated with Facebook changing their advertisement policy based on controversy. There are cases where openness evolves and is changed for another goal than maximizing market potential.

Additionally, some studies do find that privacy and security considerations affect platform openness design (c.f. Mosterd 2019; Broekhuizen et al. 2019). Yet, this does not cover how openness is adjusted as organizations learn about safety and privacy risks and ultimately guide platform openness. Studies do provide insight in how platforms open up their platform (e.g. Wessel, Thies, & Benlian, 2017), but do not show how safety and privacy risks affect the degree of openness. Nonetheless, research on platform openness does show trade-offs in deciding on platform openness due to interdependencies between actors. Whereas increasing openness of suppliers might give rise to additional competition between suppliers (De Reuver, Verschuur, Nikayin, Cerpa, & Bouwman, 2015). Consequently, differing strategic objectives and interests might give rise to conflict. These trade-offs can also be identified in other cases. Cambridge Analytica enjoyed great data collection capabilities, at the cost of Facebook user's privacy (Broekhuizen et al., 2019).

Literature defines openness as a unidirectional process, instead it appears bidirectional and reflexive in nature. As safety and privacy risks are not always foreseeable in the design of a platform, openness can be adjusted upon learning about safety and privacy risks. Hence, highlighting the reflexive and bidirectional nature between safety and privacy risks and platform openness. Furthermore, after platform launch, a platform can encounter new risks. Hence, the academic relevance is that theory on platform openness should link architectural configurations with societal risks. Research is necessary that can facilitate understanding on how safety and privacy risks adjust openness of platforms. This thesis aims to offer a first step on the expansion of current theory on platform openness by investigating the interaction of platform openness with safety and privacy risks.

1.2 Research objective

As explained in the section above, current events such as the Facebook and Cambridge Analytica events highlight a need for understanding how platforms manage risks such as safety and privacy risks. In some cases platform openness also evolves upon learning about risks such as safety and privacy. Additionally, research has also pointed out that in deciding on platform openness privacy and security risks affect openness. Similarly, safety outcries over Amazon selling unsafe products highlight the severity of the threat to the safety of users. Nonetheless, current research on digital platform openness does not explain how digital platform openness adjusts upon learning about safety and privacy risks.

Current theory on platform openness does not explain how platform openness adjusts due to safety and privacy risks. Although conceptualizations of openness are made in other studies, the process through which openness evolves is studied sparingly. Furthermore, the drivers of openness are till this day primarily studied from the perspective of financial and innovation dynamics. Whereas, a certain degree of openness is theorized to impact factors such as market potential and innovation on the platform. Secondly, research on digital platform openness introduces the concept of generativity. The concept of generativity helps to explain why a platform experiences unforeseen changes. Subsequently, the mechanism of generativity might also explain why open digital platforms encounter unforeseen safety and privacy risks after their inception. Yet, these dynamics do not cover how openness interfaces with safety and privacy or how organizations adjust openness upon learning about safety and privacy risks. Hence, research on expanding existing theory is necessary.

Previous research on platform openness suggested that privacy and security risk are factors which affect openness (e.g. Mosterd, 2019; Schreieck, Hein, Wiesche, & Krcmar, 2017). Yet, no research has studied the phenomenon on how platform openness is adjusted upon learning about risks such as safety and privacy. Hence, this research will perform an exploratory study on the process of how platform sponsors

adjust digital platform openness upon learning about safety and privacy risks. This research studies platform sponsors specifically. According to research by Eisenmann et al. (2009) platform sponsors are the owner(s) of the platform and have the architectural control over the platform. Hence, platform sponsors is the role that actually has the decision power to change or adjust openness. This leads to the following research objective:

Research objective:

- *This research aims to develop a description of the process on how a digital platform sponsor adjusts platform openness upon learning about privacy and safety risks.*

Specifically this research will provide a novel conceptual model on how digital platform openness is affected by safety and privacy risks. Hence, the objective includes researching the relationship(s) between digital platform openness and safety and privacy risks. A practical objective of this research is to provide insight in how platforms can account for privacy and safety risks in their platforms and ultimately become more responsible platforms.

This theory will be derived from two different understandings created in this research. First, from a review of relevant literature (refer to chapter 2) a preliminary model of the process on how a digital platform sponsor adjusts platform openness upon learning about privacy and safety risks is defined. This model has the purpose defining the pattern (or processes) between major variables identified in the literature. In this model the phenomena (e.g. risk) and activities (e.g. adjusting openness) found in the case are captured.

Secondly, utilizing the analytical approach of pattern matching (Yin, 2018) the theoretically derived pattern is compared with an empirically derived pattern on how a digital platform sponsor adjusts platform openness upon learning about privacy and safety risks. In essence this entails comparing the propositions (or conditions) from the theoretical model with the empirical model. Using the empirical findings the research assesses whether the theoretically derived pattern matches the pattern derived from empirical findings. If the patterns match then a conclusion can be made (Yin, 2018, p. 224) on how digital platform openness is affected by safety or privacy risks. In the case that the patterns do not match then the theoretical propositions will be questioned. This matching of patterns is part of the analysis section of the research.

The model will follow a network (also referred to as operational model diagram) display format as described by Miles & Huberman (2014) and Saldaña (2013). For example the below network model was created by Saldaña (2013) based on a study by McCammon et al. (2012).

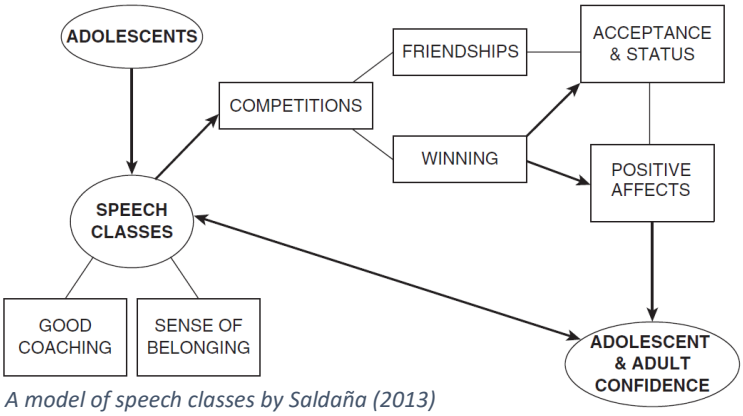

Figure 1 A model of speech classes by Saldaña (2013)

Miles & Huberman (2014) argue that network models are especially fit for displaying activities, events and processes. Moreover, they help in communicating complex relationships between variables (Miles et al., 2014). In above model the central proposition is that when adolescents take speech classes they develop confidence later on in life (Saldaña, 2013). The study also identified that for example good coaching and a sense of belonging in the speech classes are conditional for the effect to occur. These relationships are highlighted in the diagram above.

Similarly, for this research a set of propositions and a conceptual model that describe the process of how digital platform openness adjust upon learning about safety and privacy risks will be the deliverable of this project. This research either confirms or disproves the relationships proposed based on theoretical literature. In both cases, the conceptual model will be enriched based on empirical findings of the case in order to produce a detailed contribution to theory. In addition, to the model, practical recommendations will be provided to the case company on how to become a more responsible digital platform using concepts from responsible innovation.

1.3 Research questions

The research aims to answer the following research central research question:

- *How does a digital platform sponsor adjust openness upon learning about privacy and safety risks?*

The central research question is answered via the following sub questions. The first question aims to ground the research in state-of-the-art research on digital platform openness. Following this literature, other available theories are used to explain how digital platform openness is affected by safety and privacy risks. Alternatively, this question forms the starting point to formulate an initial conceptual model on how an organization adjusts digital platform openness upon learning about safety and privacy risks. Consequently, this sub question is answered via the literature review.

It should be noted that at the start of this research the focus was primarily safety and privacy risks, but during data collection it was found that a broader perspective of risks were relevant too. It would be unfitting to edit questions to fit the data. Hence, the research questions are kept the same while at the same time not ignoring alternative variables such as other types of risks.

1. What theories in available literature explain how platform openness is adjusted upon learning about privacy and safety risks?
    - Topics:
        - What are digital platforms?
        - What is digital platform openness?
        - How does digital platform openness evolve?
        - Why do organizations change due to safety or privacy risks according to legitimacy theory?
        - How do organizations learn about safety and privacy risks according to theory on organizational learning and responsible innovation?

Following sub research question 1, the case study is performed at the unit of analysis. The sub questions focus on different parts of the question, namely safety and privacy. Whereas the questions are answered via findings made in interviews and document analysis at the case study firm. If the researcher

deems it interesting additional lines of enquiry will be added based upon findings of the data collection phase.

2. How do platform sponsors adjust openness upon learning about safety risks?
    - How does the organization learn about safety risks?
    - How do safety risks affect platform openness?
    - Why do safety risks affect platform openness?
3. How do platform sponsors adjust openness upon learning about privacy risks?
    - How does the organization learn about privacy risks?
    - How do privacy risks affect platform openness?
    - Why do privacy risks affect platform openness?

Finally, the results of the case study are analysed for the final sub questions. The results of this analysis will be used to potentially expand theory on digital platform openness.

4. How does the conceptual model explain how privacy and safety risks affect platform openness?
    - What can we learn from the case study?
    - How does the empirically derived process match to the conceptual model developed in RQ1?
    - Do privacy and safety risks adjust digital platform openness differently?

1.4 Reading guide

This research report is outlined to first provide an account of the problem and literature gap. Based on gaps identified in platform literature an alternative theory is developed on how platform openness is adjusted due to safety and privacy risks in section 2 Literature review. Section 2 also answers the first research question. Following this section 3 Methodology outlines the research approach taken in order to investigate the case and collect and analyse data on the case study. In addition section 3.2 and 3.3 provide a description of the case itself and the market environment the case is situated in. Following, section 4 Results describes findings of the case and answer the second and third research question. Accordingly section 5 Analysis of results analyses the propositions developed in section 2 according to the findings from the case. This section answers research question four. Finally section 6 answers the main research questions followed by a section that outlines the theoretical and practical implications of the study. Alongside, the chapter also describes the limitations of the study and practical recommendations for digital platforms.

2. Literature review

This chapter will describe the literature review performed on the research domain. First the literature review[1] will present a chronological review of important literature on platforms, digital platforms and platform openness. Second, the literature review provides an alternative perspective on platform openness using theories from other fields. Finally, an initial conceptual model is defined based on the alternative perspective.

2.1 Platform literature

In a research agenda on digital platforms, De Reuver et al. (2018) distinguishes different fields that add to conceptualization of platforms. Furthermore, De Reuver et al. (2018) also describes how digital platforms are fundamentally different from non-digital platforms. These fields are economics, industrial innovation management and information systems (De Reuver et al., 2018). In order to conceptualize digital platforms in the literature and understand how platforms function, this review will first cover relevant platform theory in the aforementioned fields. Following the suggestion of Jesson et al. (2011) a chronological approach is followed to show the evolution of the theory and use this to understand how the theory currently explains a phenomena. Consequently, these findings allow certain conclusions to be made regarding the current state of literature and how it can potentially be improved (Jesson et al., 2011). Whereas the guiding aim of this literature review is to gather an understanding on how digital platform openness interface with safety and privacy risks.

2.1.1 Economic perspective

Rochet & Tirole (2003) raised the idea of multi-sided platforms based on the earlier concepts of multi-sided, or two-sided, markets (De Reuver et al., 2018). Whereas a multi-sided market is a market where two distinct groups of consumers "are connected through interdependent demand" (Evans, 2003, p. 1). In this definition each side represents a distinct group of consumers. Whereas the value for a group increases by the size of the opposite group and vice-versa. For example the value of Airbnb for potential renters as more rooms/houses are offered on the platform. Conversely, the more users are on the platform, the more interesting it is for estate owners to offer their rooms on Airbnb. Evans (2003) argued that in these type of multi-sided markets, *multi-sided platforms* (hereafter MSP) can emerge. In this case an MSP is an intermediary that internalizes the network externalities present in many two-sided markets (i.e. indirect or direct network effects). Network externalities define that increased use of a certain product increases the value of the product for another or the same group of consumers (Katz & Shapiro, 1985). The Airbnb example above is an example of positive indirect network effects, or positive cross-side network effects. Direct network effects, or same-side network effects, occur when the value of a service increases due to having more of the same users on the platform. To illustrate, the value of Facebook increases for users if more users join the platform because this means that a user can connect with more people.

Rysman (2009) builds upon MSP literature researching different cases of MSPs by identifying market strategies a MSP can use. One of these strategies relates to a platforms openness. Whereas Rysman (2009) introduces two dimensions of openness. The first dimension is the number of sides of a MSP. Whether a MSP is one-sided or even three-sided has an effect on the economic performance of the MSP. The second dimensions relates to compatibility between platforms. What can be deduced from this is that openness can change, but the economic literature does not explain how or why this occurs.

[1] Please note that parts of the literature review have been adapted from an earlier version of a literature review made in preparation for the master thesis. Both literature reviews are from the same author.

In order to better conceptualize MSPs, Hagiu & Wright (2015) distinguish platforms form alternative business models in multi-sided markets. They identified the following two fundamental features of a multi-sided platform:

- "They enable direct interactions between two or more distinct sides.
- Each side is affiliated with the platform." (Hagiu & Wright, 2015, p. 5)

Affiliation alone is not enough to be a MSP. Affiliation is defined by Hagiu & Wright (2015, p. 5) as "users on each side consciously make platform-specific investments (e.g. opportunity costs) that are necessary in order for them to be able to directly interact with each other". In addition, if a firm still controls variables such as prices (e.g. a retailer), then a firm is more of a reseller than a MSP. A MSP enables direct interactions between two or more sides. Which allows each side to control variables such as prices.

Economic literature on MSPs distinguishes multiple modes of configuration for a MSP. However the primary dimensions of the theory only include consumers and platform competition. Moreover, the economic literature focusses on platforms from a perspective of financial dynamics in a market rather than innovation dynamics (De Reuver et al., 2018). The economic literature mainly utilizes theory on network effects to explain economic effects of platform openness.

2.1.2 Engineering design perspective

Conversely, Gawer (2014) denotes two limitations of the economic literature on platforms. First, platforms are viewed to be exogenous and fixed. Whereas economic models do not describe how or why platforms evolve. Second, all sides of a platform are reduced to consumers. Gawer (2014) states that this simplification ignores important relations such as the relationship between platforms and developers of complimentary products. Especially in technological platforms this group of platform users are important to consider in order to understand platform evolution and innovation (Gawer, 2014).

In contrast to the economic literature on platforms, Gawer (2014) provides a different conceptualization of platforms originating from engineering design literature. Based on the notions of design hierarchies and modularity by Clark (1985), the concept of *technological platforms* arose (Gawer, 2014). An early conceptualization of platforms is attributed to Wheelwright & Clark (1992). Wheelwright & Clark (1992, p. 73) characterize a platform as a product that meets the needs of a distinct group of customers while allowing for the addition, removal and modification of features.

In earlier research, Baldwin & Woodard (2009) point to empirical evidence for such technological platforms in different contexts. These context are platforms in a firm, across firms and in multi-sided markets. These findings seem to coincide with the economic literature on multi-sided platforms. Upon analysis of these cases Baldwin & Woodard (2009) find that all these platforms share a modular architecture. Consequently, Baldwin & Woodard (2009, p. 24) define a platform as a "stable core component and variable peripheral components". It is in this article on platforms that the importance of interfaces and modularity are highlighted. Whereas interfaces between modular components in a platform affect the versatility of a platform's components (Baldwin & Woodard, 2009; Parnas, 1972). Gawer (2014) adds to this by stating that the openness of interfaces affect the room for innovation of a platform for users such as complementors.

The openness of an interface highlights the technological nature of technological platforms, and differentiates from the economic literature by utilizing the concepts of interfaces and modularity to

explain innovation dynamics. From a perspective of network effects, having an open interface can affect the complementary products made for a specific platform. Consequently, the value of a platform increases for users and positively affects adoption (West, 2007).

Gawer (2014) states that the engineering design literature on platforms do not clarify how platforms evolve. Therefore, Gawer (2014) developed an integrative framework on technological platforms and how they evolve and compete. Gawer (2014) proposes a set of processes on how platforms compete and why they become open or not via for example Application Programming Interfaces (API's). First, the more open a platform is, the more innovative capability a platform will have access to. Second, not all of this innovation will be platform-enhancing, instead some will be competitive to the platform. An example being Netflix moving from being a complementor to the broadcast network HBO, to a competitor (Gawer, 2014). Third, platform governance influences the amount of competition that arises from complementors by altering incentives for innovation and competition. Finally, in reaction to complementor competition, a platform may adjust its interface openness.

The theory proposed by Gawer (2014) adds to the dimensions of openness by stating that it is not a fixed variable of platforms and adds to the notion of how and why the architectural configuration of platforms changes. Yet, this only explains drivers of openness form a perspective of innovation dynamics. Whereas this does not explain other drivers or context on why or how openness changes in digital platforms (cf. Twitter and Google changing policy on political ads[2]). Moreover, Gawer (2014) does not distinguish technological platforms from digital platforms, even though she researches specifically digital platforms such as Google, Twitter and Facebook (De Reuver et al., 2018). While, De Reuver et al. (2018) states that the concept of digitality is theoretically relevant on account of digital and non-digital platforms not necessarily having the same organizational arrangements.

2.1.3 Information systems perspective

Tiwana (2014, p. 7) defines digital platforms as the "extensible codebase of a software-based system that provides core functionality shared by apps that interoperate with it, and the interfaces through which they interoperate". Whereas the main differentiator of digital platforms compared to multi-sided or even technological platforms is the concept of digitality. In comparison to how digital technology differs from earlier technologies, Yoo et al. (2010) distinguishes three characteristics unique to digital technologies. Firstly, the re-programmability of digital technology provides flexibility to technology. Whereas analog technologies do not possess this trait. Second, where analog technologies produce heterogenous data, digital technologies homogenize data (e.g. binary) from heterogenous sources. Hence, dissolving product, industry and service borders (Yoo et al., 2010). Third, due to the self-referential nature of digital innovation, digital technology is required for digital innovation. Consequently, positive same-side network effects increase and reinforce the diffusion of digital innovation. This results in lowered entry barriers, running down the learning curve and an increased diffusion of the specific technology. In contrast, this is not necessarily the case with non-digital technologies. These traits position digital platforms distinctly as a subset of platforms, different from conventional technological platforms (e.g. a modularly designed camera). Furthermore, due to these traits unique to digital platforms, digital platforms challenge concepts such as the speed of change possible in distributed technical systems (De Reuver et al., 2018).

In an earlier paper, Ghazawneh & Henfridsson (2010) add to importance of apps in a platform by focusing on the importance of third-party development for digital platforms. On account of a platforms

[2] Source: https://www.theguardian.com/technology/2019/nov/20/google-political-ad-policy-facebook-twitter

apps (i.e. modules) extending the functionality of a platform (De Reuver et al., 2018; Tiwana, 2014). Specifically, through the use of so-called boundary resources (Bergman, Lyytinen, & Mark, 2007), a platform can provide design capabilities to users while maintaining control over the platform (Ghazawneh & Henfridsson, 2010; Von Hippel & Katz, 2002). Ghazawneh & Henfridsson (2013, p. 174) define boundary resources as "the interface for the arm's-length relation-ship between the platform owner and the application developer". Whereas the boundary resources a platform can offer to enable third-party complementary development are software development kits (SDKs), application programming interfaces (APIs) and other tools (Ghazawneh & Henfridsson, 2010). In contrast, a platform can maintain control of platform development by maintaining clear agreements in order to include or exclude foreign boundary resources or platforms from taking advantage of third-party boundary resources. The sum of a platform and its apps is also referred to as the platform ecosystem (Tiwana, 2014, p. 7). Boundary resources can be used to form an alternative perspective on how technology openness functions.

Furthermore, due to the layered modular architecture of digital platforms, digital platforms possess a characteristic of generativity (Yoo et al., 2010). Generativity is defined by Zittrain (2009, p. 1980) as "a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences". Yoo et al. (2010) distinguishes a digital platform from modular products on account of its generativity. Specifically, layered modular products, such as digital platforms, allow differences in kind, compared to offering only differences in degree via a modular product. This on account of each component of a digital platform being able to originate from heterogenous design hierarchies. Hence, digitality allows the loose coupling of components in a platform.

As a result of generativity and the boundary resources of a platform, digital innovation becomes a distributed process (Boland, Lyytinen, & Yoo, 2007; Yoo et al., 2010). Distributed among heterogenous actors which are not necessarily coordinating. As is seen in the previously discussed literature, different architectural configurations of a platform can lead to different outcomes in competitiveness, but also in innovation and value creation. Nonetheless, the innovativeness, and thereby the generativity, of a platform is affected by its openness (Boudreau, 2010). Whereas, a platform can be considered open by making it easy for external actors to use services of the platform or build on the platform (Evans et al., 2006). Furthermore, a platforms openness can affect the adoption rate of a platform (West, 2003). Conversely, opening a platform can also decrease switching costs of users (Eisenmann et al., 2009). This makes platform openness a crucial balancing act for platform growth and survival.

The information system literature on digital platforms introduce the concept of generativity to explain unprompted changes in a platform. Yet, the literature does not consider the implications of this concept for platform openness. Which is how innovation, or the effects of innovation, affect societal values.

2.1.4 Digital platform openness

As can be seen from previous paragraphs, the literature on platforms continually evolved notions on platform openness. Whereas the economic literature implicitly refers to openness of a platform in the number of sides a platform has (i.e. the number of user groups a platform serves). In contrast to the economic literature, the design engineering literature adds notions of openness on the level of a platforms technology. Whereas, openness is defined by complementary product compatibility (i.e. openness of interfaces). Nonetheless, although openness is commonly referred to as a binary concept, platform openness can exist out of many different degrees of openness (West, 2003).

Eisenmann et al. (2009) defined different architectural roles which can be used to distinguish platform openness. These levels are on the user, platform provider and platform sponsor level. Whereas the user-level exists out of openness for demand- or supply-side users. Determining how easily a demand- or supply-side users can use a platform. The platform provider level determines how the platform itself can be combined or integrated with other platforms. Finally, the sponsor level determines who is engaged in developing or owning the platform (e.g. a community or sole ownership). The architectural roles introduced by Eisenmann et al. (2009, p. 1) defines an open platform as having no restrictions on platform participation, commercialization or use. In addition, standards of fees are applied in a non-discriminatory manner if they are used.

Additionally, Evans & Schmalensee (2010) argue that among other factors platforms must reach a critical mass of users to launch. Whereas platforms must often coordinate heterogenous user groups to join the platform, before it can effectively be used. This can also be referred to as the merchant problem, or the chicken and the egg problem. For example, in order for a payment platform to be interesting for users to join, enough merchants must offer the platform. In contrast, merchants will only consider utilizing the platform if enough users utilize it. Therefore, Ondrus et al. (2015) argue that a platform's ability to meet this critical mass of users is primarily determined by architectural decisions. These decisions affect a platforms accessibility, interoperability and ownership structure. In other words, they affect a platform's openness.

Building on the roles of Eisenmann et al. (2009), Ondrus et al. (2015) adds to the dimensions of openness by introducing levels of openness based on the previously introduced roles. Whereas, Ondrus et al. (2015) adds a new level, the technology level. In line with the levels proposed by Eisenmann et al. (2009), Ondrus et al. (2015) visualized the levels as seen below.

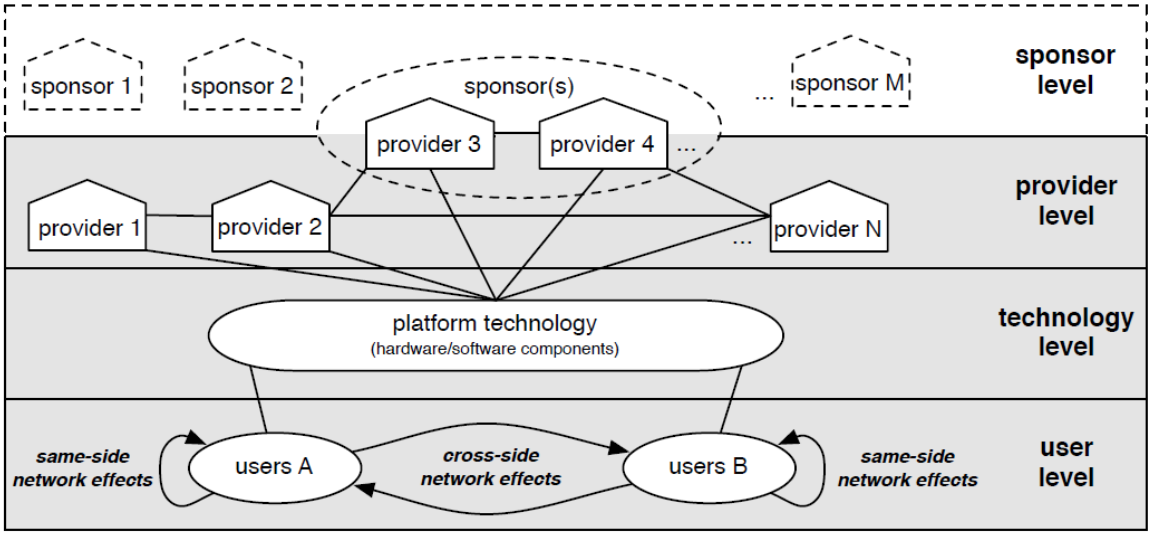

Figure 2 Openness levels visualized from Ondrus et al. (2015)

The study of Ondrus et al. (2015) distinguishes four different levels of openness. First, sponsor level openness is taken into account. Whereas sponsors level openness determines who has ownership of the platform and who controls the development of the platform. Second, provider level openness determines whether other platform providers can join the platform. Third, technology level openness defines how interoperable or compatible the platform is with other technologies. Finally, the user level openness discerns the openness toward demand-side and supply-side users and how easy they can join.

On the provider openness level, three strategies are identified (Ondrus et al., 2015). Namely, competition, coopetition and collaboration. Whereas collaboration entails that a provider will collaborate with other platform providers which could be complementors or even competitors. In contrast the competition strategy entails being closed on the provider level and competing against other platforms. Technology level openness entails the degree of interoperability between other platforms (Ondrus et al., 2015). Consequently, the platform enjoys a larger market potential due to the compatibility with another user base. Finally, openness at the user level entails indiscriminately accepting users. Whereas an example of this is Google being available as an app and via browser on any mobile device.

In a different conceptualization of digital platform openness Broekhuizen et al. (2019) provide five dimensions of platform openness. These are customer openness, supplier openness, complementary openness, category openness and channel openness. Whereas the first three dimensions affect an actors directly, the last two affect only the platform directly. They define customer openness as the degree of access that a customer has to a platform and what they are allowed to do. Secondly, supplier openness refers to the degree of access and what they are allowed to do on the platform (Broekhuizen et al., 2019; Van Alstyne, Parker, & Choudary, 2016). Thirdly, complementary openness refers to the degree of access and authority of complementary service providers. Broekhuizen et al. (2019, p. 3) defines the service providers quite broad as payment, financing, insurance, security, delivery and other platforms. The striking difference in this dimension is that other platforms are viewed as solely complementary instead of complementary and as competition. While other research acknowledges that platform-to-platform openness exists they consider it distinct from complementary products or services (cf. Eisenmann et al., 2009; Ondrus et al., 2015). Moreover, there seems to be no mention of apps or API's as a form of a complementary product/service to digital platforms.

The fourth dimension is category openness. Category openness is defined by Broekhuizen et al. (2019) as the product categories or items offered on the platform. The last dimension is channel openness and refers to the channels a platform uses to communicate or distribute the services or products (Saghiri, Wilding, Mena, & Bourlakis, 2017). These dimensions do not seem exclusive dimension. Instead they can overlap and affect the earlier mentioned dimensions. To illustrate, a platform decides to change their openness and impose a restriction on what users it serves. This change results in a change in what channel is used to distribute the platforms services. Resultingly, it becomes unclear whether this affects customer openness or channel openness. In addition, it becomes unclear whether channel openness is not a sub-category of customer, supplier and complementary services openness. For category openness the conceptual issue of 'what is a digital platform?' arises. Category openness assumes that a digital platform carries products or offers items. Compared to the definition given by De Reuver et al. (2018), the category openness dimensions seems to only relate to a more narrow definition of digital platforms. Nonetheless, Broekhuizen et al. (2019) does show a distinction in types of openness a platform can confer. Based on the research by Boudreau (2010) two dimensions are added to openness which is access (e.g. who is allowed access) and authority (e.g. what can an actor do on the platform) (Broekhuizen et al., 2019). These dimensions are not taken into account by the paper of Ondrus et al. (2015).

In contrast, Benlian et al. (2015) operationalize platform openness from the perspective of supply-side users (cf. Anvaari & Jansen, 2010). Whereas, they reason that considering platform openness from the perspective of the platform, abstracts the decision-making process of individual supply-side users such as complementors. Consequently, the platform perspective assumes that all supply-side users react in

the same way to different degrees of openness. Therefore, Benlian et al. (2015) argue that on account supply-side users being a heterogeneous group, this assumption does not hold. Furthermore, on account of platform ecosystems being reliant on persuading supply-side users to a platform instead of being able to coerce them (e.g. via sanctions), individual motivations for joining platforms are more interesting from the supply-side perspective (Benlian et al., 2015; Yoffie & Kwak, 2006). In their study, Benlian et al. (2015) utilize two dimensions to describe platform openness; transparency and accessibility. Transparency is defined the extent to which complementors are informed about what platform changes are happening and for what reason. The other dimensions, accessibility is defined as the extent towards a platform provides or constrains resources to support development of complementary products for the platform. Nonetheless, this does not explain the process of how platforms open up.

Wessel et al. (2017) do explain the implications of increasing platform openness for a digital platform from a perspective of trade-offs. They find that increasing platform openness resulted in an increased revenue for the platform. Yet, the increase in openness resulted in deteriorating conditions for users of the platform. This study coincides with findings of the de Reuver et al. (2015). Whereas increasing openness of suppliers might give rise to additional competition between suppliers (De Reuver et al., 2015). Nonetheless, looking at the research question of this project, this leaves the question: what effect does platform openness have on societal values?

The literature on platform openness describes different methods of opening up a digital platform. Additionally, literature describes different drivers of this openness mainly regarding market potential and innovation potential. Yet, these views do not capture other drivers such as safety and privacy risks. Although as previously shown with the Facebook and Cambridge Analytica case it can be seen that digital platforms do adjust their openness based on for example discovered privacy risk. This suggests a gap in theory. If openness is adjusted based on discovered risk then openness can maybe also be adjusted based upon anticipated risk. There are cases where openness evolves and is changed for another goal than maximizing market potential. This might also be explained via the concept of generativity. Additionally, some studies do find that privacy and security considerations affect platform openness design (c.f. Mosterd 2019; Broekhuizen et al. 2019). Yet, this does not cover how openness is adjusted as organizations learn about safety and privacy risks.

Secondly, platform openness can evolve over time (Gawer, 2014). Current platform literature describe the opening up of platforms via unidirectional models (cf. Ondrus et al., 2015). To illustrate, innovation might be a driver for greater openness. However, greater openness can also give rise to competence-destroying innovation. Consequently, a platform may adjust its platform openness based on this competition (Gawer, 2014). Moreover, literature shows that opening up a platform can be a double-edged sword in terms of resulting for example in increased revenue but also deteriorating conditions for platform users. Nonetheless, literature does not capture this trade-off of opening up platforms and the effect on societal values such as safety and privacy.

In another case, anticipated safety and privacy risks might guide platform openness. Yet, due to the subsequent platforms generativity resulting from a platforms openness, new risks might be identified later on. In turn these risks can inform the adjustment of platform openness. This is indicatory of a reflexive relationship between platform openness and risks. Furthermore, this also highlights that a platform opening up is not a unidirectional process, but instead bidirectional.

2.2 Organizational learning, legitimacy and risk

This chapter provides perspectives from established theories outside the platform literature to construct an alternative perspective. The alternative perspective will describe how digital platform openness is adjusted upon learning about safety and privacy risks. This question requires delving in why organizations change due to risks, how organizations learn and how organizations deal with societal risks such as safety and privacy.

2.2.1 Legitimacy theory

What drives an organization to adjust openness to minimize privacy or safety risks for its users? Drawing upon the inclusive definition of legitimacy provided by Suchman (1995, p. 574) legitimacy is: "a generalized perception or assumption that the actions of an entity are desirable, proper or appropriate within some socially constructed system of norms, values, beliefs and definitions". Whereas legitimacy theory explains why an organization changes their behaviour in order to regain, maintain or increase legitimacy (Suchman, 1995). As Suchman further points out, legitimacy reflects the *perceived* congruence between an entity and the values, beliefs or norms of a social entity. Consequently suggesting that a social contract exists between an organization and society (Deegan, 2006). For this research legitimacy theory is picked on account of it being a potentially viable alternative perspective on why organizations do certain activities. Moreover, the theory has also seen a recent surge in use in the field of corporate social responsibility (e.g. Beddewela & Fairbrass, 2016), which is a field that closely relates to the topic of this study. In addition, according to Fernando & Lawrence (2014) the theory still has a growing number of empirical studies that support legitimacy theory (e.g. Archel, Husillos, Larrinaga, & Spence, 2009; Chu, Chatterjee, & Brown, 2013).

Legitimacy theory provides an explanation on why an organization should act to manage privacy and safety risks. Hence, legitimacy theory might prove to be a supplemental theory for understanding how platforms adjust openness. An organization might strive to maintain its legitimacy if a privacy risk for its users is discovered. In contrast, this also explains why an organization can maintain legitimacy if an organization diverges significantly from societal values (Suchman, 1995). For example a privacy risk that is not yet discovered by the public does not have to harm legitimacy. Consequently, if the organization's legitimacy is not harmed then an organization can choose to undertake no action.

In a typology of legitimacy, Suchman (1995) introduces three types of legitimacy. These types are moral legitimacy, pragmatic legitimacy and cognitive legitimacy. Whereas Suchman refers to moral legitimacy as the evaluation of an organization's actions and whether they are judged to be moral. Pragmatic legitimacy is the evaluation of an organization by the effects they have for the constituency. Finally, cognitive legitimacy is legitimacy gained by an organization pursuing desirable actions. In this case desirability is also highly influenced by norms. For this review moral legitimacy will be further investigated because privacy and safety risks can be moral and regulatory issues.

Moral legitimacy refers to the normative dimension of legitimacy. Among different fields such as sociology and institutional theorists moral legitimacy is recognized as a primary determinant of legitimacy (Scott, 2001; Tost, 2011). Whereas Scott (2001) states that moral legitimacy is gained by the extent to which an entity adheres to moral values and ethical principles. Suchman (1995) defines four different forms of moral legitimacy. Consequential legitimacy relates to companies that produce or do something that is normatively considered good (e.g. healthcare). Procedural legitimacy is obtained by adhering to social norms and routines (e.g. regulation). Structural legitimacy refers to an organization

having the correct 'form' of organization. Suchman (1995, p. 581) provides an example of a question that refers to structural legitimacy: "Does the organization have a quality control department?". Lastly, personal legitimacy refers to legitimacy gained by an organization with charismatic leadership.

Aldrich & Ruef (2006) add to legitimacy theory by distinguishing between two types of legitimation strategies an entity may follow. These are cognitive and socio-political strategies. Specifically, socio-political strategies explain why an organization aims to manage privacy and safety risks. Socio-political legitimacy is defined as "the acceptance by key stakeholders, the general public opinion leaders and government officials of a new venture as appropriate and right" (Aldrich & Ruef, 2006, p. 198). For socio-political legitimacy Aldrich & Ruef (2006) recognize two components. Namely, moral (acceptance) legitimacy and regulatory (acceptance) legitimacy. These two categories explain not only why organizations deal with privacy risks on account of regulatory pressures, but also on account of doing what is right on account of their perceived values, beliefs and norms. Subsequently, they depart from Suchman's typology of moral legitimacy and adopt moral legitimacy as a component of socio-political legitimacy. For this research this the concept of socio-political legitimacy seems more appropriate. This on account of the concept of socio-political legitimacy referring to all cultural and regulatory processes, whereas solely moral legitimacy doesn't necessarily cover this outside of what is right or wrong (Aldrich & Ruef, 2006, p. 186).

According to Tilling & Tilt (2010) there are four generally accepted phases on how the legitimation of an organization functions. These are establishing, maintaining, extending and defending legitimacy. The last phase, defending of legitimacy entails that legitimacy must be defended when legitimacy is threatened or challenged (Tilling & Tilt, 2010). For this research knowing in which phase of legitimation the company find or found itself in might help explain what why certain organizational behaviour is observed.

Although compliance with regulation provides an organization with regulatory legitimacy, compliance is oft challenging to achieve in the domain of privacy and security (Culnan & Williams, 2009). In the case of security and privacy regulation, organizations are expected to implement "reasonable procedures" to be compliant (Culnan & Williams, 2009; R. D. Lee & Mudge, 2006). Consequently, this creates ambiguity on what constitutes compliance. Hence, making regulatory legitimacy difficult to garner in the domain of privacy and security regulation. Whereas, the relatively recent General Data Protection Regulation (GDPR) in the EU did not change this aspect of privacy and security law (Houser & Voss, 2018). This can be observed in the GDPR as it requires 'adequate controls' to be implemented.

Therefore, moral legitimacy can be complimentary to regulatory legitimacy. Driven by the external judgment on what activities are the right thing to do (Suchman, 1995), an organization will act on privacy and safety risks they identify. Yet this requires that the organizations values, beliefs and norms agree with those of society or other social groups (Culnan & Williams, 2009). If this is not the case, then events such as the Facebook and Cambridge Analytica event might occur. Here an organization deviated from societal values while still retaining regulatory legitimacy.

Legitimacy theory provides an explanation on what motivates an organization to adjust platform openness in light of safety or privacy risks. However, legitimacy theory does not explain how the organization does this. More specifically, legitimacy theory does not explain how an organization adjusts platform openness upon *learning* about safety and privacy risks. Hence, how an organization learns needs to be investigated.

2.2.2 Organizational learning

In order to understand how organizations adjust platform openness upon *learning* about safety and privacy risks, an understanding of organizational learning is required. In a theory of learning, Argyris (1976) define organizational learning as the detection and correction of errors. In this context errors are knowledge that bars learning. Theory on organizational learning is one of the most used streams of theory to explain how organizations learn. In addition, the theory is often used in studies to explain the process of learning in organizations (e.g. Chiva & Alegre, 2009; Sosna, Trevinyo-Rodríguez, & Velamuri, 2010). Hence, theory on organization learning is considered a viable theory for understanding how a platform learns about safety and privacy risks.

Argyris & Schön (1978) distinguish between two forms of learning called: single-loop and double-loop learning. The two models are explained by Argyris (2002, p. 4) via an analogy: "a thermostat that automatically turns on the heat whenever the temperature in a room drops below 68 degrees is a good example of single-loop learning". In contrast, a thermostat questioning why it is set to 68 degrees or thinking about how to heat the room in a better way would be involved in double-loop learning. If an organization continues following current policy and achieving current objectives then single-loop learning is used (Argyris, 1977). In this case any errors encountered are detected and corrected. If an organization questions these same policies and objectives then double-loop learning occurs. This distinguishes between an organization producing a product (single-loop) versus questioning whether the product should be produced (double-loop).

Yet, not every organization always uses double-loop learning. Argyris (1976) denotes various causes of why organizations do not utilize double-loop learning. These causes are categorized by Argyris in: the degree that social and bureaucratic factors create valid information for decision makers to monitor decision effectiveness; and the receptivity of decision makers to corrective information. An example of how the first category can inhibit double-loop learning is conflicting norms (Argyris, 1977). An employee might be told to hide errors, while policy states that errors should be revealed. Ultimately, this conflict between norms might be accepted by the employee as a norm in itself (Argyris, 1977). On the other hand norms such as taboos can also inhibit scrutinization of existing strategies, results and norms. In order for double-loop learning to occur despite these barriers, Argyris (1976) argues that either a (self-created) crisis or a revolution must occur. This might explain why some privacy and safety matters are only resolved after public outrage on privacy and safety risks being ignored for the sake of another norm such as increasing shareholder value.

In order to understand why organizations make certain decisions and act the way they do, Argyris & Schön (1974) conceptualize *theories of action*. Theories of action for an organization constitute the norms, strategies and assumptions internalized by a company (Argyris & Schon, 1978). In essence these theories contain the link between an action and a result materialized via norms, strategies and assumptions. The instrumental theory of action of an organization determines how resources are allocated and how individual performance is evaluated. Whereas two categorizations are made based on theories of action, namely *espoused theories* and *theories-in-use.* Espoused theories can be described as the formal, justificatory, theory of action of an organization. In contrast, theories-in-use are the theories of action that companies actually use. These theories arise from a shared and tacit understanding of how an organization approaches tasks. The theory-in-use is based on direct observation of the behaviour of the organization (Argyris & Schon, 1978). Single-loop learning aims to

perfect these theories, whereas double-loop leaning questions the norms, strategies and assumptions made in the theories.

Nonetheless, it remains unclear exactly when double-loop learning occurs. In his work on organizational learning Schein (1993) identified two types of tension: survival tension and learning tension. These tensions either impede or facilitate learning in individuals. Survival tension trigger an individual in an organization to learn. In contrast, learning tensions bar individuals from learning. Hence, these tensions affect how an organization learns. Learning tension originates out of the being afraid to try a new activity (Coutu, 2002). For example an activity might seem too complex, or in attempting to do the activity one might lose face. It can also mean deviating from existing norms and routines. According to Schein in Coutu (2002) these fears threaten one's self-esteem or even identity. Learning might even entail losing membership of certain social groups. In the field of change management these barriers are commonly referred to as the 'resistance to change' (cf. Lewin, 1947). Schein (1993) argues that in order to overcome this tension for learning, paradoxically, another tension is needed. Moreover, he states that in order for learning to occur survival tension must outweigh learning tension. Survival tension is the tension experienced as the perceived threat to someone's life or current way of working if changes do not take place. Sun & Scott (2003, p. 211) adds to survival tension with the following examples: the threat of a competitor, threat of job loss, continued heavy workload, criticism of customers and stakeholders and the chance of promotion. Another psychological dimension of survival tension relates to the personal development of the individual (Sun & Scott, 2003). In essence this entails that individuals want to learn something based on their personal interest or motivation in the subject.

Theory on organizational learning highlights that organizations act based on their own norms, strategies and assumptions. Conflict might exist between what an organization aims to do (i.e. their espoused theories) and what an organization actually does (i.e. theories-in-use). An example of this might be a company's privacy statement describing how customer data is cared for, while in practice this might differ. The theory describes how an organisation learns and respectively how an organization can change. Additionally, the theory also explains why sometimes an organizations doesn't utilize double-loop learning. In the context of safety and privacy risks, this can explain why some organizations do not change their behaviour until public outcry occurs.

However, theory on organization learning does not explain how organizations adjust to risk. Especially the *unforeseeable* nature of risk as a result of a platform's generativity and innovation isn't elaborated upon. Moreover, theory also does not explain why companies would change openness without a threat to legitimacy. Hence, how an organization accounts for anticipated and unforeseen risks, and by extend, societal values needs to be further researched.

2.2.3 Responsible innovation

The unforeseeable nature of innovation requires innovators to think about risk before, during and after the development of an innovation. Yet, effectively managing risk is a major challenge. Formal risk assessment methodologies help in anticipating some of the risks associated with innovation. Yet, according to Stilgoe et al. (2013) these methodologies are often coming up short in identifying significant impact from risks in advance. Moreover, there are risks whose impacts never occur and risks that were foreseen but not acted upon (Hoffmann-Riem & Wynne, 2002; Stilgoe et al., 2013).

Instead of appealing to *moral luck* (cf. Williams, 1981), research has moved towards dimensions of responsibility such as care and responsiveness in managing risk (i.e. responsible innovation). Whereas moral luck can be used to argue that due to the unpredictability of innovation and the inability to reasonably foresee risk a person can avoid moral accountability (Stilgoe et al., 2013). Nonetheless, this traditional view of responsibility lacks consideration for the future and specifically care of future values (Adam & Groves, 2011). Thus far, anticipation of potential futures (e.g. risks) is not necessarily fool proof as it relies on yet unknown knowledge (Nordmann, 2014). Additionally, Nordmann (2014) argues that future scenarios also inhibit future people and subsequently also inhibit another system of values. Consequently, future capabilities of innovation cannot be judged by the present and the current value system. This leaves the question: how does and should an organization address risks that impacts moral values such as privacy and safety? Alternatively, how does an organization manage ethical issues such as privacy and safety risks?

It is often considered desirable to address ethical concerns during technological development (Schot & Rip, 1997), exploitation and disposal. To address risk, Stilgoe et al. (2013) argues that organizations need to *reflect* on their own impact, purpose, motivations and values. In order to reflect, Grin & Van de Graaf (1996b, 1996a) suggest that organizations utilize first-order and second-order reflection to address ethical concerns such as risks more responsibly. Whereas the definition and origin of first and second-order reflection originate from the aforementioned organizational learning theory of Argyris & Schön (1978) and the work of Schön (1984) on first and second-order reflection. In a comparison of conceptualizations on first-order and second-order reflective learning Van de Poel & Zwart (2010) provide a definition on both. First-order reflective learning in an ethical assessment refers to dealing with moral issues within the bounds of the belief and value system of the actor. While second-order reflective learning also reflects on the belief and value systems of the actor (van de Poel & Zwart, 2010, p. 180).

Learning differs per individual as not every individual will hold the same beliefs or values. Grin & Van de Graaf (1996a) refer to this as actors having different frames of meaning. They describe two types of frames of meaning per type of learning. For first-order learning the frame of meaning consists of an actor's definition of the problem and evaluation of a solution. Secondly, for second-order learning an actor reflects upon his or her empirical and normative background theories. These background theories shape the problem definition and evaluation of a solution to problems. Zwart et al. (2006) further conceptualize these background theories as the value and belief systems of an actor. They state that a belief system refers to the actor's view of how the world *is.* Whereas an actor's value system refers to their normative conception of how the world *should be*. This also includes an actor's normative and ethical theories (Zwart et al., 2006, p. 671). Van de Poel & Royakkers (2011, p. 86) define a value as: "Lasting convictions or matters that people feel should be strived for in general and not just for themselves to be able to lead a good life or to realize a just society". Societal values are also embedded in the engineering design of technology (van de Poel, 2009). For example, values such as safety and privacy are often discussed in relation to technology (Friedman & Kahn, 2002; Westra & Shrader-Frechette, 1997). Moreover, designing technology with certain users or purpose(s) in mind make technology value-laden (van de Poel, 2009).

Grin & Van de Graaf (1996a) suggest that second-order reflection is unlikely to happen between actors in the same 'community' (e.g. engineers). Nonetheless, organizations that either experience a 'greater than normal' threat to their business or have a safe internal environment have a higher likelihood of

second-order reflection (Grin & Van de Graaf, 1996a). It can be suggested that if an organization's legitimacy is threatened (e.g. a significant privacy issue becomes public), second-order reflection is thus more likely to occur. However, this line of reasoning can be quite misleading. Van de Poel (2016, p. 191) defines this as "the danger of equating [social] acceptance with [ethical] acceptability". Whereas Taebi (2017, p. 1818) distinguishes social acceptance and ethical acceptability as follows: "Social acceptance refers to the fact that a new technology is accepted—or merely tolerated—by a community. Ethical acceptability refers to a reflection on a new technology that takes into account the moral issues that emerge from its introduction". In addition he states that both concepts need to be considered by an organization.

Hence, an organization might be perceived as legitimate by society and thus gather social acceptance on a certain technology. Yet, the risks of the technology itself might not be ethically acceptable. Therefore, theories on responsible innovation, legitimacy theory and organizational learning might prove to be complimentary in order to explain why and how an organization might change its platform openness in different context.

In the context of handling ethical concerns such as privacy and safety risks a more specific kind of learning such as first and second-order reflective learning might be utilized by an organization. In contrast, it can also be suggested from legitimacy theory that in an effort to maintain their legitimacy an organization can respond to safety and privacy risks regardless of their moral beliefs. If organizations aim to maintain their legitimacy, and utilize double-loop learning, then a new theoretical framework can be created, expanding theory on platform openness.

2.3 Definitions

The definitions of important concepts for the study are defined below.

Openness:
Openness is not conceptualized in this study as a binary concept. A platform is not just open or closed (West, 2003). Instead, platform openness is defined in this study as: the degree of ease for external actors to use services of the platform or build on the platform (Evans et al., 2006, p. 12). Whereas this definition is expanded upon by studies of Eisenmann et al. (2009) and Ondrus et al. (2015) highlighting that openness also differs per level it is viewed (e.g. sponsor-level or user-level). In addition, the concept of digitality also introduces openness on a technological level. Furthermore, the concept of boundary resources is also used to explain platform openness as the "extent to which platform boundary resources support complements" (De Reuver et al., 2018, p. 127). Whereas 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 & Henfridsson, 2013, p. 2). In a further conceptualization of openness dimensions Karhu et al. (2018) introduce access openness and resource openness. Access openness refers to the level of access external actors have to participate and utilize services of a digital platform. Resource openness entails a platform forfeiting certain parts of their intellectual property rights and granting access to their resources. For the purpose of this study only access openness will be investigated on account of having access to a revelatory case for access openness only. Consequently this study will investigate openness using the levels of Ondrus et al. (2015) and the concept of access from Karhu et al (2018).

Risk:
The concept of risk knows several different definitions and is used often in this document. Hence, a definition of risk, as it is referred to in this study, is provided. Hansson (2009, pp. 1069–1070) provides the following definitions of risk:

- 1) an unwanted event that may or may not occur (e.g. dying).
- 2) the cause of an unwanted event that may or may not occur (e.g. smoking).
- 3) the probability of an unwanted event that may or may not occur (e.g. chance of 1 in 10 to explode).
- 4) the probability-weighted value of an unwanted event that may or may not occur (e.g. risk of fatality of 0.2, given 200 people perform a task with a chance of death of 0,1%).
- 5) the fact that a decision is made under conditions of known probabilities (''decision under risk'')

The fourth definition of risk is the most commonly used definition of risk in engineering circles (Hansson, 2009). Nonetheless, there is debate that these technical definitions of risk miss important social aspects (Taebi, 2017). Moreover, there is in fact a rich debate on risk conceptualizations across fields such as social science, psychology and moral theory outside of the engineering field (Van De Poel & Fahlquist, 2012). Hence, the many different conceptualizations across fields make the definition of risk problematic.

Regardless, in the cases presented such as the Facebook and Amazon cases, it seems doubtful that risk was communicated as a statistical expectation value. More likely, the first definition of risk was utilized to communicate what issues, or risks, warrant a response. In the case of Facebook and Cambridge Analytica the events can be described as the privacy or safety impact to a certain amount of people. Hence, for the purpose of this study, the first definition will be used to define risk. Furthermore, often standards on risk management (such as the ISO 31000) define risk as likelihood multiplied by impact. The above definition implicitly defines impact. Yet, in some cases it can be important to classify what the expected impact actually is. A likelihood can be high, but have a relatively low impact. Thus it makes sense to not make this risk as high of a priority compared to high impact and likelihood risks. Consequently, this can explain how people deal with certain risks of the same likelihood differently.

Safety:
Hansson (2009, p. 1074) distinguishes safety between, absolute safety (i.e. no harm) and relative safety. In this case relative safety is defined as a situation in which risk is reduced in a feasible and reasonable manner. Hansson also argues that this definition of safety is more compatible with the earlier chosen definition of risk. This is due to the fact that the inverse statistical value of a risk is not the same as safety. Furthermore, Hansson (2009) also introduces an important distinction. Which is the distinction between safety and security. Hansson notes that in languages such as German one word is used to describe both terms. The same is true for Dutch ("veiligheid"). The conceptualization of Hansson denotes the difference between security and safety being intentionality. An example of this is protection against the threat of intrusion (security) versus protection against the threat of falling (safety). For the purpose of this study, unintentional threats will be covered in the concept of safety. On account of the unforeseeable nature of open platforms unintentional threats can occur for society. Hence, safety is referred to as the reasonable and feasible protection from unintentional threats (Hansson, 2009).

Privacy:
Much like definitions of safety and risk, privacy is a frequently used term in different fields such as moral philosophy, law and public policy. Resultingly, there is not one agreed upon definition of privacy. In a review of the conceptualization and critiques on privacy DeCew (2018) reiterates this point. Yet, DeCew

argues following multiple streams of literature that three key contexts where the moral value of privacy arises. These contexts are “threats of information leaks, threats of control over our bodies and threats to our power to make our own choices about our lifestyles and activities” (DeCew, 2018, Chapter 3.6). Consequently, DeCew argues that privacy has moral value in these contexts because privacy provides freedom from scrutiny, prejudice, confirmatory pressure, exploitation, judgment and is an aspect of human dignity. Subsequently, some authors argue that privacy is important for values such as freedom and autonomy (Schoeman, 1984). Van den Hoven et al. (2019) adds to these reasons by also stating that not upholding people’s privacy could lead to informational inequality and injustice such as discrimination. Besides regulatory influences such as the GDPR, they also denote the importance of informed consent for the processing of personal data of people. On account of these reasons, the concept of privacy in this study is broadly defined as a value and an aspect of a person’s freedom and human dignity protected via the control of their personal information, their bodies and autonomy.

2.4 Initial conceptual model

As is illustrated with the Facebook and Cambridge Analytica events, open digital platforms can carry privacy risks. In this event the data of millions of people was unjustly used without consent for purposes of political advertising. Furthermore, the example of Amazon opening up their platform to more retailers, resulting in thousands of unsafe products for their customers, highlights that safety risks can be observed too. These above cases suggest that other dynamics such as financial dynamics guide platform openness instead of societal values. Therefore it is of practical relevance to research the relationship between platform openness and safety and privacy risks.

The cases above also illustrate that there is a relationship between safety and privacy risks and platform openness. Yet, current literature on digital platform openness does not explain this relationship. As safety and privacy risks are not always foreseeable in the design of a platform, openness can be adjusted upon learning about safety and privacy risks. Furthermore, after platform launch, a platform can encounter new risks based on evolving openness.

Legitimacy theory, specifically moral and regulatory, can explain why organizational sometimes choose to (not) adjust their openness due to privacy or safety risks. Moreover, theory on organizational learning and theory from responsible innovation on reflective learning can explain how organizations adjust their openness upon learning about safety and privacy risks. Yet, literature does not explain what exact dimension of platform openness can be affected (e.g. supplier or consumer openness). Hence, an expansion of theory on platform openness is desired. This requires research in conceptualizing theory on how digital platform openness changes due to safety and privacy risks. For this an initial conceptual model is developed (See Figure 3). This model will be used as a starting point in the research. Because it is unclear on what dimension of openness safety and privacy risks affect the dimensions the more abstract term platform openness is used. The term platform openness is expected to evolve over the course of the study. The exact propositions and relationships in the model are outlined in the following sections.

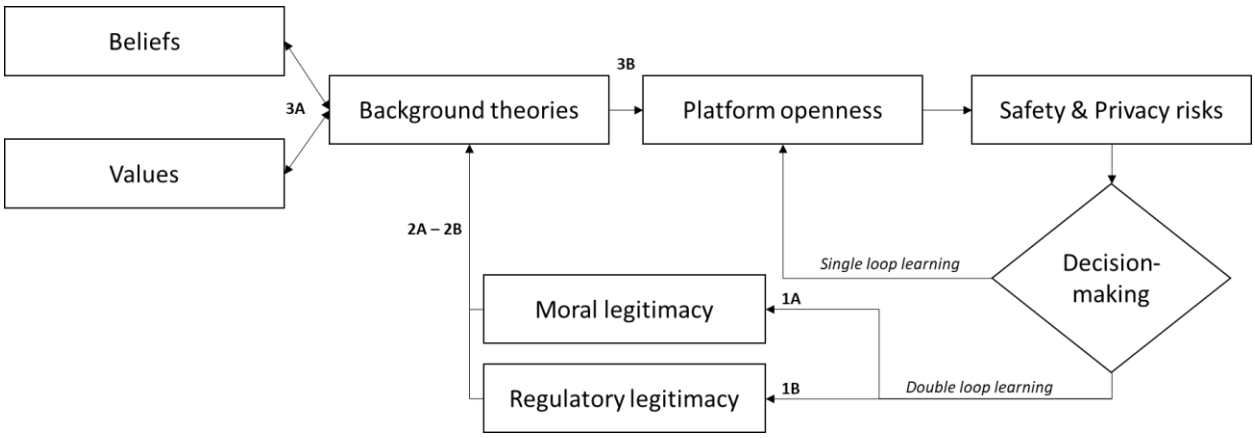

Figure 3 Initial conceptual model

Theoretical mechanisms underlying the model:

- The concept of generativity (See Zittrain, 2009) explains why digital platform openness can create and affect (new) risks;
- Organizations want to maintain or increase their (perceived) legitimacy (Suchman, 1995).

Description of model

In summary the model utilizes several theories as mechanisms to explain how available theory explains that platform openness is adjusted due to safety or privacy risks. The model starts at the platform openness of a platform. Due the mechanism of generativity safety and privacy risks can occur unprompted due to the openness of a platform but safety and privacy risks can also be inherent to the design of the platform. As the organization identifies these risks a decision is made on whether single-loop learning or double-loop learning can occur. This decision is accepted as a given in this model on account of a risk itself not being able to threaten legitimacy, but an agent *can perceive* legitimacy as threatened. Hence, as Argyris & Schön (1978) state – the individual is the agent of learning in the organization. The processing of information is done by an agent which results into decisions or actions. This processing decides whether legitimacy is threatened or not. If threatened then double-loop learning is likely to occur. If not, then single-loop learning or business as usual remains the case.

To illustrate via an example – a privacy risk is identified by an agent as a result of a Privacy Impact Assessment mandated by the GDPR. There are presumably routines, rules and other norms for the management of such a risk in the organization. Furthermore, the identified risk does not threaten the legitimacy of the organization because no criticism or noncompliance with regulation is observed. Thus, the existing routines are used to manage the risk. This is referred to in the model as single-loop learning.

In another case, a security or privacy risk is identified by the organization – or newspapers/regulators have outed criticism on the continued treatment of the risk. Consequently, the agent can perceive a threat or experience a damaged moral or regulatory legitimacy. A threatened legitimacy can endanger the continuity of the organization (Suchman, 1995). Subsequently, a perceived crisis for the organization arises. Yet, not all threats to legitimacy trigger double-loop learning. Only when survival tension outweighs learning tension double-loop learning occurs. An example of survival tension might be the fear of job loss, the threat of fines or critique from important stakeholders. This survival tension must outweigh learning tension that arise from for not wanting to break existing routines.

In this case existing routines do not cut it to prevent legitimacy from being threatened. Hence, theory on organizational learning and reflective learning describe that an organization will then question its background theories upon which it bases its existing routines, strategy and rules among other things. Therefore if an organization changes it background theories it may change the configuration of the organization's rules – and by extend its openness.

The propositions from the model are outlined and explained below.

2.4.1 Proposition(s)

This paragraph outlines the propositions defined for the initial conceptual model. Following a deductive method, the literature is used to derive propositions on how platform openness is affected by safety/privacy risks. These propositions form the patterns used to match the empirically derived patterns.

Below three categories are defined containing propositions which are derived from existing relationships found in the literature review on legitimacy theory, organizational learning and responsible innovation. In this paragraph the propositions are first outlined and numbered. The below propositions make up the threefold pattern on how platform openness is affected by privacy and safety risks. In the second paragraph, they are separately described and operationalized via the literature used to define them. The numbers of the propositions are mapped to the relationships provided in figure 3.

1. Legitimacy theory

- 1A – A safety or privacy risk threatens or negatively affects the moral legitimacy of the platform sponsor;
- 1B – A safety or privacy risk threatens or negatively affects the regulatory legitimacy of the platform sponsor.

2. Organizational learning

- 2A – A threat or negative effect to legitimacy increases survival tension;
- 2B – Double-loop learning changes a platform sponsor's theories-in-use when survival tension outweighs learning tension.

3. Responsible innovation

- 3A – Double-loop learning changes the background theories of the platform sponsor;
- 3B – The changed background theories of the platform sponsor affect the platform openness.

2.4.2 Description of propositions

Proposition 1A – A safety or privacy risk threatens or negatively affects the moral legitimacy of the platform sponsor

As Suchman (1995) states legitimacy reflects the perceived congruence of an organization and the values, beliefs and norms of a society entity. More specifically, moral legitimacy is referred to by Scott (2001) as the *extent* to which an organization adheres to moral values. Hence, a threat or negative impact to moral legitimacy would arise from a company that does not adhere to the same moral values

held by society. Drawing upon the earlier definitions of privacy and safety it is suggested that both safety and privacy have moral value. Therefore, if a platform sponsor does not seem to adhere to these values *to the extent that is expected* then legitimacy may be threatened or damaged. The difference between the extent that is expected and the current extent of the platform ultimately allows legitimacy to be threatened.

Using the concept of socio-political legitimacy an important distinction can be made on the definition of moral legitimacy by Aldrich & Ruef (2006). Namely, Aldrich & Ruef (2006) subsume their definition of moral legitimacy under the concept of socio-political legitimacy. Consequently, moral legitimacy is referred to as: "the moral value of an activity within cultural norms" (Aldrich & Ruef, 2006, p. 198). This definition departs from simply assessing whether something is wrong or right. Instead, by making it part of socio-political legitimacy Aldrich & Ruef (2006) acknowledge the cultural and normative acceptance of the organization. This is considered important for this study as culture can affect what risks to safety and privacy are accepted. Attitudes toward adhering to values such as safety and privacy might differ greatly per culture. For example, cultural patterns toward safety and privacy can differ between the context of this research, Western Europe, and East Asia where standards on safety and privacy may differ. Moreover, the concept of legitimacy also helps to explain why not every risk triggers double-loop learning.

Operationalization:
Moral legitimacy can be damaged via "criticism or negative assessment by opinion leaders, civil society organizations and key stakeholders" (Teixeira, 2009, p. 65). In a study on the legitimacy of the tuna fishing industry Teixeira specifically studies print media such as newspapers as a measure that both reflects and influences public opinion. Hence, the threat of impending criticism or negative assessment by these actors by an actor can also shape the threat to moral legitimacy.

For proposition 1A and 1B a safety and privacy risk is operationalized as follows. A safety and privacy risk is operationalized as an unwanted event that may or may not happen (Hansson, 2009) which can affect the safety and/or privacy of people. As stated before, the (perceived) likelihood and impact of a risk might affect the handling of the risk by people. Similarly people might perceive the same risk differently and therefore some might choose to ignore it where others do not. Consequently, this raises the importance of understanding how people perceived the risk in the case. Finally, although this research focusses on safety risks and not security risks, it should be taken into account that security risks also have an effect on platform openness (Mosterd, 2019). They will not be investigated, but the research will not ignore other risks if they are found in the case.

Proposition 1B – A safety or privacy risk threatens or negatively affects the regulatory legitimacy of the platform sponsor

Besides moral legitimacy there is also the second component of socio-political legitimacy namely, regulatory legitimacy. Regulatory legitimacy refers to an organizations "conformity with governmental rules and regulations" (Aldrich & Ruef, 2006, p. 186). As stated before, regulatory legitimacy can be considered a complementary form of legitimacy moral legitimacy. The threat of fines and other sanctions can incentivize an organization to take privacy and safety into account in their platform. Yet there are also important causes of variation in the effectiveness of regulatory legitimacy to be noted. These are (1) the ambiguity of current privacy legislation and (2) the exhaustiveness of legislation for safety risks.

Compliance can be challenging to achieve in the domain of privacy (Culnan & Williams, 2009). The ambiguity in current privacy legislation (Culnan & Williams, 2009; R. D. Lee & Mudge, 2006) makes regulatory legitimacy challenging to garner in this domain. Even now, privacy regulation such as the GDPR still contains requirements that refer to controls as needing to be 'adequate' (European Parliament and Council, 2016). Similarly in a report on the safety of products on the Dutch market it was found that there are a great amount of products where it remains difficult to determine what kind of product category it is in (Woutersen et al., 2017). Consequently for some products it is challenging to define what regulation is applicable. Therefore, Woutersen et al. (2017) state that it is sometimes unclear what supervision and rules are applicable for some products. Accordingly this introduces potential safety risks for consumers. Consequently, some existing ambiguity on legislation of privacy and safety might explain why regulatory legitimacy itself is sometimes not enough to gain socio-political legitimacy. Nonetheless, besides these cases a clear deviation from regulation is expected to threaten or negatively affect regulatory legitimacy of the platform sponsor.

Operationalization:
Teixeira (2009) measures regulatory legitimacy via investments in the activity and protective or supportive regulations for the specific entity. From the perspective of the organization itself regulatory legitimacy is gained via compliance of applicable rules and regulations (Aldrich & Ruef, 2006). Specifically, regulatory legitimacy is compliance with relevant laws, regulations, rules, standards and expectations (Guo, Tang, & Su, 2014; Zimmerman & Zeitz, 2002).

Proposition 2A – A threat or negative effect to legitimacy increases survival tension

In this case there are also some cases which could attribute to inhibiting double-loop learning. According to Argyris (1976) these amount to two categories: the degree that social and bureaucratic factors create valid information for decision makers to monitor decision effectiveness – and the receptivity of decision makers to corrective information. Argyris (1976) argues that in order for double-loop learning to occur a (self-created) crisis or revolution must occur (See also L. Kim, 1998). This idea is complementary to Schein's (1993) conception of survival and learning tension.

Schein's (1993) idea of survival tension relates to the tension that might be experienced as the perceived threat to someone's life or current way of working if changes do not take place. As mentioned before, Sun & Scott (2003, p. 211) provide the following examples of drivers of survival tension: threat of a competitor, threat of job loss, continued heavy workload, criticism of customers and stakeholders and the chance of promotion. An organization lacking in legitimacy can encounter issues in credibility and continuity (i.e. financial issues) (Suchman, 1995). Hence this research expects a perceived threat to or negative effect to legitimacy to increase survival tension. The mechanism of survival and learning tension is important for understanding how legitimacy can induce organizational learning.

Operationalization:
Building upon the drives proposed by Sun & Scott (2003) survival tension can be measured on account of the aforementioned drivers (e.g. perceived threat of criticism of stakeholders).

Proposition 2B – Double-loop learning changes a platform sponsor's theories-in-use when survival tension outweighs learning tension

According to Argyris & Schön (1978) double-loop learning entails an organization questioning/changing their theories of action. These theories of actions capture the norms, strategies and assumptions of the organization. Furthermore, Argyris & Schön (1978) divide this theories of action into espoused theories and theories-in-use. As mentioned before, double-loop learning is more likely to occur when a crisis or revolution becomes more apparent. For this research the mechanism of survival and learning tensions introduced by Schein (1993) is used to denote what exactly entails a crisis. Schein argued that learning tensions that arise from for example: existing norms or routines. Hence, giving rise to the feeling of unwillingness or inability due to the complex or disruptive nature of learning. Yet, the concept of learning tension does not explain all barriers to learning (Sun & Scott, 2003). Hence the inhibiting factors introduced by Argyris & Schön (1978) might be used to fill this gap. Argyris & Schön (1978) defined two factors relevant for the individual, group and organizational level – 1) valid information production for decision makers and 2) the receptivity of feedback for the decision making unit. Argyris & Schön (1978) hypothesized that decision makers exercising unilateral control for their environment and tasks would lead to negatively affecting the aforementioned two factors. Moreover, both theories on organizational learning introduce that a more pressing tension or crisis is needed to overcome barriers and allow for double-loop learning. Therefore, this research expects a platform sponsor's theories-in-use to be changed via double-loop learning when survival tension outweighs learning tension.

Operationalization:
In the operationalization of double-loop learning on theories-in-use there are some challenges. First, Argyris & Schön (1974, p. 7) state: "When someone is asked how he would behave under certain circumstances, the answer he usually gives is his espoused theory of action for that situation". Thus someone's theory-in-use is unlikely to be garnered via direct interview questions. Accordingly Argyris & Schön (1978) an individual's theories-in-use can only be found out via direct observation of their decisions and behaviour. This also introduces the second issue – do organizations themselves also have theories of action? A person's theories of action guide interpersonal behaviour, but an organization cannot be said to show interpersonal behaviour.

Argyris & Schön (1978) distinguish a collection of people from an organization on the following conditions. An organization makes decisions in the name of the organization itself. Secondly, certain individuals do or do not have the authority to act for the organization. Thirdly, the organization must be a separately identifiable entity for collective action and decision. Finally, when a group of people define rules on decision making, delegation of actions and membership they are considered *organized* (Argyris & Schon, 1978, p. 13). This distinguishes an organization from what Argyris & Schön (1978) call a mob.

On account of this distinction Argyris & Schön (1978) argue what organizational theories of actions are. Much like personal theories-in-use, organizational theories-in-use are argued to be observable from the decisions and actions of an organization. Yet, they suggest that decisions and actions carried out by individuals in the name of an organization are only considered organizational if they are "governed by the collective rules for decision and delegation" (Argyris & Schon, 1978, p. 13). Consequently, if the organization is considered the agent which solves a certain problem (e.g. growing crops) then the norms, strategies and assumptions used to solve the problem define the theories of action of organizations. They provide the following examples of norms, strategies and assumptions of an

organization: the use of labour (norm), which land to cultivate (strategy) and what yield to expect from a certain cultivation process (assumption) (p. 14). Hence, these theories of action determine how an organization does resource allocation, performance or human resource management and it's governance and communication to stakeholders.

Earlier it was suggested that in order to find out what the theories of action of an organization are, the organizations actions and decisions need to be investigated. However, Argyris & Schön (1978) state that often each member of an organization only possesses partial knowledge of their organizations exact actions and decisions. Therefore, it makes sense to consider multiple sources of evidence in order to construct the theories of action of the organization. Specifically, this also applies to having multiple sources of evidence which can be used to corroborate evidence on different platform openness dimensions. These views also align with the multi-level perspective of Crossan et al. (1999) on organizational learning. Whereas Crossan et al. suggest that organizational learning does indeed happen through the individual and then progresses through groups and only then reaches the organization.

Proposition 3A – Double-loop learning changes the background theories of the platform sponsor

Literature on first and second-order reflection shares a background in organizational learning. In this research first and second-order is seen as a branch of single and double-loop learning. This is based on the view that work from Grin & Van de Graaf (1996a) is partially based on theoretical concepts from Argyris & Schön (1978). Similarly to the concept of theories of action, Grin & Van de Graaf (1996a) conceptualize so-called background theories. These background theories exist out of an individual's belief and value system (Zwart et al., 2006) and shapes an individual's behaviour. Van de Poel & Zwart (2010, p. 180) define second-order reflective learning as a process that entails questioning the belief and value systems (i.e. background theories) of an individual. For the sake of consistency second-order reflection will be referred to as double-loop learning hereafter on account of both processes affecting the background theories of an individual or organization. Therefore this research expects that double-loop learning changes the background theories of the platform sponsor.

Operationalization:
Using the same logic applied to theories of action. An organization is also expected to have background theories. These background theories are made up of the beliefs and values of the organization. Whereas beliefs and values become organizational insofar that they are the apparent from the collective rules and delegation of the organization. Much like how individuals are the agent of organizational learning in an organization, they are also the agent of reflection in an organization. Thus, the values and beliefs held by individuals when they act in the name of the organization are parts of the values and beliefs held by the organization.

Proposition 3B – The changed background theories of the platform sponsor affect platform openness

As mentioned in the literature review, designing technology with certain users or purpose in mind make technology value-laden (van de Poel, 2009). Using the definition of access openness from Karhu et al. (2018) it is suggested that a specific platform openness affects which actors can access the platform. Hence, designing and adjusting platform openness is value-laden. Van de Poel (2009) provides the example of functional requirements being an expression of expected utility value. Similarly ethical considerations, taking into account values such as privacy and safety, are also often seen as a

requirement in design of technology (Friedman, Kahn, & Borning, 2009). Thus, the values of a designer or owner of technology can be incorporated into a technology.

Grin & Van de Graaf (1996b) define that an actors background theories guide how an actor will solve a problem (i.e. single-loop learning). Hence, the background theories or the theories of action of an organization affect how an organization does its tasks or aims to achieve its objectives. Thus, it can be suggested that it is expected that platform openness is adjusted based upon the background theories of the platform sponsor. Whereas the platform sponsor is the organization in control of the platform openness of a platform.

Operationalization:
As stated before the belief and value system of an individual are defined as follows. First, the belief of an individual relate to their view of how the world is. Second, the values of an individual are reflected in their views of how the world should be (Zwart et al., 2006, p. 671). Nonetheless according to Zwart et al. (2006) it is important to note that value and belief systems are not always completely unique to each individual. Instead they can be influenced depending on the role and responsibility of an individual in a network. Boudon (1981, p. 84) defines a role as "a group of norms to which the holder of the role is supposed to subscribe" (Zwart et al., 2006). For example a privacy officer (e.g. privacy) can have different values than an IT manager of the platform (e.g. stability). Moreover, this also implies that an individual's role in the organization can differently affect how openness is affected. In addition, different roles could affect different openness dimensions (e.g. technology or supplier-level openness). This underlines the importance of garnering multiple source of evidence to understand the value and belief systems of the organization.

Finally, the term platform openness is kept abstract for this proposition. This is done on account of the interdependency of different levels of openness (Broekhuizen et al., 2019). For example, a sales manager can be involved in determining which clients to accept to a platform. Yet, a similar decision can be made or affect decision-making of an IT manager. Technology-level openness can limit which clients are accepted similarly by for example restricting the access to the API of a platform. Hence, on account of the different levels of openness that can be affected, the research approaches openness holistically. The exact effect on different levels of openness is expected to evolve based on later empirical findings.

3. Methodology

Earlier research and real-life events suggest that privacy and safety risks affect digital platform openness. Yet, it remains unclear how exactly privacy and safety risks affect digital platform openness upon learning about them. Hence, an in-depth of understanding of this process is desired. In order to provide this in-depth understanding an exploratory case study is performed. Yin (2018) argues that case studies are especially fit for understanding how or why a social phenomenon works.

A case study is a useful research design for problems where not all variables at work are known yet (Yin, 2018). Firstly, information on contemporary phenomena under investigation do not solely reside in the 'dead past'. Instead, information can reside in archival records, documents and people. Hence, a research design is necessary that facilitates both analysis of documents and people to better understand a certain phenomenon. Secondly, because not all variables are known yet, the context of the case under study can be important (Yin, 2018). As it may contain yet unknown variables and can therefore be found using an exploratory case study. Because some variables may yet be unknown they cannot be controlled yet. This rules an experiment out, because an experiment needs to manipulate certain variables. Therefore, researching the context of the case becomes important as to explore what variables are at work in the phenomenon.

Easterby-Smith et al. (2000) also state that research investigating organizational learning does not lend itself to one stream of methods (e.g. positivist or interpretative methods). They argue that each research problem in organizational learning can warrant a different method, but those opting to research a complete organization in depth often choose for (longitudinal) case studies. Whereas case studies allow for interpretivist methods to be used while still investigating the complete context of a case or multiple cases.

Before starting research or knowing where to look it can be useful to 'know where to look' by deriving some implicit theoretical notions from existing theory (Yin, 2018). Yet, as Vaughan (1992) notes looking too much at theory might prohibit seeing beyond the theory. However, some preliminary theory as is developed in the theoretical framework of chapter 2 can help shape the direction of what data needs to be collected via the research. Furthermore, having some theories to support the lessons learned from a case study can help analytically generalize the findings of the case study (Yin, 2018). In addition, to the earlier mentioned principle of Vaughan, the seminal paper of Eisenhardt (1989) also states that some preliminary research on important variables and existent literature is necessary before starting data collection. Hence, the initial conceptual model is framed as a basis for exploratory work on privacy and safety implications for openness. Consequently, this will be used as a starting point for the objective of the research to study the relation between platform openness and privacy and safety risks.

3.1 Research framework

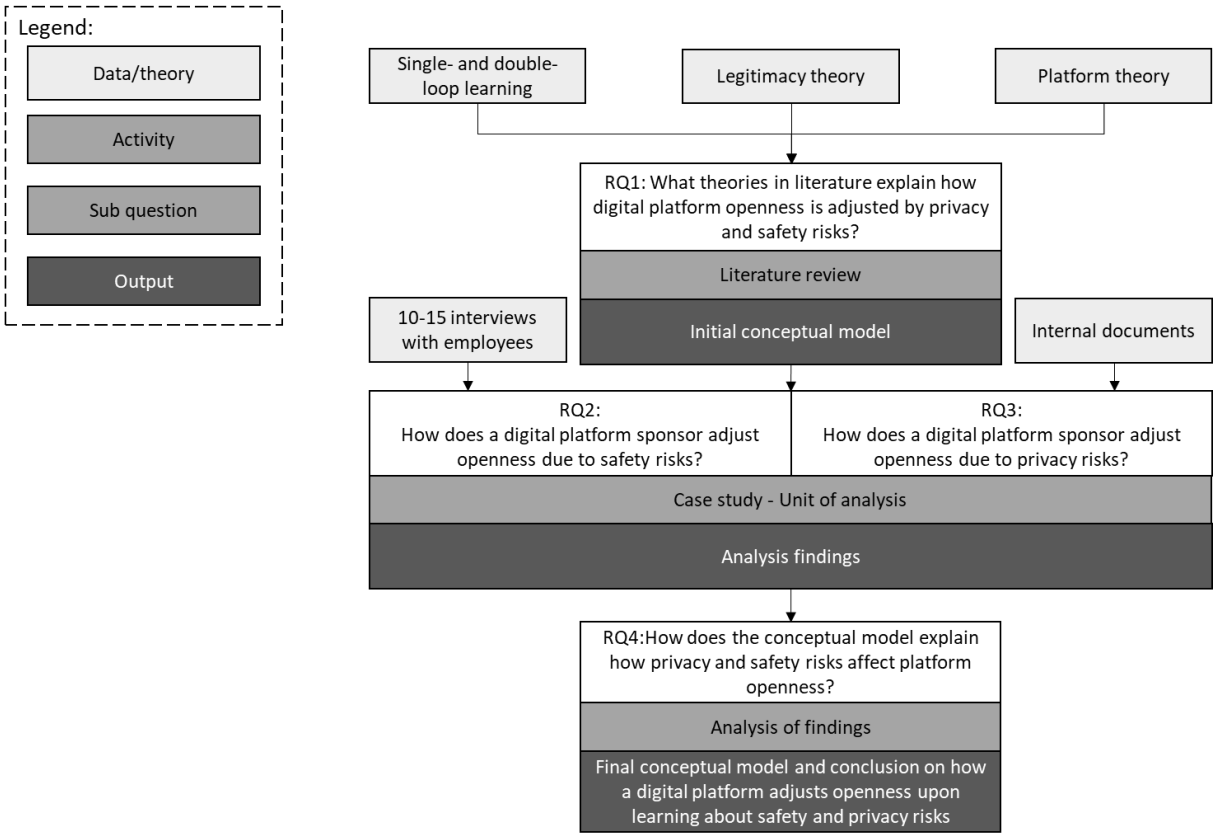

Figure 4 Research framework

The above figure outlines the research framework of this research. The framework specifically aims to provide an overview of the research process on a high-level. The exact decisions on the research approach will be described throughout this chapter.

The main research question central to the project is as follows:

- *How does a digital platform sponsor adjust openness upon learning about privacy and safety risks?*

The first step entails the literature review. The aim of the literature review (refer to chapter 2) is to gain a state-of-the-art understanding of the current literature on digital platform openness. More specifically, in this step the literature review aims to see how current literature on digital platform openness explains the phenomenon of adjusting openness due to safety or privacy risks. Second, based on a review on the digital platform openness theory a knowledge gap is proposed. Using established theories from other fields an alternative perspective is constructed which could explain the behaviour. Consequently, from this alternative perspective an initial conceptual model is made.

Following the literature review, step 2 begins. Step 2 entails the collection of empirical data of the unit of analysis. For this a general analytical strategy for case studies is followed called, pattern matching. Yin (2018) describes this as using theory to try and 'predict' the phenomena and then comparing this to the empirically-based pattern. If patterns coincide internal validity of the study can be strengthened (Yin,

2018). Step 2 answers the research questions on how a digital platform sponsor adjusts their openness due to safety and privacy risks. Specifically, documents and interviews are collected.

The case study will be performed at PayNow, a digital platform based in The Netherlands. PayNow provides payment solutions to a multitude of web shops and has been active since early 2010. On account of the allotted time of the thesis report (5 months), a maximum of 15 interviews with unique employees will be held. Based on an informal conversation with the key informant at PayNow at minimum 10 employees affect the policy, strategy and management of the platform. Hence, the research started with 10 relevant employees identified. In order to start document collection a meeting was held with the key informant in order to provide a list of relevant documents.

After step 2, step 3, the analysis of findings can take place. In this step the previously determined theoretical pattern is compared to the empirically derived pattern. Hence, certain findings can be reported on how closely the pattern is matched. This section also serves to provide evidence why the pattern can be considered matched and, if applicable, ruling out any rival explanations (Yin, 2018). Based on the findings an empirically-enriched and more detailed model will emerge. Finally, this leads the research into the conclusion and discussion of results. Whereas the conclusion will provide a description of the process on how platform sponsors adjust their openness based on safety and privacy risks. This answers the main research question. In the discussion section some practical recommendations/lessons learned for PayNow will also be made regarding the responsible handling of safety and privacy risks as a digital platform.

3.2 Financial payment service sector

This paragraph highlights the context of the financial payment service sector. This paragraph aims to help the reader better understand the temporal context of case and the trends and forces at work specific to the Dutch financial payment service sector. This sector is picked on account of the payment service sector being the niche in which the case study is positioned.

The payment service sector, and the financial services industry in general, have experienced a large impact due to the introduction of IT in many of the products and services offered in the market (Puschmann, 2017). Not only automation but also innovative new products and actors are entering the market. Consequently, some streams of literature refer to these products and services as “Fintech”. Puschmann (2017, p. 69) attributes this to the following trends: changing role of IT, changing consumer behaviour, changing ecosystems and changing regulation. As mentioned IT does not only enable automation but also allows financial service organizations to offer new products. Second, consumers are increasingly using more digital channels to utilize financial services (including payment). Third, financial service providers are specializing instead of broadening their scope of activities. Hence, there is an increasing variety of firms offering specialized products and services. Finally, changing regulation affected the entry barriers to the financial service market after the 2008 crisis (Puschmann, 2017). According to Philippon (2016) the regulation in place (post-2008) created a less than favourable environment for fintech start-ups to enter the financial service market. Whereas current regulation does not allow for a level playing field for fintech companies.

Regardless of these barriers, the payment service sector did see a significant increase in market entry of fintech organizations (Philippon, 2016). Rysman & Shuh (2017) argue that three type of innovations in consumer payments are particularly attractive for market entry. These are mobile payments, real-time

payments and digital currencies. They suggest that while these innovations disrupt how payments are handled the innovations do not necessarily require a fundamental change in the payment system (back-end) itself (Philippon, 2016). As many transactions in retail are categorized as small-value transactions there do not need to be special arrangements made with the banks that handle the 'back-end' of the transactions (Gomber, Kauffman, Parker, & Weber, 2018). Hence, allowing fintech companies to 'improve' the customer experience of retail transactions while still using the existing infrastructure of the financial industry.

Hence, the payment service sector is an interesting market for fintech firms as the barriers to market entry are lower due to being able to use existing infrastructure. The AFM (2019) adds to the assessment of Philippon by stating that Dutch fintech start-ups are often not able to enter the financial services sector due to the high cost of compliance. They also find that Dutch fintech start-ups do seem to be able to enter the market of payment services regardless of existing barriers. Accordingly, other markets such as the banking and insurance markets are still largely dominated by incumbent actors.

These findings are interesting to note and also explain in part why digital payments are gaining more traction than traditional methods of payment in the Netherlands (CBS, 2016). Bolt & Butler (2017) attribute this growth also to the rise of e-commerce in the Netherlands. Furthermore, according to a market report by Capgemini (2019) the growth in digital payments is part of a larger trend in payment innovation. Due to the rising expectations of customers the payment service is driven to develop new services and technology to accommodate for these expectations. This drive of innovation in the payment service industry is also presumed to be further enhanced by the entrance of several big tech companies such as Apple with Apple Pay. Globally a 12% growth in 2016-17 in non-cash payment transaction volume has been observed and is projected to grow (compounded annually) to 23,5% by 2022 (Capgemini, 2019).

Regulation

As stated before regulation in the financial service sector could increase entry barriers for fintech organization. Regulation plays a large role as potential barriers, but also offers opportunities for innovation. For example, Den Butter & Mallekoote (2017) contend that the, since 2018 enforced, PSD2 directive is set to offer a more competitive environment in the payment sector. In addition, with the introduction of the GDPR additional requirements arose for the protection of personal data of EU citizens. Lee & Shin (2018) add to this by stating that regulation on anti-money laundering, security and privacy, and capital requirements act as a barrier to start-ups in the financial industry.

The implementation of the new EU Payment Service Directive (hereafter PSD2) allows non-financial companies to access the financial information of banking customers. The directive is said to improve competition, stimulate innovation and improve choices for banking end-users. Furthermore, according to Romānova & Kudinska (2018) external parties such as fintech are uniquely positioned to innovate in the financial service industry. This on account of them being able to replace traditional financial processes with better technology to improve and offer new services. Kasasbeh et al. (2017) states that the factors that influence the competitivity of financial services largely relate to: customer service, pricing, access to services and the product/service mix offered. Consequently, the PSD2 opens this earlier only bank dominated area of payment information up to external third parties such as for example fintech or financial service providers (den Butter & Mallekoote, 2017).

PSD2 requires financial organizations such as banks to offer two new services: on payment acquisition and account data sharing services. Using these services accountholders can request third parties to perform transactions on their behalf. In addition, they can also let third parties aggregate and analyse their payment data. These services offer an opportunity to create new methods of payment and services that offer some sort of analytics on payment data (den Butter & Mallekoote, 2017). PSD2 is part of the larger movement called *open banking*. Open banking is referred to as the "collaborative model in which banking data is shared through APIs between two or more unaffiliated parties to deliver enhanced capabilities' to the marketplace" (Brodsky & Oakes, 2017, p. 2). The potential benefits of open banking entail an improved customer experience, but also potentially new revenue streams (e.g. personal finance analytics).

Nonetheless, one could argue that additional regulation would also raise the entry barriers for the payment service niche. This is in line with the aforementioned problems raised (e.g. Philippon, 2016). According to Dapp (2014) this is due to the lower regulatory requirements of non-banks (Romanova & Kudinska, 2018). However, Romanova & Kudinska (2018) also argue that the regulation openness up the financial sector to several risks related to fraud, security, privacy and the need for increased investment in new IT solutions to manage these risks. Consequently, the margins and market share of banks are threatened.

PSD2 was enforced at the same time the EU General Data Protection Regulation and the Dutch interpretation of the law the AVG (Algemene Verordening Gegevensverwerking) were introduced. The AVG aims to put into place controls for the protection of personal data of EU citizens. Yet, as Van der Cruijsen (2017) states the data made available by open banking/PSD2 the payment information of consumers is often personal in nature. Using the payment information of consumers patterns in consumption could be identified and marketing could be targeted more precisely. Nonetheless, a survey by Van der Cruijsen (2017) suggests that most Dutch consumers do not want their data shared for commercial purposes.

The GDPR (EU 2016/679) and PSD2 (EU 2015/2366) both went into force in 2018 (European Parliament and Council, 2015, 2016). Meaning that they both needed to be implemented in *practice* in all relevant organizations from their respective enforcement dates onward. The GDPR is a European regulation that aims to provide a unified regulation for the protection of the personal data and privacy of its citizens.

Important to note is that the GDPR is a regulation instead of directive. This entails that the member states have a bit more freedom to provide their own *legal* implementation of the regulation in each member state. Resultingly, each implementation can be more or not that much more strictly defined than the regulation already does. For example the GDPR (2016, sec. 78) defines that "appropriate technical and organizational measures" must be taken to protect the processing of personal data. This leaves room for interpretation up to each member state to what is considered appropriate. In contrast the PSD2, which is a directive, is a law that states what results and measures need to be in place for all member states. How each member states chooses to implement these measures can be decided upon nationally.

As the purpose of PSD2 is to improve competition by opening up financial data of bank customers. The GDPR could limit the impact of/and usage of this service for fintech companies. A report by Deloitte also denotes similar issues between the PSD2 and GDPR (Singer, Batch, Tannock, & Wiebusch, 2018). Both the PSD2 and GDPR require explicit consent before sharing data with (third) parties. Yet, as Singer et al.

(2018) notes, consent needs to be on a granular level and permissions cannot be bundled together in one broad consent form. Therefore, mandatory data protection and mandatory data sharing via the PSD2 could be at odds. Hence, in order to utilize the data offered by banks, third party organizations must first be able to comply with the relevant GDPR requirements. Thus possibly raising the regulatory barriers for third parties to enter the niche of processing data acquired via PSD2 mechanisms.

An expert group on Regulatory Obstacles to Financial Innovation (referred to as ROFIEG) (2019) reported similar findings to the European Commission. They state that "both data protection and competition law may be perceived by some as inhibitors of a rapid uptake of FinTech, notably because fast developing non-EU financial markets operate under considerably less stringent standards than European markets" (ROFIEG, 2019, p. 12). Accordingly they recommend that even though both competition and data protection law is necessary, they need to be tailored to not inhibit start-ups such as fintech's.

Public values

De Bijl & van Leuvensteijn (2017) in their article discuss the effects of innovation in the payment sector on Dutch public values. They argue that IT is rapidly affecting more than just the efficiency of financial processes. IT is changing not only how people pay, but also changing the process before and after payments. Hence, these new changes affect how public values, such as the privacy of consumers, are safeguarded. Based on the concept of market failures as described by Wolf (1986) they highlight three types of market failures – negative externalities, monopolies due to network effects and market imperfections (de Bijl & van Leuvensteijn, 2017).

Specifically, the sharing of data and increased analytics of payment data could have negative externalities. One such negative externality is affecting the privacy of consumers while gathering insights on consumption behaviour from payment data. Therefore De Bijl & van Leuvensteijn (2017) suggest that the GDPR is a regulatory desirable to counteract the negative externality of payment innovation (in this example: privacy and data analytics).

Second, the payment transaction market is characterized by cross-side network effects (de Bijl & van Leuvensteijn, 2017). Consequently, this could maybe lead to monopolies and potentially lead to exclusion of market entry. Thirdly, de Bijl & Leuvensteijn argue that payment innovation can also have positive effect such as lowering transaction costs for consumers. Therefore they argue for a unified regulatory 'pressure' that equally protects public values but still allows for market entry to occur. The word pressure is used here on account of pointing to the different degrees of strictness in regulation in each EU member state. Consequently, De Bijl & van Leuvensteijn indicate that this could allow for so-called regulatory arbitrage or policy shopping between member states. Whereas if the Dutch market is considered more strict, then fintech companies may choose other member states to enter the market over the Dutch market.

Lee & Shin (2018) contend that privacy and data security play a role an important role for fintech but also in developing trust for users. Moreover, they state that this trust plays a larger role in the adoption of innovative services in the financial industry. Nonetheless, there are no specific mentions of safety playing a larger role than any other industry in the payment service market. Hence this chapter largely focused on the relevant market and regulatory trends that shape the financial payment service sector in the Netherlands. This chapter aims to provide the reader with the market forces present outside the case study and may explain why certain phenomena are present in the case.

3.3 Unit of analysis

For this case study a holistic single-case study design is opted for. In building or expanding theory via a case study several reasons can be provided for choosing a holistic single-case study. One of the reasons can be researching a critical case which can help confirm, extend or test a theory (Yin, 2018). On account of the case being a critical case a single, instead of a multiple, case study is performed. In this case study, the research problem states that current theory on digital platform openness does not explain how platform openness can change upon learning about safety and privacy risks. Hence it is interesting to research a case of a platform sponsor that has adjusted its platform openness on account of a safety or privacy risk. This on account of a platform sponsor being the role of an organization that makes decisions on the configuration of a platform (Ondrus et al., 2015).

For this research a case study is performed at PayNow, a digital platform providing payment solutions to web shop users. Whereas the unit of analysis is the platform sponsor itself. Firstly, the case is relevant because it concerns a digital platform. Second, in informal talks with the Manager IT of the organization it has been observed that previously platform openness towards supply-side users has been adjusted upon learning about a safety risk for demand-side users. Therefore, the case represents a critical case. Thirdly, using the platform roles of Eisenmann et al. (2008) PayNow can be identified as a platform sponsor. Furthermore, PayNow possesses a degree of openness on a technological level as can be seen by their support for API's and various plug-ins. In addition, PayNow possesses a certain degree of openness toward their users via a credit check that they have to perform before they can join the platform. Moreover, they also possess a certain policy in which web shops they accept as clients. Also, PayNow outsources payment transactions to a single provider. Subsequently their provider openness is considered as fairly closed. Finally, PayNow is closed at the sponsor level. Hence, this final dimension of openness will not be investigated in the study.

Based on preliminary conversations with the key case informant at PayNow a similar dynamic outlined in Figure 3 occurred. Firstly, as mentioned before, PayNow learned about a safety risk after reasoning whether to keep serving a certain client. At PayNow, internal discussion started about the purpose of serving web shops that sold products in manner unbecoming to PayNow. Based on the internal discussion at PayNow a decision was made to discontinue serving the web shops because they did not agree with their way of doing business. Specifically, they did not agree with how consumers were treated. It can be suggested that a manner of double-loop learning led to the revised policy (read: user-level openness) towards serving certain web shops (supply-side users). Consequently, based on the notion of organizational legitimacy, it could be suggested that there was a perceived threat to the organizations moral or regulatory legitimacy. In contrast from a perspective of privacy there has not been such as distinct case identified as is the case for the safety risk. Yet, with the introduction of the General Data Protection Regulation by the EU, and consequently the Dutch Algemene Verordening Gegevensbescherming (AVG) law, almost every organization processing personal data needs to identify, assess and manage their privacy risks. Based on the privacy statement and informal talk with PayNow they have indeed performed such risk assessments and subsequently implemented controls for this. Hence, it is argued that for both safety as privacy risks organizational learning took place. What remains interesting for research is seeing how moral and regulatory legitimacy played a role in each of type of risk. Therefore, PayNow represents a critical case for studying the dynamic shown in Figure 3.

This research essentially researches how platform openness is adjusted due to risks that affect societal values. Specifically this researches used safety and privacy risks as starting points for risks that affect societal values and have anecdotal evidence that they affected openness. Nonetheless, throughout the case various risks besides safety and privacy were seen to affect the organization in ways that are relevant to this research. In addition, not all risks identified directly affected societal values. Hence, safety and privacy risks are used as the starting point of research but in each case additional risks that seemed to affect openness were also taken into account with the research. The reasons for this change in scope are outlined in the sections 4.1.

3.3.1 Selection of sources and documents

The interviewees are sampled based on two criteria: 1) their involvement in specific platform openness dimensions and 2) their experience in identifying and managing a safety or privacy risk for the case company.

For the first criteria the following openness dimensions are included based on earlier reviewed literature (Broekhuizen et al., 2019; Ondrus et al., 2015): sponsor level, provider level, technology level, supplier level and customer level openness. For the second criteria, based on a conversation with the case informant is asked who helped/helps/should help to identify and managing safety or privacy risks.

In order to interview relevant interviewee's, participants are selected based on them fulfilling the above listed criteria. Interviewees that do not affect consumer openness, supplier openness, provider openness or technology openness via policy or other interactions in the firm are considered less relevant. Hence, on account of different dimensions of openness it can also be assumed that different people are involved in how a certain dimension is affected. For example, a sales manager can be involved in determining which clients to accept to a platform. Yet, a similar decision can be made or affect decision-making of an IT manager. Technology-level openness can limit which clients are accepted similarly by for example restricting the access to the API of a platform. This example underlines the importance of gathering different people to interview in the organization. Furthermore, by being exhaustive, instead of selective, potential rival explanations can be ruled out. For example if this study finds that safety risks only affect user-level openness while having only interviewed people involved in this layer, then the validity of the results is not very high.

Subsequently, documents are selected based on the relation to the same criteria. However, not only corroborating evidence will be sought. Also negative evidence will be sought in order to increase internal validity of the findings (Miles et al., 2014). In addition, searching for negative evidence can also help rule out or confirm rival explanations to the conclusions (Yin, 2018).

In a meeting with the key case informant the following interviews and documents have been identified as relevant and to which access is possible:

Interviewee code:	**Function/role:**
IN1	Compliance manager/ legal officer
IN2	Manager IT / Case informant
IN3	IT specialist
IN4	Operations manager
IN5	Finance manager
IN6	Due diligence manager partner
IN7	Sales / partner manager

Interviewee code:	Function/role:
IN8	Due diligence assistant / customer service
IN9	Due diligence assistant / customer service
IN10	Chief technology officer
IN11	Chief executive officer

Table 1 Interviewees accessible for case study

Document:	Description:
Field notes made on investigation documentation	Investigation involving web shops that sold in a dubious manner
Due diligence process	Web shop client due diligence process documentation.
Due diligence introduction presentation	Presentation that outlines the reasons for introducing the due diligence process.
Terms and conditions for users / suppliers	Terms and conditions for web shops and consumers. Versions available range from the year 2016, multiple changed version in 2018 and the most recent version from 2020.
Data processing agreement	Data processing agreement for new clients (web shop) on how their data is used.
Contract for clients	The contract signed by new web shops joining the platform.
Privacy statement	The policy document describing the internal controls that manage the security and privacy risks identified. Versions available are from 2014 and February 2020.
Privacy assessment (Data Privacy Impact Assessment)	Privacy assessment and management of the risk carried out on the organization. Describes how a relevant privacy risk was handled and identified.
Internal data leakage procedure	The internal data leakage procedure of PayNow.
Data processing activities register	All processing activities are registered in this register.
Data leakage register	The data leakage register of PayNow.
Transaction policy	Transaction policy describes how the external payment transaction processer processes transactions of PayNow.
API documentation	API documentation describing how the API works and what kind of access is provided by PayNow.
Responsible disclosure agreement	Responsible disclosure agreement of PayNow for reporting vulnerabilities.

Table 2 Documents accessible for case study

3.4 Case study protocol

In order to increase the reliability of the case study, Yin (2018) recommends creating a case study protocol. Whereas the case study protocol helps the researcher in formalizing the data collection and analysis process. Yin (2018) suggests three principles of data collection namely: use multiple sources of evidence, create a case study database and maintain a chain of evidence.

3.4.1 Data collection

For the case study access has been granted and guaranteed via a key informant in PayNow. Permission for data collection via interviews and document analysis has been granted. Between 10-15 interviewees have been identified as relevant interviewees in the organization. For the case the key informant who agreed to the research and provides access to the case is the Manager IT of PayNow. Whereas the researcher is external to PayNow on account of the research being part of an internship at Deloitte.

The second and third principle relate to managing data and evidence. In order to follow these principles ATLAS.ti[3] will be used to manage both evidence and create a case study database separate from the case study report itself.

Data collection procedure

Yin (2018) describes protocol questions as a general line of inquiry, or questions, that guide the researcher on what data to collect for a single case. These questions can help shape what data needs to be collected in order to answer the research question. It is important to note that these questions do not constitute an interview protocol, but may help forming one. Moreover, in this protocol there are five levels of questions that can be asked (Yin, 2018). Each level constitutes a different type of questions.

Levels:	**Research:**
Level 1: verbal questions to interviewees	
Level 2: questions about a case	Research question 2 and 3
Level 3: questions about a pattern of findings beyond multiple case studies	
Level 4: question asked of an entire study	Research question 4
Level 5: normative questions about policy recommendations and conclusions	

Table 3 Five levels of questions, adapted from Yin (2018)

On account of empirical data collection occurring at level 2, protocol questions will only be defined for research question 2 and 3. Level 1 questions constitute the actual interview protocol which does not cover the entire data collection process. Below tables describe the protocol questions for the research questions. In addition, the sources of data and collected methods are highlighted per question.

For this research data source triangulation is used to strengthen the findings of the case. This form of triangulation is chosen on account of it being more feasible given the time than a method or researcher triangulation. Moreover, data source triangulation also helps to lessen the effects of recall bias present when only interviews are used. Sekaran & Bougie (2016) argue that a research can be more confident in a result if different sources or methods lead to the same result. Primarily interviews and if possible documents will be utilized to generate the findings. This allows for a convergence of evidence and thus more reliable findings (Yin, 2018). According to Smith (1981) interviews are particularly suited to the exploration of values, beliefs, motives and attitudes. Interviews will be recorded (with permission) in audio format and transcribed afterwards. Recordings are destroyed after transcription. In the thesis report interviewee names are anonymized and the case name is also anonymized. This decision was made in order to maintain to protect the privacy of interviewee's and the case company. Finally in order

[3] See: https://atlasti.com

to ensure the correctness of the transcripts, the interviewee's will be asked individually to check them for any errors.

Research question 2: How do platform sponsors adjust openness due to safety risks?	**Data sources:**	**Collection method:**
How does the organization learn about safety risks?	People Documents	Content analysis Interviews
How do safety risks affect platform openness?	People Documents	Content analysis Interviews
Why do safety risks affect platform openness?	People	Interviews
What role does (moral or regulatory) legitimacy play in adjusting openness?	People	Interviews

Table 4 Protocol questions RQ2

Research question 3: How do platform sponsors adjust openness due to privacy risks?	**Data sources:**	**Collection method:**
How does the organization learn about privacy risks?	People Documents	Content analysis Interviews
How do privacy risks affect platform openness?	People Documents	Content analysis Interviews
Why do privacy risks affect platform openness?	People	Interviews
What role does (moral or regulatory) legitimacy play in adjusting openness?	People	Interviews

Table 5 Protocol questions RQ3

Based on the above section a line of inquiry arises on what level 2 question should be 'asked' and ultimately guide the forming of level 1 questions and determine what data to collect from documents.

Interview protocol

The research will utilize semi-structured open questions to perform the interviews. On account of the research investigating a previously unstudied phenomena the questions are open-ended and not fully structured (e.g. not every person will be asked the same questions). Asking questions in an unstructured manner allows a researcher to question more freely and thus understand the totality of a situation better (Sekaran & Bougie, 2016). Nonetheless, on account of the literature described, the researcher does have some impression of what data needs to be collected. In contrast, structured interviews are conducted when the interviewer knows what information is needed (Sekaran & Bougie, 2016). Hence, the interviews will be semi-structured on account of having some guidance of the literature but remaining open to study the full phenomena. This also follows from the earlier mentioned reason of Vaughan (1992) to not look too much at the theory as it might prohibit looking further than the theory.

As mentioned above the interviews will be semi-structured and asked in an open-ended manner. Therefore the protocol questions and literature will guide the design of the interview protocol. For the interview protocol please refer to Appendix A: Interview protocol.

3.4.2 Data analysis

A desirable analytic strategy for case studies is pattern matching (Yin, 2018). Here a case study compares the empirical findings of the case studies with the predicted findings. Whereas the predicted findings are made before data analysis via for example relevant theory. As is the case here, a conceptual model is provided utilizing a set of theories. After performing the empirical data collection for the research, the findings will be matched with the initial conceptual model. From the matching of patterns between the conceptual model and the empirical findings a conclusion can be made on how platform openness adjusts via safety and privacy risks. If the pattern does not match the conceptual model then the proposed conceptual model will be questioned.

Content analysis

Interviews and documents will be analysed via a coding approach. Whereas coding is defined as: "the analytic process through which the qualitative data that you have gathered are reduced, rearranged, and integrated to form theory" (Sekaran & Bougie, 2016, p. 334). A coding approach lends itself to various qualitative research. One of these purposes is pattern recognition and theory building (Saldaña, 2013). Hence, a coding approach is utilized for this research. Furthermore, in order to gain a basic understanding of the organization the documents are analysed first. Afterwards interviews can be held. Based on the understanding derived from documents, interviewer can investigate more specific lines of inquiry that arose from document analysis. If documents are analysed last then it might not be possible to ask interviewees specific questions which might originate from the document analysis.

The coding process will follow two iterative cycles namely: a first cycle of coding – initial coding (Corbin & Strauss, 1990) and a second cycle of coding – pattern coding (Miles et al., 2014). First a preliminary list of codes will be defined based on the literature gathered. This is done in order to guide the search and not miss any relevant codes. If any relevant patterns occur that do not fit in existing codes then a new code will be made (Sekaran & Bougie, 2016). Following this step, initial coding will derive a first set of codes for interviews and documents based on selected words, sentences or paragraphs (Saldaña, 2013). Secondly, via pattern coding so-called pattern codes are defined that group a set of codes or categories together to identify themes, explanations or configurations (Miles et al., 2014). According to Miles & Huberman (2014) pattern coding is especially fit as a search for rules, causes and explanations in data. Subsequently, this allows the formation of constructs and processes. Considering the purpose of this study, this coding approach seems fitting as a coding approach. These pattern codes can form categories of codes and lead to identifying themes in the data. Finally the themes and relationships between them are the result of the analysis (Saldaña, 2013)

An example of potential initial codes and a subsequent pattern code is provided in the figure below:

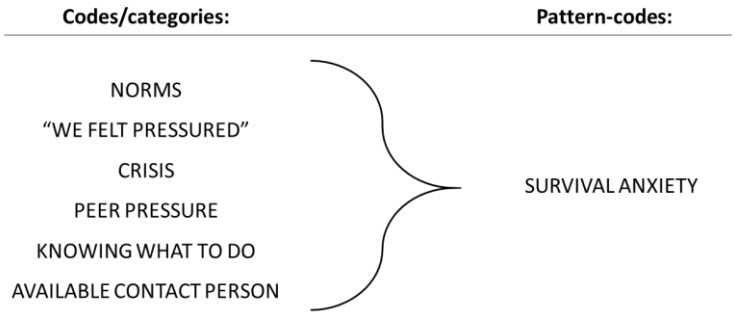

Figure 5 Example of codes, categories and resulting pattern-codes

In order to maintain evidence of the researchers coding activities and subsequent changes to codes, categories or relationships so-called analytical memo's will be made. The purpose of these memos are to document and reflect on the coding process, choices made during the coding process and the emergent patterns that lead towards theory (Saldaña, 2013, p. 41).

4. Results

This chapter answers research questions two and three. First, this chapter describes how the platform adjusted openness to due to safety risks according to the results found. Secondly, this chapter highlights how privacy risks adjusted the platform openness.

Each chapter follows the structure of first outlining a relevant event (referred to as context). Following the provided context the event is analysed according to the content analysis performed. Whereas first the risks observed are discussed. Consequently, how and if these risks affect legitimacy is discussed. Then survival tensions are described in order to understand how this led to changed background theories. Subsequently, any, if at all, changes are described in the background theories section. Finally, a description of how openness changed is provided.

Actor network

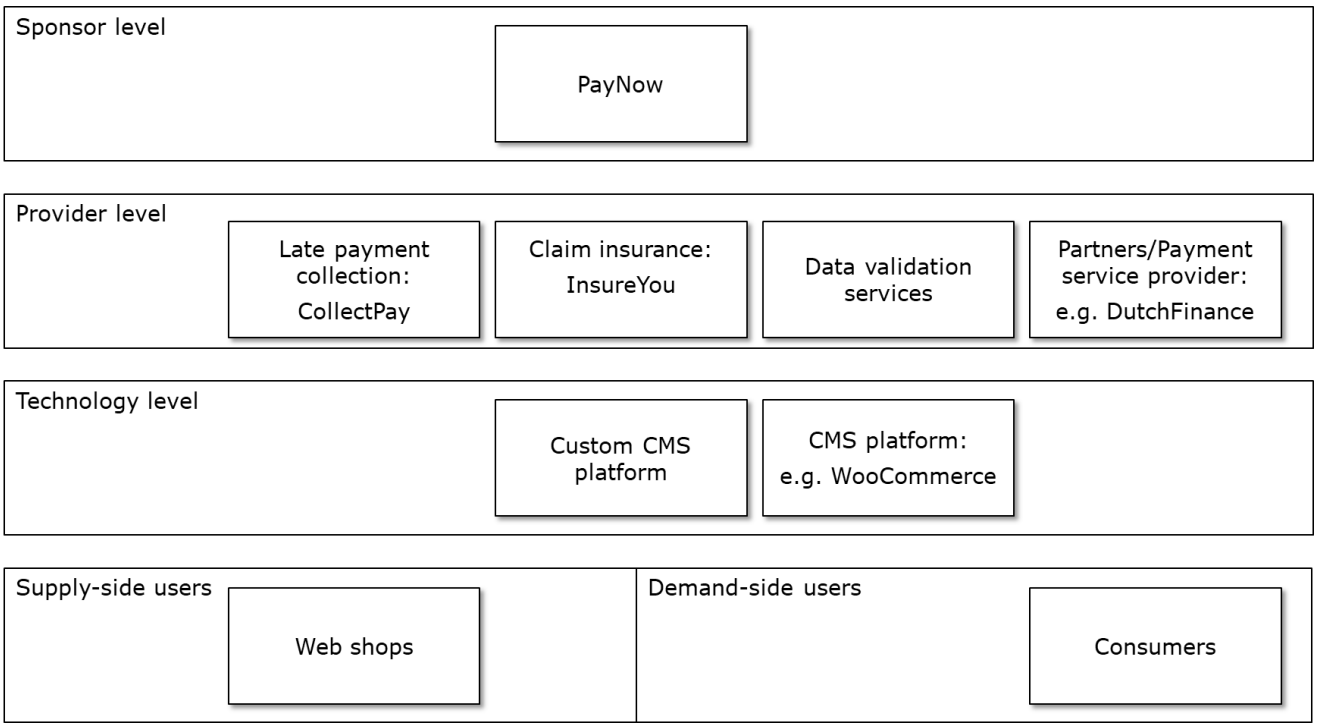

Figure 6 Actor network PayNow platform, based on Ondrus et al. 2015 structure

Figure 6 graphically represents the actor network per openness dimension of the platform. Whereas PayNow provided the payment solution for web shops, which consumers could use to order items online. The above map is not exhaustive and only includes the parties which affected or were indirectly or directly affected by the changes in openness according to the interviews and documents collected. In addition, the above actor network describes actors that of which some were present from 2018 and onward or were no longer present from 2018. Details on these transitions are described in the findings.

On the provider level no distinction is made between complementors and partner providers. As described similarly by Ondrus et al. (2015) complementors do not extend a platform's openness directly (e.g. increasing total user base). Yet, in this case they do indirectly have an effect on openness. Hence, they are viewed as necessary and included on the platform level. For example, CollectPay, collects any

unfulfilled payments for PayNow. Although this does not extend the maximum potential user base of the platform, it can restrict it. If CollectPay chooses to have a more restrictive collection policy than PayNow, then this can constrict the openness of PayNow. Another example of this is InsureYou. InsureYou essentially insured the company against non-payment forms such as fraud. If they chose to no longer insure certain parties then openness will be restricted for PayNow A similar dynamic will be explained in detail later for the actors performing data validation. Finally, also partner platforms do affect the userbase on account of payment service providers or partners being able to connect existing users with PayNow's userbase.

On a technology level PayNow allows for custom plug-ins or pre-made plugins for major content management platforms (CMS) such as WooCommerce to be able to be used by web shops. Hence, the openness toward these platforms affect the total possible userbase.

With PayNow as the focal case, this chapter describes the findings related towards the changes over time to openness on account of certain risks.

Data analysis

In order to analyse the data the widely-used qualitative data analysis software Atlas.ti version 8 was used to code the documents and interviews. In order to steer the data analysis to relevant concepts an initial code list was developed based upon the literature review. However, in order to remain open to interesting concepts outside the pre-defined literature, for both documents and interviews one item was open coded without the initial code list in order to verify the usability of the initial codes and not miss any other codes. The codes resulting from these first-passes of one document and one interview were merged or in case there did not exist a code for the concept added as a new code to the initial code list. Subsequently, first all documents and then interviews were coded. Documents were analysed before the interviews were held in order to provide the researcher with sufficient understanding of the context and if necessary adjust the interview questions based on the information gathered from documents. The coding focused on concepts that involved background theories, risk, legitimacy, survival tension and platform openness dimensions. Besides these concepts the researcher kept an open mind to other factors that explain why or how platform openness was adjusted.

The initial code list existed out of 91 codes based upon literature (See appendix B for initial list of codes). Open coding used the list and created new codes and categories if an applicable code did not exist yet. Consequently, open coding resulted in a total of 253 codes (and categories included). After cutting and merging codes and categories a total amount of 122 codes was left (See appendix C for final list of codes). Codes that were seldom mentioned or viewed as not essential to the research were removed. Furthermore, codes that overlapped, were considered as too specific or described similar concepts were merged (Friese, 2012). In addition some sub-categories became categories on their own due to relationships that were not shared with the above categories. Pattern codes were developed based on one interview and verified with other interviews. Subsequently, a pattern code for the case was developed. Resulting in six pattern codes describing identified patterns (i.e. processes) in the data. Pattern codes were developed following the identification of rules (i.e. if-then relations) (Saldaña, 2013) and causal relations between codes. Relationships between codes were verified by re-reading quotations from codes and if unclear then re-reading transcripts. The process of introducing, removing and merging codes/categories is described alongside the findings. Codes and categories are referred to in text via italics (e.g. *risk identification*). In some chapters, a supplementary diagram of relationships is

provided. These diagrams serve as a reading aid to better understand the relationships described in the findings. They also underline the complexity of the case and may clarify the sequentially of events. These diagrams are only provided for chapters with many different codes/categories interacting. The process with examples of codes and merging is provided below.

Coding phase:	**Number of codes/categories:**	**Example of coding:**
Initial code list	90	Codes are introduced based on researched literature • Sun & Scott (2003, p. 211) provide the following examples of drivers of survival tension: threat of a competitor, threat of job loss, continued heavy workload, criticism of customers and stakeholders and the chance of promotion" Categories are capitalized: • TENSION Sub-categories are written as follows: • Tension: survival • Tension: learning A code subsequently looks like this: • Tension: survival: threat of competitor
First cycle - Initial coding of documents/interviews	253	First cycle coding of documents used the initial code list for coding, but created new codes if an existing code did not describe the phenomena. "Guys I don't think you should want this as a company. Doing business with these kinds of parties. Although those parties are in principle responsible for their own processes, we as a platform also have a role in this. And also we have to be very careful for our own image. And if we want to increase that in the long term in a sustainable way, say, that image. Then we have to make sure that we also do business with parties who contribute to it and, above all, do not negatively affect it." • Codes: *Duty of care, Moral legitimacy: threat, Risk: reputation, Platform openness: supplier, Theories-in-use: strategy* "But if you suddenly receive ten calls about web shop X […]: Hey I have not received something, or they said I would receive this but I have something completely different, or they said that I may not return it while that is actually allowed. At some point it will simply stand out." • Codes: C*lustering of complaints, Complaints, Criticism of customers*
Cutting/merging codes	125	Categories and codes are re-evaluated and cut or merged: • New category *risk identification* is defined, because *complaints* are not necessarily risks, but are necessary for identifying risks; • A new code is created *Usage of personal data* denoting how this usage is affected due to privacy values or risks;

Coding phase:	Number of codes/categories:	Example of coding:
		• Merged *Younger organization* with *Organizational maturity*.
Pattern codes	7	Pattern codes were developed from codes that seem to denote a certain process or pattern in the organization. Pattern code: LEGITIMACY AND ORG. MATURITY Codes/Categories: • Responsibility, duty of care, Profitability, Moral legitimacy, Regulatory legitimacy. Description: • According to several quotations it seems as if organizational maturity affects the regulatory and moral legitimacy, as well as the profitability and responsibility/duty of care of an organization. Hence there might be a pattern there.

Table 6 Coding process examples

4.1 How does PayNow adjust openness due to safety risks

In order to answer the research question a sub-set of questions was developed. These questions steer the direction of the chapter. Below findings are based on documents received and interviews[4] held with PayNow employees.

Context

In order to understand how the organization learns about safety risks, first the safety risks must be put into context and described. In the PayNow case there are a few events where PayNow learn about risks that made them adjust their platform openness. However, in this research the most interesting event is focused on the event leading up to PayNow identifying a risk that potentially hurt consumer trust, and where they subsequently acted to oust these parties from the platform.

In 2018 PayNow ousted several web shops on account of their methods of doing business not aligning with those of PayNow. Other actors such as a Dutch authority also investigated the web shops. Consequently, they also enquired about these parties with PayNow on account of their involvement in facilitating payment. However, to the benefit of PayNow they ousted these web shops from their platform a few months before the investigation. Nonetheless, if the investigation was unexpected, then what motivated PayNow to limit their platform openness?

The web shops in question were part of a shopping segment that sold supplements. Some of these web shops allowed 'free' sample packages for trying out the product. However, these sample packages ended up being not free for *trying* after all, as consumers were obligated to pay for their order once they opened the package. Hence, this caused a large amount of complaints directed at PayNow (IN1). Yet, complaints are not an immediate cause for concern. Moreover, often web shops that sell a particular type of product attract consumers that are more inclined to complain online. Consequently,

[4] Interviews were all held in Dutch and transcribed and coded in Dutch. Hence, quotes used from interviews are translated by the author from the original Dutch transcription.

the amount of complaints per web shop does not determine whether a web shop is treating consumers poorly.

Almost every interviewee attributed the risk and the kicking out of these web shops to misleading consumers. Consequently, a safety risk did not seem to affect the decision-making of the organization in any significant way. More prominently, it was the fact that these web shops seemed to actively mislead consumers that was deemed morally reprehensible by the directors of the organizations (IN1).

How did the organization learn about this risk? Before 2018 complaints that were put through via mail or calling ended up at the customer service desk of PayNow. When consumers received a bill from PayNow, quoting a sample package of pills sold. They would try to call the web shop that sold them the pills. However, the dubious web shops were often unreachable. Consequently, PayNow would start to receive the complaints of these consumers instead. Some interviewees stated that from the moment these clients started selling via the PayNow platform complaints already starting pouring in. The amount of a complaints was deemed disproportionate relative to other clients (IN5). The disproportionate amount of complaints caused some employees to take note of the web shops and would try to contact them. One interviewee said that there were a lot of non-paying consumers with these clients and only a small amount of them would complain (IN1). Hence, it was not immediately clear why they weren't paying, as PayNow was only an online payment solution. Yet over time the complaints started to noticeably cluster around certain web shops (IN5; IN7; IN8; IN9). Subsequently, although these web shops ran a lot of orders and were at some point in time responsible for a large part of the total revenue of the organization, they were also responsible for a large part of the complaints at customer service (IN5). This clustering of complaints led to an undue burden on the customer service, but also motivated PayNow to start asking questions on the behavior of the web shops. A second factor that contributed to the identification of the risk was the fact that the percentage of paying consumers was significantly lower than other web shops. Hence one interviewee recalled questioning:

> *"Why don't those consumers pay? Are they being lured by that web shop, or is it that the products are not good? Or is there more to it?*" (IN1)

Consequently, PayNow confronted the web shops multiple times with their misbehaving. Although the web shops said they did nothing technically (i.e. legally) wrong, they reluctantly made changes to their web sites. However, soon thereafter new complaints would come back (IN7). As one interviewee said it: "they were treating symptoms, but they never had the intention of actually changing their methods" (IN2).

In May of 2018, there was a tipping point in the disposition of PayNow toward these firms. PayNow decided to no longer offer their platform to these type of web shops. According to IN1 this was triggered after there was disagreement between the founders (directors) on keeping this type of clientele. One director found the practices of the client morally reprehensible, while another director did not agree it was their responsibility to think anything of a web shop's practices. Regardless, this triggered the directors to ask the company lawyer to perform a due diligence/compliance investigation into a selection of web shops that contributed to the large amount of complaints. This led the company lawyer to report to the director that five web shops were actually misleading consumers. In addition, he reported that this could have legal repercussions and could damage the reputation of PayNow. This left the choice for the dubious web shops: become compliant with [PayNow's terms of business] or leave the platform (IN1). This decision was not made lightly.

In fact the decision led to the organization questioning: will we let our openness remain the same in the future? In a company presentation the connection was made between accepting everyone and potentially risking similar clients or starting to look at the longer term (IN2). Leading to the question: will a selection of even larger or better clients want to do business with a company that is associated publicly with these type of companies (IN2)? Associating with these companies would hurt the company's reputation but also their future prospects (IN1, IN2).

Ultimately, this led to the installment of stricter due diligence process before onboarding new clients and the implementation of a compliance officer role. Not soon after the external investigation into these dubious web shops occurred. According to IN1 a matter of luck that they implemented the controls before, seeing that they did not expect the investigation. Nonetheless, the question can be asked. Why did PayNow decide to let the parties go? According to IN2, the discussion was triggered after the owners of the dubious web shops wanted to add a large number of new labels (i.e. web shops/products) to the PayNow platform. In addition, the prospect of the additional 'hassle' of processing the complaints was not favored in the organization. Furthermore, IN5 also introduced a second factor that triggered a re-organization of some practices in the organization.

As stated before PayNow essentially takes over the debtor-risk, by paying the web shop and taking over the debt of the consumer and then collecting it. The debtor-risk is the risk of a web shop (not) receiving payment from debtors (i.e. consumers). Before the events, PayNow insured this risk at a third-party called InsureYou. This party also decided which consumers were allowed on the platform based on their so-called credit check. Around that time, the third-party announced that they were stopping the debtor-risk insurance service. Forcing PayNow to handle the debtor-risk themselves and develop a credit check. At that time PayNow was already working on a transition towards their own credit check. Previously if consumers did not pay then third party would try and collect, however, when they had to start doing it themselves, this risk also became theirs. Hence, not only the complaints became a problem but also the financial risk of keeping these clients increased (IN5). This was raised by the finance manager as an additional factor that motivated PayNow to stop servicing these clients.

Nonetheless, stopping the service for these clients and implementing a due diligence was not enough. The authorities also investigated PayNow's involvement in the matter. To the satisfaction of the authority PayNow ousted the web shops as soon as they learned of the misleading. Yet, PayNow argued that they were not responsible for holding web shops compliant with the law or certain standards (IN1). More so, the platform exists to protect the consumer (IN11) and that is what they did by ousting these parties. On this matter the authority did agreed. Yet, although PayNow is not responsible for making web shops complaint, the authority argued that they do have a duty to steer web shops that seem to be unfair in their business practices. In essence, this communicated that PayNow has a duty of care to safeguard the quality of service for consumers.

This event in the case highlights how and why the risk of misleading web shops affected platform openness. In addition, it also describes how the organization went from identifying risks via consumers (i.e. reacting) to identifying risks also via the due diligence procedure (i.e. anticipating). Yet, as can be seen in this event and other events in the case it was not necessarily a safety risk that influenced the decision-making in the organization.

4.1.1 Types of risk

This research hypothesized in the introduction (section 1.1) that risks affecting societal values also influence openness. Specific anecdotal evidence was found on the impact of safety and privacy risks. Hence those risks were used as the starting point for the research. Instead, as became clear in the various interviews, that a safety risk was not a prominent risk to the platform. Based on the first few interviews it became clear that the employees in the case acted upon learning about other risks. Hence, the researcher made the decision to utilize the more general definition of risk which is: an unwanted event that may or may not occur. This decision was made on account of the first few interviews already questioning the existence of a safety risk. Hence, the interview script was adjusted to account for other risks identified that seemed to have an effect on the openness and/or the decision-making of the organization. These risks are outlined below. Some risks also relate to a different event than the one described in the previous section. This event will be clarified alongside each risk.

As a result the conceptualization of risk was expanded to include other types of risks encountered that seemed to have altered decision-making related to openness. This led to the overarching category of *risk* to be introduced. Furthermore, it was observed that risks were not directly identified (*risk identification*) a priori, instead there were certain triggers that allowed the organization to react (e.g. questions/complaints at the customer service) and anticipate (e.g. due diligence policy) risks. Whereas the former provided the organization with the experience (*earlier experience*) to anticipate in the future.

Misleading / unfair trade practices risk

The most prominent risk that affected PayNow, as was apparent from the context description above was the risk of *misleading consumers / trade practices* otherwise also referred to as illegal or unfair trade practices. Hence, when PayNow learned about the risk caused by other web shops they instated the due diligence process. Whereas the due diligence was utilized to prevent similar 'bad apples' from joining the platform again. In doing so, the due diligence verifies whether the web shop does not try to mislead consumers via marketing, hidden agreements and/or does not conform to the terms of service of PayNow among other legal requirements.

Firstly, PayNow provided a payment solution to these parties, whereas these parties sold ordinary supplements normally. Yet, one of their marketing methods was to offer sample packages that were 'free' to try. However, as soon as consumers actually tried the sample they were obligated to pay. This generated a lot of *customer complaints* for PayNow. Complaints were a natural part of any web shop, sometimes caused by maleficence but mostly on account of negligence on the web shops part. As in this case, customers that were unhappy reached out to the web shop, however as they were very difficult to reach (web shop negligence), they started reaching out to the company that actually billed them, PayNow. Yet, at some point in time these complaints started to cluster (*Clustering of complaints*). Moreover, the clustering of complaints actually also started to threaten the reputation of PayNow (*Risk: reputation*) by association. As a result of consumers that felt misled, the amount of people that actually paid started to go downhill (*payment percentage*). Leading to criticism from a partner (*partner complaints*) organization that had to deal with the lowered payment percentage. The moment the owners of the web shops wanted to add more web shops to the platform a discussion started internally at PayNow. Did they want more complaints? Moreover, what was going on at these web shops to cause non-payment and all these complaints? Upon investigating further PayNow found that although the details required for purchase were all there, the marketing and tiny letters on some web shops (*Web*

shop marketing) were found to be a morally reprehensible method of sales. One interviewee stated that based on common sense alone there was something wrong with the way these parties did business (*Common sense*). Finally, leading to PayNow starting a compliance investigation into the dubious web shops resulting in the identification of the risk of misleading.

Taking advantage of vulnerable groups risk

In some interviews it was mentioned that the *type of customer segment* targeted by the dubious web shops weren't critical people (*vulnerable group affected*) (IN2; IN5; IN6). As stated before on paper, everything needed to make a sale was there. Yet, on account of some of the complaints PayNow received, various consumers did not understand the agreements they signed when they signed up for free samples. One interviewee said this on the matter:

> *"In general the information they [web shops] provided was, if you read it, it was correct. It just said how it [the product] worked, and it just said what could and could not be expected. It was expressed this in such a way and promoted in such a way, that someone who is less smart and less attentive. Such a person falls for it [the marketing] and takes other assumptions on the basis of which they make the purchase."* (IN2)

Hence, some interviewees said that the way these web shops weren't doing anything seemingly illegal upon first sight, but they did have ethical issues with the methods of marketing and selling these products to specific consumer that were less equipped to read the purchase agreement they agreed to.

The figure below highlights the codes and their interrelationships using (bi)directional arrows indicating the type of relationship. Three types of relationships are used to convey the model. First, 'is cause of' relays the finding that one variable affected another variable unidirectionally or caused it. Second, 'is associated with' describes a relationship that is not directly causing an outcome to occur. Instead it conveys an indirect or bidirectional relationships between variables. Thirdly, 'is part of' denotes a code that is part of a category or larger super code.

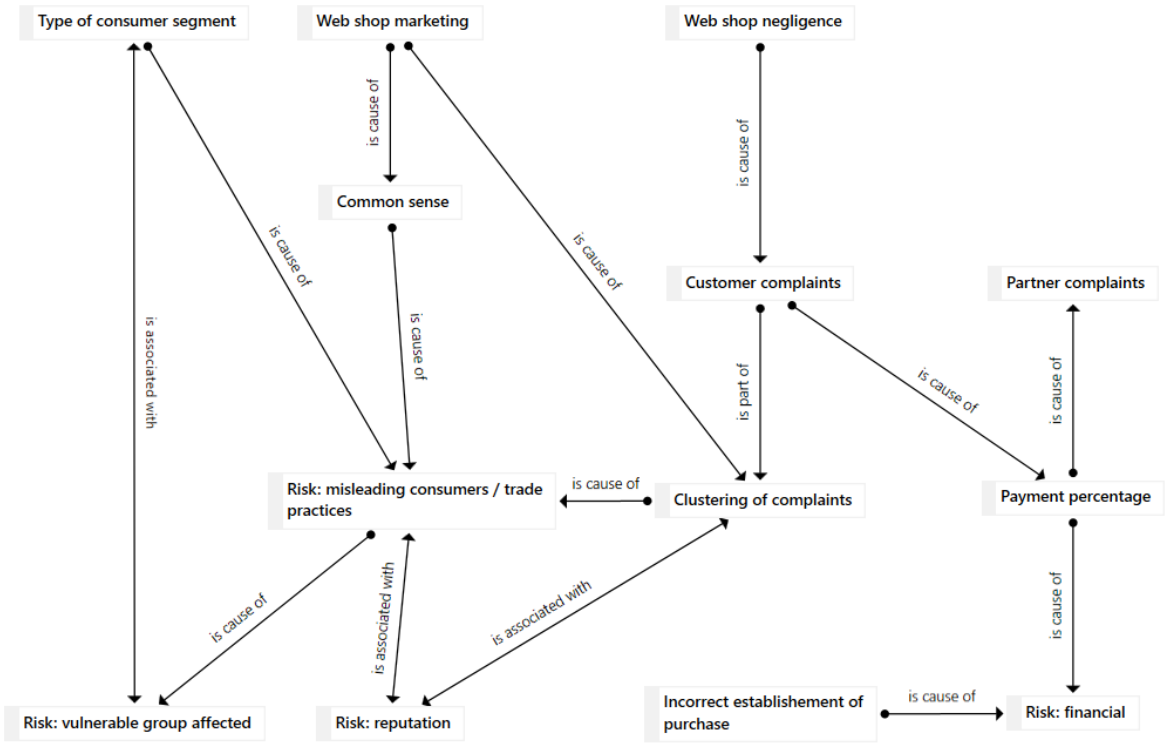

Figure 7 Network diagram risk of misleading

Regulatory risk

Before the dubious web shops were ousted, an internal compliance investigation that was performed highlighted the possible regulatory risk by abetting the web shops in their practices (*Incorrect establishment of purchase*). In another event in the case, PayNow recently decided to halt the onboarding of new smartshops. Smartshops are retail shops that sells among other things, psychoactive substances or the gear to create them. These shops are not necessarily illegal unless some strict rules are followed. Yet, according to some interviewees (IN4, IN6) these shops (*type of web shops*) operate in a legal gray area with the type of product (*nature of product*) that they sell and there is an especially thin line between what is legal and illegal. For example selling a small amount of a psychoactive substance is legal, but if large amounts are sold through PayNow then they could be charged with abetting to large-scale drug trading (IN6). This suggests that *regulatory ambiguity* affects the *risk appetite* of the organization. One employee responsible for deciding to take on no more smartshops cited the 'impossibility' of making sure that every order sent is complaint (IN4). Hence, making it a risk to serve these type of shops. In one interview with an employee of CollectPay the issue was raised that he doesn't accept smartshops as clients citing the regulatory risks (*Partner complaints*) but also mistrust of these web shops (IN6). Furthermore, if a web shop was not compliant with relevant laws (*non-compliance web shop*), then this could introduce a regulatory risk for PayNow in (unknowingly) facilitating the sale of *illegal products* or illegal quantities of goods.

Illegal products risk

The interview with IN6 also highlighted the differences in due diligence between PayNow and

CollectPay. As CollectPay has strict sector-specific regulation overseeing that they do not collect money for illegal products they verify that a web shop does not sell illegal products before onboarding them. According to IN6, trying to collect money for an illegal product legally voids the sale. This is also the same for PayNow, but they do not verify whether illegal products are sold via the due diligence check. Upon investigating further this might have something to do with the platform openness of providers of PayNow. In addition, in various interviews (IN4, IN5, IN6, IN7) the type of products sold are quoted as reasons that affect the platform openness of PayNow itself. Thus, while this might not be codified in the due diligence policy, PayNow does indeed check for what products are being sold before the platform is onboarded (IN11).

An alternative explanation might also be that third-party openness might affect the openness of PayNow. PayNow works together with another Payment Service Provider called DutchFinance to pay web shops for their orders. Recently DutchFinance announced to PayNow that they would no longer accept smartshops on their platform. Hence, limiting PayNow's own openness toward these smartshops (IN9). Another partner is CollectPay. After 90 days of late payment, CollectPay will take over the debt and try to collect it form the late-paying consumer. However, reportedly CollectPay shuts down the majority of smartshops on the platform. Hence the openness of a third-party might limit the openness of PayNow if they cannot collect on late payments or credit all web shops.

Second, the type of products sold also seem to affect the *type of consumer segment* reached. Whereas, in this case smartshops attracted a segment that did not pay on time often or at all (*payment percentage*). In an interview with the employee that decided to stop serving smartshop said that "Not because of their products, I don't want to have a discussion about that. But purely because it attracted an idiotic customer group" he made the decision to stop onboarding new smartshops (IN4). Whereas the payment percentage also adds to a financial risk (*Risk: financial*) in accepting such web shops onto the platform.

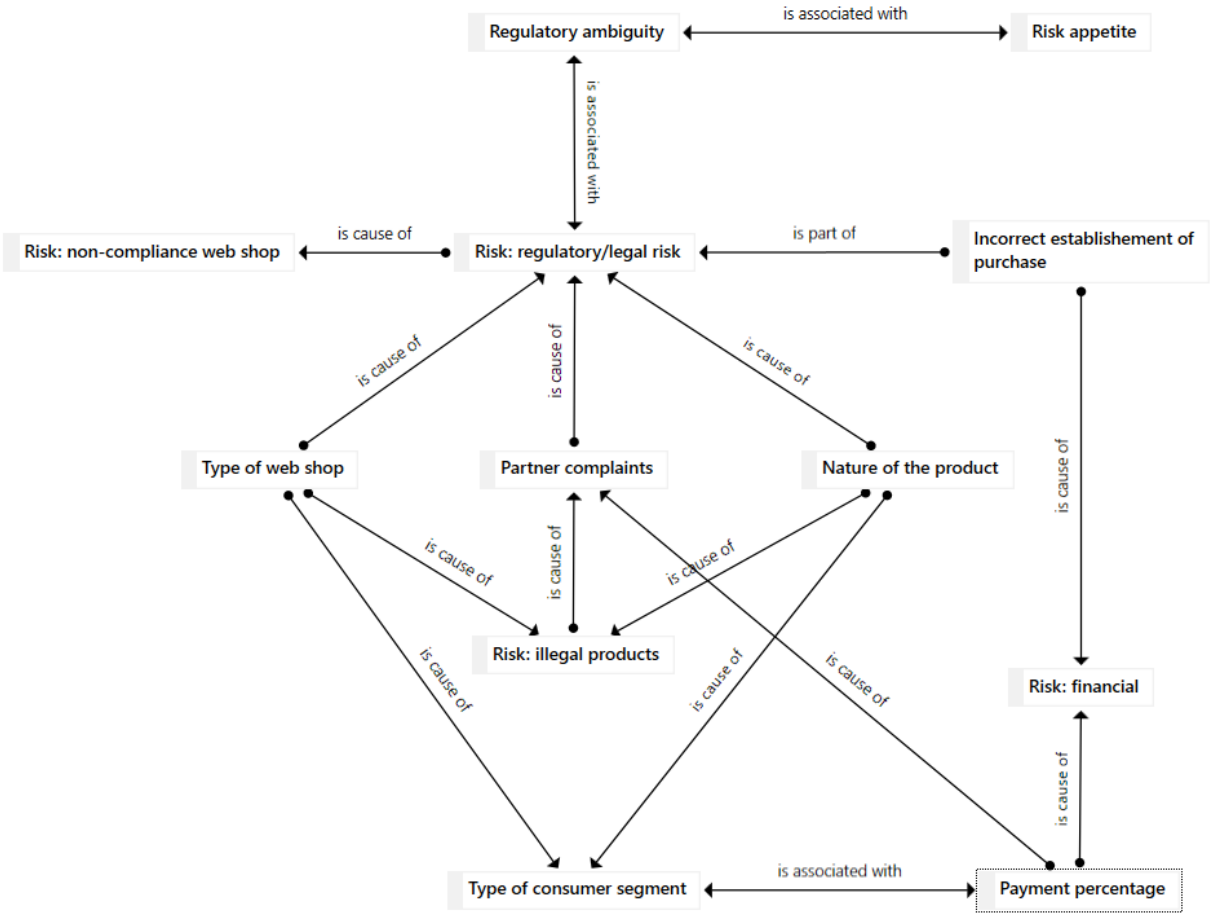

Figure 8 Network diagram of illegal products risk

Fraud risk

Although not affecting a societal value directly, but the fraud risk (*Risk: fraud*) of consumers defrauding PayNow affected user openness. PayNow utilizes a credit check that requires each consumer's data to meet certain integrity criteria. If those criteria are not met, then a consumer is denied access to the platform. Based on *earlier experience* PayNow noticed that certain *type of products* and the *price of products* affected how much fraud occurred via a web shop. Subsequently, they started adjusting the user openness per web shop based on their product mix and product value using their *common sense* on what they think would further attract fraud. Specifically common sense could be argued to delineate the assumptions about fraudulent shops due to the connection of value and the nature of the products to fraud. The detailed effect of this on the openness of users is outlined in section 4.1.2. In addition, if a web shops was negligent in their payment configuration then it also allowed for certain types of fraud to occur and consequently leading to a lower payment percentage on some web shops that sold fraud-sensitive products.

It can be argued that there was no threat to legitimacy here. However, as a sales employee said, being sure of payment is one of PayNow's guarantee (IN7). Besides the financial impact of fraud, it was noted that they also want to prevent negative publicity (*Risk: reputation*) on account of being negligent in preventing fraud on their platform (IN7). However, this view was not shared by other employees.

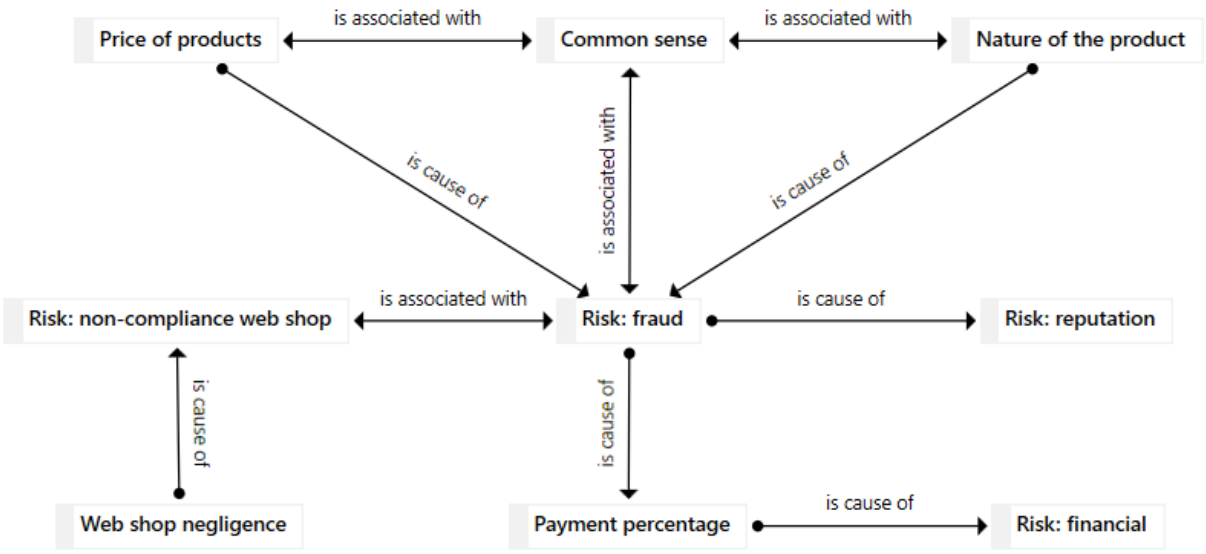

Figure 9 Network diagram of fraud risk

Financial risk

A risk that was mentioned besides many other risks, or more as an effect of another risk, was the financial risk (*Risk: financial*). PayNow that started doing the credit check themselves introduced financial risk in the form of fraud risk. Furthermore, according to one interview the cause for PayNow to oust the dubious web shops was not reputation related, but instead purely a financial decision (IN5). The amount of non-paying consumers was relatively high for these web shops and this introduced an undue financial risk to the organization. Subsequently, the organization was motivated to let these web shops go. Furthermore, non-payment was also an effect that lowered the *payment percentage* and was a result of different risks.

In an interview with CollectPay, financial risk was also introduced as caused by the potential voiding of agreements. If PayNow or CollectPay try to collect money for illegal products then this could void the agreement of sale, because you cannot legally sell illegal products. Yet, PayNow itself does not inspect for illegal products in their web shops as much as CollectPay does. In other cases, where the establishment of a sale is not correctly done by a web shop (i.e. hiding costs/price) then a sale can also be voided (*Incorrect establishment of purchase*).

4.1.2 Moral and regulatory legitimacy

In the interviews it was found, and shared, by employees that the decision to let go of the web shops was based on impact or threat to three factors: *moral legitimacy*, *regulatory legitimacy* and the profitability of the organization (*Profitability of platform*).

First and foremost, moral legitimacy. PayNow received negative critique from consumers on reviews, complaint sites, via emails, calls and even became the topic of discussion on a public complaint forum, which is used by a quite a few people. This not only threatened but also impacted the moral legitimacy of the organization. In different interviews some interviewees asked themselves whether these web shops were doing business in the right way? As mentioned before, a discussion on the morality of the

web shops between the founders of the organization started a due diligence investigation on these web shops. Moreover, it was raised that if PayNow wanted to garner a higher-class of clientele then they should not be associated with parties such as these (IN1; IN2).

The compliance officer of the organization highlighted three factors on advising the founders on why these web shops should be let go:

> *"Please note that you have a reputation risk here by being associated with this party that does indeed violate the law. In addition, from a legal perspective, you take over their claims, hence it may also be the case that you take over nullifiable agreements or secondly, take over agreements where the willingness to pay is bizarrely low."* (IN1)

Another interviewee stated that if a party can make your reputation worse, then you shouldn't want to do business with that party (IN2). Hence, indicating a perceived threat and impact to the moral legitimacy of the organization.

The regulatory legitimacy of the organization also seemed threatened in the sense that judge could rule the claims of PayNow nullifiable. In addition, an interviewee also raised that the claims made by the web shops were not in line with law on consumer rights (IN1). Hence, this added to the reasons as to why they wanted to let the web shops go. Nonetheless, the fact that the organization choose to investigate the compliance of the web shops after the discussion on the morality could be performed due to a perceived regulatory threat. According to some other interviewees this was indeed the case (IN4).

After the compliance investigation finished the organization chose to let go of the dubious web shops. Afterwards, they formally instated a compliance role in the organization, and created a compliance policy together with a due diligence procedure to be performed before new web shops were added to the platform.

> *"Many people even mistook us for that party. There were so many complaints on the Internet at one point, we really had to do something with that to get our reputation polished up again. And that was a very good argument, of course, in that whole decision to stop doing business with them."* (IN2)

As the quote above highlights, some interviewees already perceived an impact to moral legitimacy to have occurred. After which restructuring of some processes took place and gradually also introduced a change of beliefs in the organization. This will be outlined further in section 4.1.4.

Finally as mentioned before there was also financial component to the decision making of the organization. One interviewee mentioned that any impact on the reputation of the organization must first be managed before another sale can be made by the organization (IN7). This suggests a relation between the profitability of the organization (*Profitability of platform*) and the reputation (i.e. *moral legitimacy*) of the organization. In addition, the risk of nullifiable sales might pose a direct threat to regulatory legitimacy, but the impact of a nullified sale also has a direct financial impact on the organization.

Nonetheless, the dubious web shops were already a part of the platform for several years (IN9). Conversely, in some interviews the dubious web shops were referred to as web shops that brought in high volumes of orders and were a large part of the revenue in the beginning of the organization. Hence, they added to the profitability of the organization while still hurting the moral and, unknowingly, the

regulatory legitimacy of the organization. After the events they were described as providing the organization poorly paying consumers. An explanation for this might be the insurance company no longer providing insurance for the claims collected. Coincidentally, and unrelated, this occurred around the same time as the dubious web shops were ousted. InsureYou announced to PayNow that they were stopping their insurance service for all consumers. Hence, from that moment onward PayNow decided to manage the financial risk of claims themselves. Yet, as one interviewee said although this exposed them to more financial risk, it cost them less because they did not have to pay insurance costs anymore (IN5). Another explanation is provided in another interview and raised in several others as well. Namely, the fact that in the beginning the organization needed these type of web shops in order to grow. As PayNow was in a financially healthy position in 2018, they did not need these type of web shops (IN2). Consequently, a tradeoff between legitimacy and profitability was made. Seemingly the maturity (*Organizational maturity*) of the organization affected how the trade-off was perceived. The concept of organizational maturity is described in more detail in section 4.1.4. The below diagram highlights the relationships between the concepts. In doing so, the diagram abstract the earlier chapter on risks to contain the categories of risk, risk identification and earlier experience to delineate how risks are identified as just a threat to legitimacy.

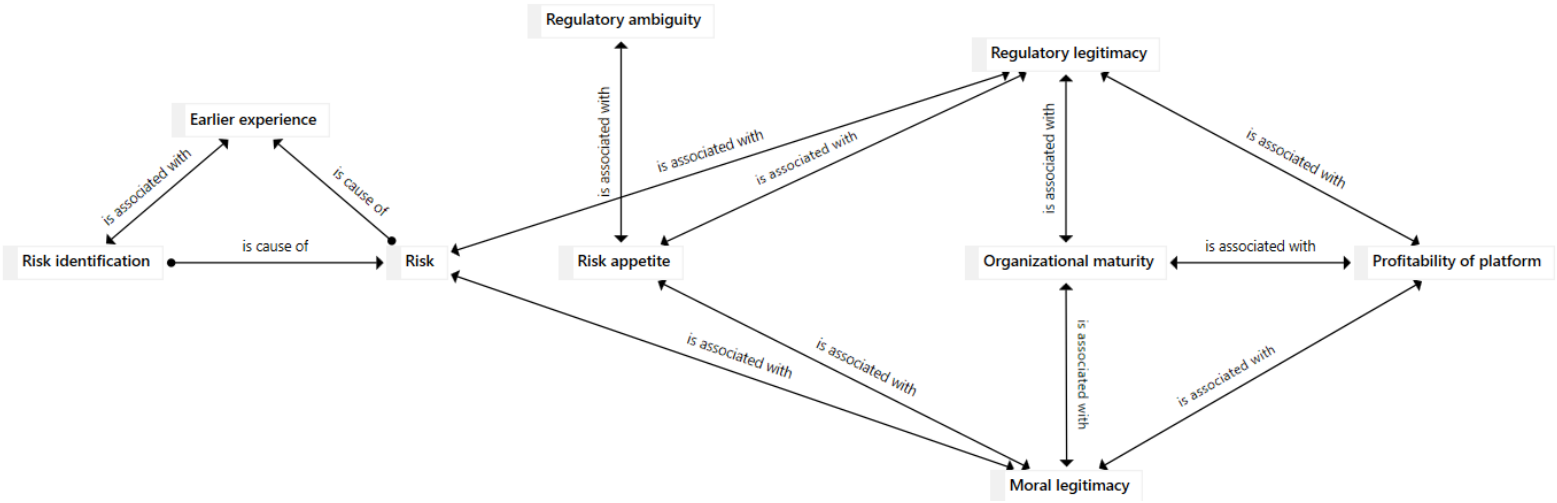

Figure 10 Network diagram threat to legitimacy other risks

4.1.3 Survival and learning tensions

What caused this change in the tradeoff and what caused the organization to let go of the web shops in the first place? This section will first outline the motivators of change or known conceptually as survival tensions. Secondly, the inhibitors of change, or learning tensions, are outlined as contrasting survival tensions.

Survival tensions

Interviews pointed to several reasons for change such as: 1) *criticism of consumers*, 2) *criticism of stakeholders*, 3) *threat of [an increasing] workload* due to complaints and 4) *threat of regulatory interference* for why they ultimately decided to let go of the web shops. The impact of these factors are outlined below.

The criticism of consumers was widely cited as a motivating reason to let the parties go. Not only the complaints the service desk added to this but also public reviews of PayNow hurt the image of the organization as illustrated by the following quotes from interviews on the dubious web shops.

> *"[…] I think that at some point that just escalated, especially when those parties suddenly wanted to add multiple labels with us. They worked with labels [of products] and then there was another request for a new label. Then we suddenly said ho-ho we already have a lot of trouble with existing labels. We are not going to connect new labels. In fact, we are going to take a look at those existing labels and maybe we should stop doing that once"* (IN2)

> *"Back then we had so many complaints about those web shops. And of course we also knew ourselves that it was not good. And I think it [the complaints] certainly played a part in the decision. Because from all sides it was negative. Also from service desk customers. Half [of all the complaints] was just about the [confidential]. And yes, then you just have to say that you shouldn't want to cooperate with this. Your customer service goes home depressed. And it is also not good for the consumer."* (IN8)

The criticism of internal departmental stakeholders also played a role in the decision to let go of the web shops. For example the customer service itself had asked multiple times over the years to change the agreements with the client or let the web shop go (IN8; IN9). In the end the answer from sales remained the same for a long time. They brought in a lot of revenue and we need them to grow. This might also be indicative of *individual* background theories instead of organizational background theories that cared. Consequently, this would explain why no action was taken earlier after complaints from another department.

In another case, CollectPay itself was also a party that told PayNow they were receiving an extraordinary amount of complaints. As CollectPay would collect money via calling, mailing and texting they more often actually talked to a consumer. These people were more ready to tell them why they weren't paying their bills as it was less easy to ignore a phone call and a text message than a mail or letter. One interviewee said that CollectPay even dedicated special resources to these web shops in order to process all the complaints received (IN2). Which added to tensions on keeping these web shops. Two side-effects of this criticism were that customers that felt wronged also had a tendency to not pay (*payment percentage*) and these web shops left a few people feeling wronged (IN1). In addition to the fact that if PayNow got negative reviews then that could mean that their competitor would rank higher than them in ratings (*threat of competitor*) (IN5). An additional reason was also given by the finance manager. When PayNow suddenly had to deal with the fraud risks and non-payers themselves they did not have sufficient processes (*insufficient process/technology*) to handle the non-payment that followed these dubious web shops and that ultimately was an additional reason why they decided to no longer service these parties (IN5).

It was also mentioned that the complaints and disputes provided the company with a lot of issues to handle, thus increasing the workload (*threat of workload*). Not only the customer service complained that the workload as a result of the complaints was disproportionate. The legal and sales team also stated that the web shops just provided them with a lot more work in the form of complaints and disputes than normal web shops do. Even more so with the foresight of more labels joining this would only increase. In addition, one employee said that after the investigation he wanted to prevent a similar

event from happening because it would take a whole month for the organization to assist with the investigation again (IN1).

Finally the *threat of regulatory interference* was not always apparent throughout interviews but is also inferred from the directors' decision to launch a compliance investigation before the investigation by the authorities started. Whereas one interviewee stated that legal concerns were first investigated and afterwards the morality of the matter (IN1). In the other case of smartshops the decision was made to not let any smartshops onto the platform due to the low paying consumer segment (*payment percentage*), but also due to the *regulatory ambiguity* they operated in. As the quote below highlights, the threat of regulatory interference was high if they crossed the boundaries of what was legal.

> *"With those smartshops you can do […], are you a little familiar with that Opium Act and the like? So you can sell certain quantities and also buy them. But you have certain [maximum] quantities of each, and well, when a web shop would do all of that in a single package, they are already in violation. But that is practically impossible to verify. Reason two is: if you offer a hundred products that are on the opium list and two that are not. Then that web shop is in violation. But we don't all have that expertise. […] But in principle it is not up to us to check, do the products of such a shop comply? Does it meet what we want or the law? That should not be our job at all."* (IN4)

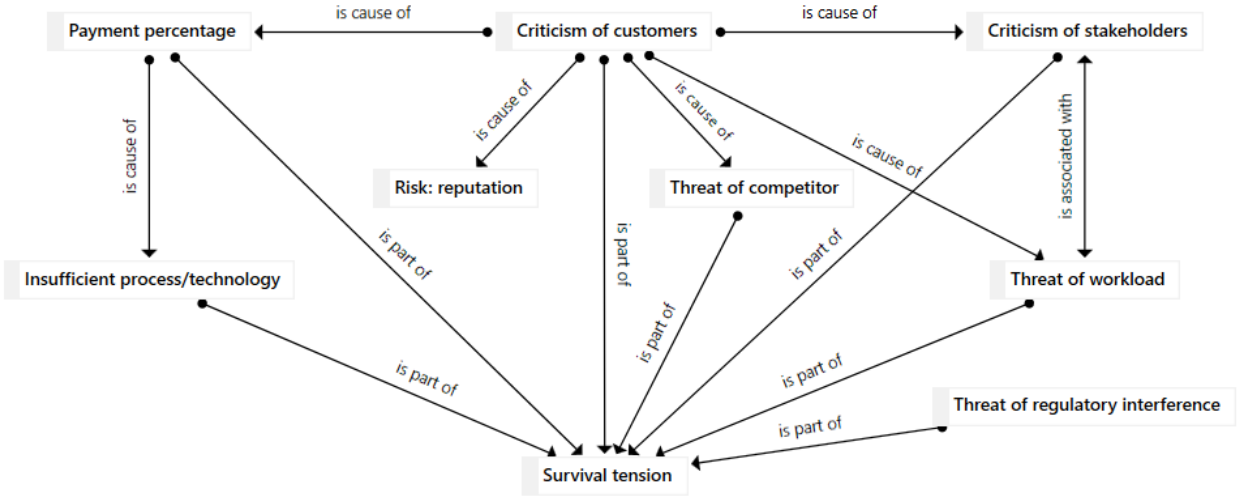

Figure 11 Survival tensions due to other risks

Learning tensions

Conceptually the aforementioned factors can be interpreted as survival tension, threatening the current way of working. Nonetheless, there were also factors which inhibited change (i.e. resistance) or more conceptually known as learning tensions.

In interviews, there were several factors identified that inhibited change in the organization. One of these factors, was primarily related to the *norms and values* of the organization. Secondly, *financial benefits* also played a role. Thirdly, the *receptivity of feedback* of people and fourthly the current *existing routines/processes* of the organization were referred to as hindering the decision to change existing practices. Conceptually these factors can be identified as learning tensions.

The norms and values of the individuals and the organization hindered the transition from occurring right away. Aforementioned quote already illustrates the value partly. Namely, some in the organization felt like it was not the duty of PayNow to 'police' web shops on how they did their business. Moreover, this also ties into the a concept or relation referred to by various interviews namely, the relation between the organization's maturity and their *duty of care* or *responsibility* beyond PayNow.

Here a distinction is made between responsibility and duty of care. Whereas responsibility is an activity obligated by norms or expectations. Accordingly duty of care is an activity that is carried out by an entity due to their own values that they should. This is akin to the difference between extrinsic and intrinsic motivation. Hence indicating that the feeling of responsibility of duty of care can either hinder or allow change.

For example some interviewees raised that it was not their job nor PayNow's responsibility to ensure that web shops did everything correctly besides keeping to the law and regulation applicable. Yet other interviews felt it was their responsibility in the chain/network to take charge in topics such as ensuring consumer trust. These two concepts are illustrated with below quotes.

> *"I think we have become increasingly aware of the fact that consumer confidence should be one of our main spearheads. And that we must also play an important role in this. And that we must also add value there on both sides. Yes, and that's a bit more than we might have thought beforehand. That our responsibility is a bit wider or bigger, that is if you take it [the responsibility], at least. Then your responsibility can be bigger than just a serving hatch"* (IN11)

> *"In the beginning we were very much like: okay you know, you have a company, you just fall under Dutch law and regulations, if the Dutch law and regulator have not yet reprimanded you, who are we to do that? In principle, if you have a business and you comply with the laws and regulations of the Netherlands that apply here. Then it is okay. That was the approach for a long time."* (IN2)

However, there was also a second tension namely the *financial benefits* the parties brought in. Restricting openness meant less possible users, hence less revenue coming in. On the other hand there is also a nuance mentioned in other interviews. Namely, the *organizational maturity* and the relationship between the *profitability of the platform*. As an organization grows, it can be inferred that an organization has more freedom of choice. It was reported that the web shops were difficult to let go at that time. Yet at a certain point they reached a maturity and subsequently were profitable enough for this to no longer be a problem. This is illustrated with below quote.

> *"There were always supporters and opponents within the company of whether or not to do business with such parties. Anyway, in the beginning they just brought in so much sales so it was hard to say: okay now we give up. But at some point we came to a point where we said: wait a minute we can do fine without them. Even then, we are very healthy as a company. So do we want this?."* (IN2)

An alternative explanation is that start-ups take whatever clients they can get and only account for their own risks (i.e. internal risks) whereas a larger organization feels more responsible for risks of the network (i.e. external risks). From a different perspective it can also be argued that a larger organization has the luxury of being selective in which suppliers may enter the platform.

Thirdly, related to the norms and values of the organization there were also departments and individuals that did not agree that companies should be ousted from the platform back in 2018 (*receptivity of feedback*). Whereas the sales department said that that they brought in money and it was not their job to care about what they did as long as it was legal. In another case, one of the directors did not immediately agree with letting the dubious web shops go, citing the relationship (*social dynamics*) that was built over the years with this client. Hence, they should first be confronted with their behavior and given the option to amend their behavior (IN1). This highlights that the receptivity of feedback from some decision-maker was possibly lowered due to existing relationships and that financial benefits definitely played a role in considering restricting openness.

Finally, existing routines and processes could have hindered learning. Only the finance manager provided an alternative explanation for why the dubious web shops were let go in 2018. Namely because of the fact that non-payment and fraud was before 2018 a problem of InsureYou.

> *"I also said once then, [that it was] not our problem, but an InsureYou problem. Because it was just like that then. So yes, because we started doing that business ourselves, we had to look very differently at the way we bring in customers"* (IN5)

In another interview it was said that this party even decided upon the acceptation of users onto the platform (IN2). Hence, when PayNow had to do their own acceptation of users and did not have insurance for the risk anymore, they were confronted with the customers accepted previously by a third-party.

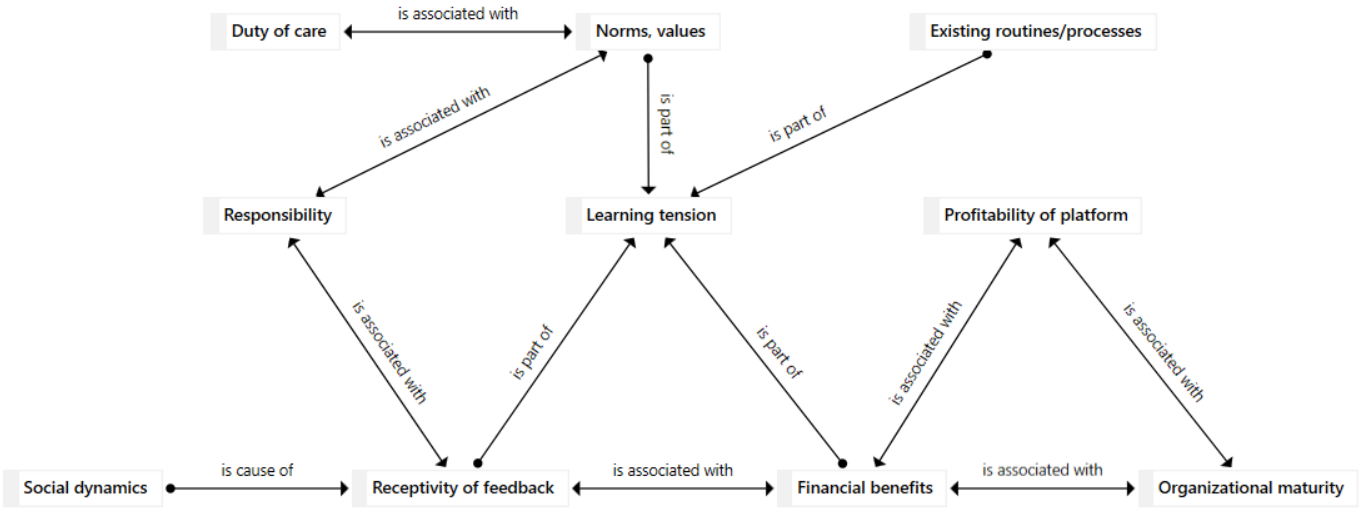

Figure 12 Learning tensions due to other risks

4.1.4 Background theories

In the beginning of the organization the norm and strategy of the organization was characterized as a broad acceptance policy. One interviewee referred to it as long as what they were doing was legal then a party was accepted. In addition, another interviewee said that parties were also evaluated based on *common sense* besides law and regulation (IN2). Common sense was characterized as the feeling that a

party is ‘wrong’ (IN2). Hence, beyond legality, supplier openness was limited to parties that did not conflict with the then-relevant values (*Theories-in-use: organizational value*) of PayNow. However, sometimes it was the case that certain parties adopted consumer unfriendly practices later on. One such example is parties using a return address in a far-away foreign country. When PayNow learned about that via complaints of consumers, they adjusted their norm that all web shops should hold a Dutch return address. Reason given was that PayNow was originally started to protect the consumer is that policy is not coherent with that mantra (IN10). Hence, a change in norms (*Theories-in-use: norm*) was observed. Similarly other incidents also caused changes in the terms of agreement (*Espoused theory*) at PayNow limiting their supplier openness. It can be noted that these changes were primarily made to protect the consumer.

In the case of the dubious web shops, this resulted in PayNow adjusting their norm into no longer accepting all parties that were deemed okay from a legal perspective. Even more so a change in values (*Theories-in-use: value*) can be noted in one interviewee stating:

> *“Anyway, it was more an ethical issue. Such a web shop that is […] that is not the way you should do business. And if we are like you as a web shop does not do business in the way we would, in which we would find it responsible. Yes, why should we want to do business with you?”* (IN2)

The above statement underlines an important distinction in the difference between individual and organizational background theories. Whereas, seemingly some interviewees background theories followed after investigating the parties. In contrast, the organizational background theories seemed to only have been changed after openness was adjusted. What can also be denoted here is that previously PayNow was of the opinion that it was not their place nor responsibility to tell other business how they should run their business and this eventually changed (*Theories-in-use: organizational belief*).

> *“In the beginning we were very much like: okay you know, you have a company, you just fall under Dutch law and regulations, if the Dutch law and regulator have not yet reprimanded you, who are we to do that? In principle, if you have a business and you comply with the laws and regulations of the Netherlands that apply here. Then it is okay. That was the approach for a long time. […] When no products are delivered, there is of course something else going on. Then it's just fraud. In this case, it was not fraud, but at one point it was headed for deception. But when is something a deception? And then comes the ethical aspect. And at some point that fortunately rose in importance”* (IN2)

As stated before this change did not happen overnight. Instead PayNow reached out to the parties multiple times asking them to correct their ways (*Negotiating*). Essentially before the decision was made to limit their supplier openness, they already confronted the parties with their behaviour. As mentioned before, each time they promised solutions, but they never followed up on their actual way of doing business. Hence, PayNow felt necessitated into letting the parties go.

Although PayNow undertook action the moment they learned of the misleading, it was noted in some interviews that the decision was difficult due to the revenue the web shops generated. In other interviews it was even noted that in the earlier stages of the organization it would have even been more difficult to let go due to importance of steady revenue in the early stages of the organization (IN2). This may suggest a relation between organizational maturity and the perceived or target legitimacy of the organization.

In addition, after the decision was made to let the web shops go, various interviewees raised the issue that they brought poorly paying customers to the platform anyway. Hence, indicating a change in assumptions (*Theories-in-use: results/assumption*) and beliefs (*Theories-in-use: belief)* about these type of parties. Even more so when getting rid of the parties was likened to getting better clients, indicating a change in strategy (*Theories-in-use: strategy*) (IN1). This can be seen in other statements of interviewees denoting the need for a broad acceptance policy in the beginning to get enough web shops on the platform. Moreover, suggesting that they were viewed as good for the profitability of the organization then, and after finding out about the business practices much less so.

A similar dynamic can be observed in the face of a threat to regulatory legitimacy due to smartshops. Before the incident a finding in the due diligence of a partner organization resulted in PayNow spotting the regulatory threat posed by a certain web shops. Hence, the decision was made to no longer run the risk of such issues with the law and supplier openness was restricted to no longer accept smartshops. Later in the interviewee said that the consumer segment attracted to that kind of web shops were dubious themselves too. As was expressed in the amount of people that actually pay.

It can be observed here that first a regulatory threat occurs and PayNow acts on it. Following the threat, existing norms are questioned. Then finally, assumptions about these parties also change as is illustrated by the quote below.

> *"We just notice that this type of product attracts a group of customers who simply pay worse than average and we don't want that."* (IN4)

Even more so, after the dubious web shops of 2018 got removed from the platform and openness was subsequently adjusted, a change in strategy can also be observed. Instead of accepting a lot of web shops to grow, the strategy of the platform can be characterized as accepting good clients in order to grow. In order to get better web shops, the image of the organization itself should also be in line with these web shops (IN2). Hence, denoting a change in strategy.

Yet, how were the values and beliefs of the organization changed over time? The beliefs and values seem to have changed if the view on responsibility of the firm is taken into account. As stated before, the company did not feel responsible for policing the behaviour of web shops. Over time, as illustrated with the dubious web shops this responsibility or duty of care started to widen.

> *"When we have said this we do not want anymore. We want all web shops that do business with us to meet a number of conditions. And those parties that did not comply, and also had a chance to comply. Did not then put all the effort there. And then we said goodbye."* (IN2)

In an earlier mentioned quote, a customer service employee requested changing the contract with these parties before the events transpired. Hence suggesting a difference between individual background theories of some employees and the collective background theory. Whereas, it took more time for the background theories of the firm to change. One reason might be resistance to change and also the survival tensions present. From this observation two findings can be denoted. Firstly, the agents of learning do not necessarily represent the overall background theories of the firm. Secondly, it could be suggested that the *individual* background theories differed from the organizational or general background theory held. Subsequently it was this difference that resulted in survival tensions such as

criticism of stakeholders. Therefore, it can be suggested that differing background theories might also be a source of change (i.e. survival tensions) in an organization.

In addition after the incident of the web shop, the investigation also affected the responsibility of the organization. As the authorities told PayNow, that they should look even further than law and regulation and suspend any activities with web shops show bad signs such as non-paying clients. As PayNow was under the belief that they didn't have an obligation to keep web shops to certain norms and values. The investigators told them otherwise:

> *"In this conversation you say that you have no responsibilities there, but we do see a certain duty of care for you. That if a web shop gives a sign of non-compliance, so to speak, or trouble in normal Dutch. Then in principle you must suspend your work until that web shop can convincingly argue that they comply with the law and that there is nothing wrong"* (IN1)

This conversation marks a change in how impact to regulatory legitimacy caused a change in the organizational beliefs.

> *"That [conversation] had quite an impact on our due diligence procedure and our compliance procedure, we have become a lot stricter. Despite the fact that we were already strict about those rotten apples for which [confidential] came by. We have indeed taken the safety policy for consumer rights a lot more seriously afterwards."* (IN1)

Despite this conversation, it was also noted that the due diligence was already strong before that investigation. This also coincides with earlier interviewees stating that they first relied upon any web shops joining the platform and due to their maturity gained a feeling of responsibility in making sure that web shops uphold consumer rights. It can be suggested that perceived or targeted moral and regulatory legitimacy is affected by the maturity of an organization.

> *"We just service the customer of the web shop. And the moment that a web shop makes a mess of it, we are indirectly stuck with the baked pears. That is not desirable A, because it just generated a lot of hassle, and B for your good name it is of course just bad. At some point [...] we ourselves had grown to such an extent that we no longer needed these types of lowly web shops"* (IN4)

Whereas above quote suggests that the type of customers is related to the stage of an organization's maturity. In another interview , a reference to the concept of generativity being the reason for some of the risks was made by the CEO of the platform and is illustrated by the quote below.

> *"Well in the beginning, you might assume clients to be more well intentioned. But do you try to take that into account? […] The people who also want to take advantage of [the platform] do so because the possibility is there. Do you understand what I mean? It didn't exist yet to try to disadvantage consumers that way [misleading], but what can happen is that - because they can pay [confidential] they suddenly come up with scenarios that we didn't think of before. And that is what you find out over time. And you just adjust your process accordingly."* (IN11)

4.1.5 Openness changes over time

Upon learning about certain risks over time PayNow's openness also changed over time. These changes are outlined below in response to some of the risks mentioned in the previous sections.

Supplier level

By far the most changes over time happened at the supplier level (*Platform openness: supplier*). Whereas suppliers, or supply-side users of the platform, are referred to as web shops.

PayNow controlled supplier in various ways in response to certain incidents or risks. For example, before the dubious web shops were ousted from the platform, they had to pay a higher price per transaction than any other web shop (IN2). Following the decision of PayNow to oust the web shops in 2018, a due diligence process was set up to keep out any 'louche shops'. This decision was made in order to prevent taking on new parties that misled consumers and prevent trouble. Later on when the authorities had investigated PayNow there were changes made to the due diligence procedure. These changes resulted in an even stricter process according to some interviews (IN1; IN2). Unfortunately due to the relatively long time ago these events happened, not all respondents could remember the exact changes made due to the investigation. Instead, via document analysis the first version of the due diligence process before the investigation and after the investigation could be compared.

This analysis showed that before the investigation the due diligence evaluated whether the merchant complied with PayNow's terms of service, such as providing the correct information to the consumers and establishing a purchase correctly. Furthermore, the compliance check was performed by sales and after the moment a merchant signed the contract. The due diligence after the investigation introduced that the customer service instead of sales onboards a new client to prevent conflicts of interest. In addition, the compliance check is performed before a new merchant is signed and a checklist is introduced. This checklist collects evidence of the website and whether the web shop is correctly listed at the Chamber of Commerce with no incongruencies. In addition to also verifying that for example a web shop was reachable for customers a set amount of time each day and also does not hide extra costs for consumers among other limitations.

Another example is caused by fraud and limits web shops that sell high value products. An example was given in some interviews of a web shop that sold high quality hair salon clippers. Apparently, because of the resell-value of the product, this type of item was highly fraud sensitive and as a result PayNow does not offer these type of web shops anymore (IN7; IN9). Similarly web shops that sell refurbished iPhone's are denied joining the platform based on similar experiences in the past. In the same vein, recently a web shop was denied based on the products they carried giving rise to ethical issues. More specifically, this web shop sold WWII replicas of a certain party.

Finally, the decision to prohibit new smartshops from joining the platform was also made in light of the risk that illegal products can be sold. Moreover, interviews stated that also the consumer segment that is reached is a poorly performing one. Hence, indicating a link between a regulatory threat and a financial incentive to limit the supplier openness. An alternative explanation is that third-parties such as DutchFinance (*Third-party supplier openness*) and CollectPay both either do not or almost never accept smartshops. On account of their role in the value chain of PayNow, they cannot accept new smartshops due to not being able to pay them via the DutchFinance platform or collect late fees via CollectPay.

User level

On the user level fraud risks largely affected which users could join the platform. Web shops that sold highly valuable products such as electronics automatically received stricter requirements for user in the credit check (IN5). PayNow used two tools to limit user openness for fraud sensitive web shops. The first tool was lowering the maximum possible order amount a user could order via fraud sensitive web shops. The second tool was increasing the acceptance criteria for the users ordering at the web shop via PayNow.

> *"When we see these are products that are susceptible to fraud, we will perhaps make that [credit] check a bit stricter, so to say. [...] the goal is in any case [...] the customers of this web shop must meet slightly more criteria. Imagine that we score them from 1 to 10. Instead of a six, a user should have an eight at this web shop. So then we can tweak the criteria a bit, on who can place an [...] order at that web shop"* (IN5)

According to the interviewee the reason why this was done, was to not only limit the financial risk of fraud, but also maybe make the platform more commercially attractive by having less fraud (i.e. a unique selling point) (IN5; IN7). Finally a similar third-party dynamic was also observed with InsureYou when they still controlled user acceptance (*Third-party user openness*).

4.2 How does PayNow adjust openness due to privacy risks

In interviews it was observed that privacy was primarily anticipated on and not so much reacted to. In contrast to the previous chapter, privacy was often thought of before impact or threats materialized.

Context

PayNow garners a lot of data from its users. Not beyond what is necessary for processing, but due to the amount of users on the platform. As with every payment service, there is a chance of certain parties to try and abuse the system by defrauding it. In order to manage this risk, PayNow developed a fraud detection system. For one of their fraud detection tools PayNow utilizes external parties to validate that data entered by a consumer exists and it is correctly entered. If new users (consumers) aren't recognized then they might be scored as a higher risk by the system and might be denied entry to the platform. On the other hand, if a user is recognized in multiple databases, then a user has higher chance of being accepted by the system. Whereas these database contain the personal data of users they submitted earlier to the data validation services. Fundamentally when developing this tool it would seem that the more databases are connected, the more users can be validated. Yet, PayNow did not necessarily opt for this. Instead, the IT manager, when he developed the system, only chose parties that allowed for data to be used for validation purposes only (IN2). Hence, avoiding that data about people would end up being used to enrich certain already large databases of personal data. This decision ultimately led PayNow to utilize only a select few providers as their partner.

Nonetheless, when PayNow chose to use the validation service there was an option to also allow the providers to save some part of the data, in order to keep their validation service alive. Consequently, also allowing for lower usage fees of the service for PayNow (*Data as a commodity*). PayNow opted for this decision, while not allowing data to be enriched any further. This event describes how PayNow anticipates on privacy risks.

Another event illustrates the decision-making of PayNow around a newly identified privacy risk. Once a web shops customer contacted the service desk and told the customer service employee that he

couldn't find his most recent bills for customers. Instead, he could see the bills of other web shops. Thus raising a potential data leakage. PayNow reported this to the relevant authorities and made sure no one else could see the same data and the issue was fixed. Although this did not result in any changes in to platform openness it might suggest that the incident had an effect on perceived legitimacy.

4.2.1 Learning about privacy risks

How does the organization learn about privacy risks (*Risk: privacy*)? According to the interviews, there were two methods the first one being the consumer or customer (web shops) complaining or asking a question about the method of how the organization used their data. The other method was the employees of PayNow asking 'can this data (use) hurt the consumer in any way?' (IN2). This is indicative of employees using their own beliefs (i.e. *common sense*) of what a privacy risk is to identify them. Using these methods privacy aware (*Privacy awareness*) consumers already made PayNow aware of how they handle their data before the GDPR came into force. This can be illustrated by the fact that PayNow does not process more data (*Usage of personal data*) than that they already did before the GDPR as is illustrated by the respective privacy statement from 2014 and a more recent one of 2020.

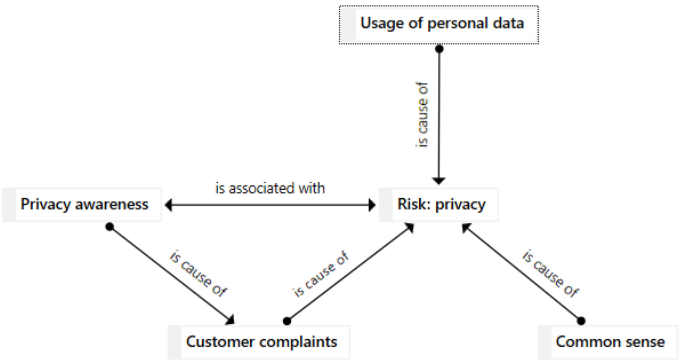

Figure 13 Network diagram privacy risk

4.2.2 Moral and regulatory legitimacy

Based on interviews moral legitimacy primarily seemed to have shaped decision making around privacy. As one interviewee said actual processes have not changed business that much, specifically openness has not changed due to the GDPR. Moreover, one interviewee referred to the GDPR as:

> *"I really think it's really for a lot of companies - it's like building a shield on the roof of my house before an airplane crashes you see? It will never happen. Of course this is very exaggerated."* (IN4)

Hence it primarily seemed to be observed as a paper burden instead of leading to change. Although the actual effect of the GDPR of the company might be minimal, besides new processes and policy. It was noted in several interviews that the attention toward the GDPR caused many to become more aware of privacy (*Privacy awareness*) in itself, even before the GDPR was enforced. The legal officer said the following on how the GDPR affected PayNow:

> *"Of course, we had certain plans about how we wanted that credit check if we could market that credit check in the business sphere. And indeed the introduction of the GDPR, despite the fact that the rules have not changed very much, has made us more aware of our duties and tradability of personal data"* (IN1)

Whereas the IT manager reaffirmed this with the following quote.

> *"We always collected everything [data] we needed and not much more than that. Practically no adjustments have been made to this in recent years. That [GDPR] has had no impact. It did have an impact on our internal processes and also on our employees, particularly in raising awareness."* (IN2)

Hence indicating that not necessarily out of regulatory threat certain decision were made, but possibly rather out of a perceived gap between actual and target moral legitimacy of the organization. One interviewee (IN10) indicated that before the GDPR PayNow already employed a person with a legal background to look at privacy issues. In addition, he suggested that while privacy might not have been the highest priority in the beginning of the organization, this changed as society itself became more aware and started asking questions (*Customer complaints*) on how data was used in the organization. Finally, from a regulatory legitimacy perspective it could be argued that the attention brought to privacy can also be attributed to the GDPR as is illustrated by the quotes of IN1 and IN2. Whereas the GDPR enforcement might have posed a threat to regulatory legitimacy and presumably made the organization more aware of their duties and how they could handle data (*Usage of personal data*).

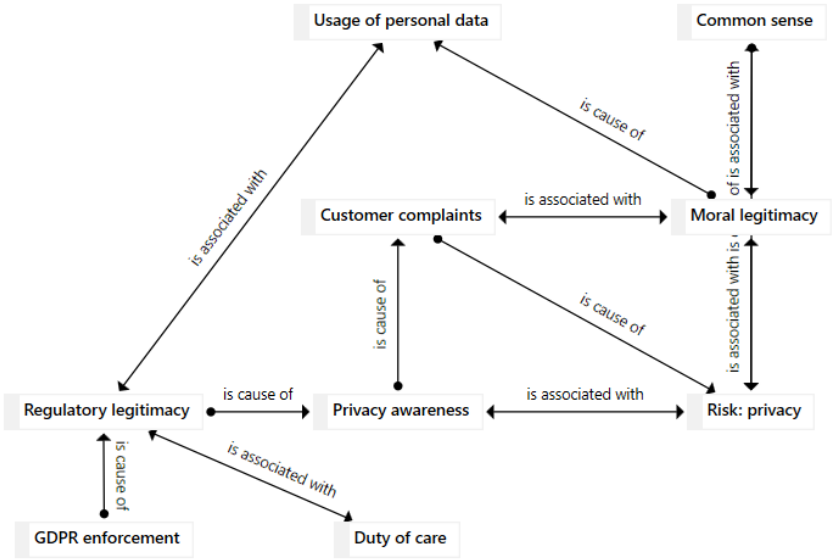

Figure 14 Network diagram threat to legitimacy due to privacy risk

4.2.3 Survival and learning tensions

Are learning and survival tensions separately applicable if a risk is anticipated on? While there might not be a specific tipping point found that triggered changed, there were both motivators and inhibitors of change found upon identifying a privacy risk. The primary survival tension observed in privacy matters was *criticism of consumers* or at least the threat thereof. Whereas consumers asked questions about how their data is handled (IN10) ultimately affecting how personal data was handled from an early stage (*Usage of personal data*). Moreover, when the data leak happened the survival tension could be referred to as the *threat of regulatory interference*. Although it was deemed by the legal officer, as not legally necessary to report, PayNow made a report to the authority anyway.

> *"We did eventually report it at the time. Also because we thought it was good to have made a report to the AP [Dutch Authority of Personal data] once. Because if you process a lot of data and you never report something to the AP, then that is ultimately also very suspicious."* (IN2)

This quote highlights that it was not necessarily law or regulatory pressure that motivated the decision to report the incident, but instead, it could be suggested to be a form of expectancy. Whereas having no incidents could maybe establish a more incongruent regulatory legitimacy. More specifically, the organization has a certain view of the regulatory legitimacy regulators expect to see. In addition, one interview with the CTO also raised another element, namely *self-improvement* or the striving for self-improvement in other words. This is illustrated by the following quote on how privacy is upheld in the organization:

> *"It is a bit of a balance between the size of your company and […] what actually is the level [of privacy controls] you want to pursue, because according to the law it is all allowed, we could still do it the same way as a start-up. But you also just want to get better. And privacy is simply a difficult thing that cannot be captured in numbers, you do it well or you do it incorrectly. But on the other hand, there are so many things involved, and every time you try to do better with your company. The same thing with finance, every year you just want to step up because - just more is expected from indeed your customer group and the people. Because you just get bigger."* (IN10)

Thus it could be said that there is some form of intrinsic motivation at the decision-making level which is affected by the size of the company and expectations of the customer (linked to the threat of *criticism of customers*). By extend this self-improvement might also have something to do by the values upkept by the organization.

One learning tension can be inferred from the decision making around which data validation service were chosen. Although PayNow's values on privacy do seem to be largely congruent with that of public values and norms on privacy, the decision to let data validation service keep data that they validate in turn for a lower transaction fee highlights a flipside (*Data as a commodity*). Subsequently, it can be suggested that *financial benefits* might have influenced the decision-making in this case.

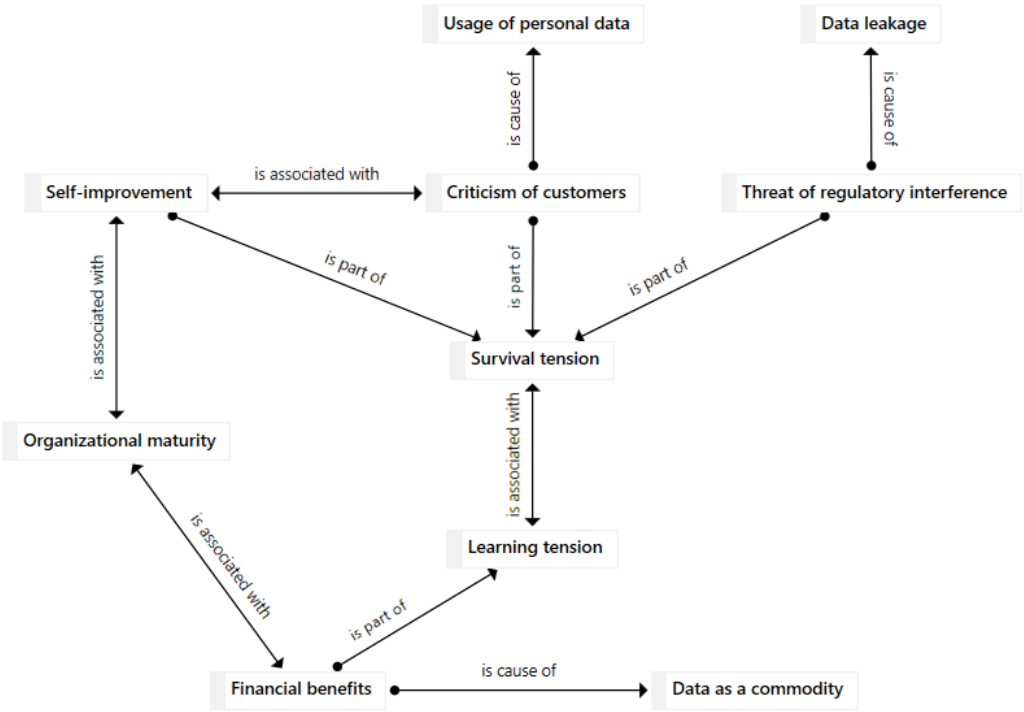

Figure 15 Network diagram survival and learning tensions due to privacy risk

4.2.4 Background theories

Can it be stated that there was an observable change in background theories according to perceived privacy risks? Background theories might not be directly observable, but their consequences might be. In terms of norms (*Theories-in-use: norm*) of the organization, it can be seen that privacy is taken seriously. As is seen in documents received form PayNow. In a comparison of the privacy statement (*Espoused theory*) from the company that was originally made in 2014 and compared to a recent privacy statement from February 2020 it can be seen that the original goals and processing activities performed upon personal data have not changed much or at all. Except for the fact that the use of tracking pixels is now reflected in the document (IN1). Consequently, this coincides with statements made by the IT and privacy officer earlier that there is no significant change other than in the espoused theories and awareness of the organization. Hence suggesting that the questions from consumers already added to the privacy awareness of the organization. Furthermore, this change in privacy as value is described by the following quote from the CTO:

> *"Yes, I think one was the realization that people did not realize how much was possible and the second was also the social pressure. That people actually started asking us about: what about my privacy data? And that actually makes you think: are we actually doing it the right way? So actually our success has also been that people reported to us more consciously about privacy and that as a company you also start to think and learn better. I always say a start-up should focus at the beginning - or well, it focuses on the things that matter at the time. And privacy was not the most important topic at the start of the company."* (IN10)

"[Did this happen before the GDPR?]
Yes, yes that happened before [the GDPR] and I think in the third or fourth year [2013/2014] that has slowly become more important. Then we also got the first people who reported to customer service. And asked from us: what data do you actually have? So how does such a credit check work? And how do you actually do that, how do you analyse me? And then we actually thought for the first time, yes what is our role in this?" (IN10)

This infers that the *Theories-in-use: organizational value* was affected by these questions and rose in importance. Furthermore, also leading to questioning what the role of the organization (*Duty of care*) was in dealing with privacy sensitive data.

4.2.5 Openness changes over time

As mentioned the risk of privacy had a relatively minimal impact on openness. This can in part be explained by the anticipatory response to privacy risks by PayNow. This is illustrated by the decision on including only a few data validation providers for PayNow's credit check. Hence, openness did not change significantly due to privacy risks after the launch of the platform. Conversely, previous risks resulted in changes to existing policy and by extend sometimes also openness.

Provider openness
The provider openness (*Platform openness: provider*) of PayNow in terms of data sharing was limited to parties that allowed for data security and privacy requirements to be met (IN2). In essence it could be argued that allowing more data validation services could only benefit the user acceptance of the credit check. Hence, there seems to be a trade off in foregoing additional users in order to uphold privacy to a certain degree. If PayNow opted for more data validators then a user has a higher chance of appearing in existing databases and thus has a higher chance of being accepted. Consequently, more databases equal a larger potential market. Nonetheless, PayNow opted to only use a select few data validators.

An additional impact from privacy could be PayNow requiring their privacy statement to be embedded in every web shops. However, this research does not view this as an impact to openness as the GDPR is applicable to all processors of personal data. Thus it is applicable for all web shops to have privacy statements and does not limit the amount of potential customers of the platform.

4.3 Comparison conceptual model and empirical findings

This chapter concludes the findings by comparing the original conceptual model with the findings. Starting with the earlier shown conceptual model, new findings and nuances are discussed which essentially form the basis for the new empirically enhanced model.

Conceptual model
This research started by formulating what available theories could explain how platforms adjusted openness upon learning about certain risks. Based on the empirical findings it can be seen that not every connection is as nuanced as found in the findings. However, social interactions are often in practice more complex than preliminary models convey. This paragraph provides an empirically enhanced model. In order to arrive at an abstracted model again, certain details are aggregated. What details are aggregated into separate variables in the model are explained below.

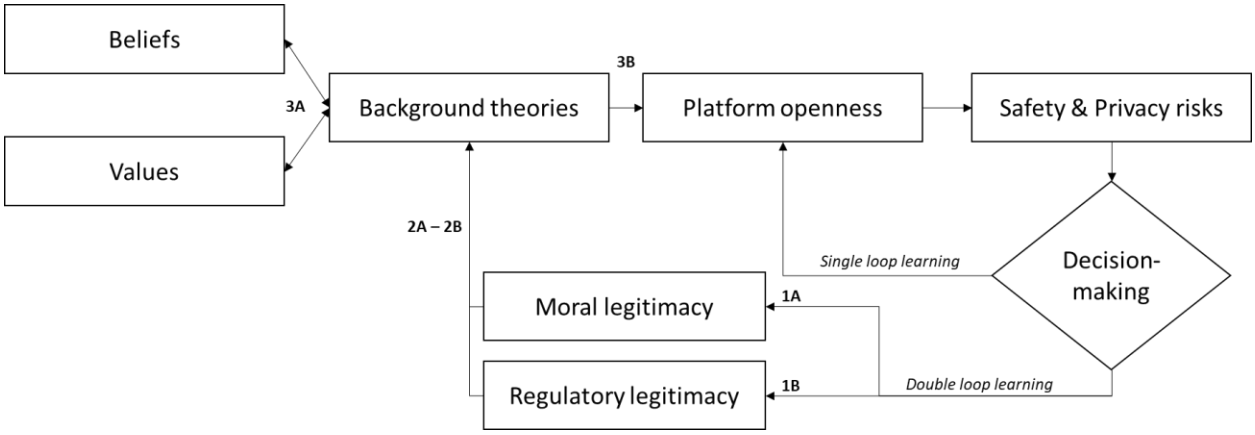

Figure 3 Initial conceptual model

Risks and identification

As was mentioned earlier. Safety risks were not necessarily a motivating factor in this case, instead other external risks such as misleading/unfair trade practices and fraud were more dominantly found in the case. Risks that affected societal values impact the legitimacy of the platform and subsequently the openness of the platform. Yet, it was also found that other risks such as fraud also have an impact on platform openness. Furthermore, it can be suggested that the responsibility of risk also affects how risks affect platform openness at all. In the conceptual model an agent is responsible for identifying risks.

Nonetheless, it was found in the case that this mechanism of risk identification is not as straightforward as portrayed in the conceptual model. Instead, the mechanism of risk identification seems to primarily function on signals or threats to legitimacy from actors. Based on these signals, a risk can be identified. Subsequently, the risk can be anticipated on. Individual recognizability of risks also affects this. This can be with risks such as privacy garnering much more attention of the years compared to the risk of misleading websites. Hence it could be stated that the ability to identify risks is affected by earlier incidents and identification. Whereas, this also affects how risks are treated and which risks are perceived as a threat to legitimacy.

Moral and regulatory legitimacy

Moral and regulatory legitimacy seemed affected by risks that affect public values. Yet, as mentioned it is also this mechanism that helps identify risks. As stated in literature, if legitimacy is harmed then an organization may experience issues in its continuity (See Suchman, 1995). Based on the findings it was found that reputation issues and non-compliance can hurt the profitability of a platform. Hence, it was found that profitability related more than once to the legitimacy of the platform. Moreover, another mechanism discovered in the case was the relationship between organizational maturity and legitimacy. This suggests that the legitimacy of a start-up maybe different from that of a mature organization. Hence, some risks that threaten legitimacy, can affect a start-up differently compared to a more mature organization.

Survival and learning tensions

Survival and learning tensions were encountered as was defined in theory. Yet, two new factors such as learning tensions from financial benefits and social dynamics within the organization were also found in

the case. Specifically, the social dynamics refer to social relationships between individuals in the organization which altered the receptivity of feedback from a decision-maker in the organization for one decision regarding openness. Furthermore, the effect of financial benefits proved to be an influencing factor in the decision whether limit openness of the platform. It could be stated that these survival tensions are also interdependent again on the profitability of the organization. Whereas some people in the case referred to the financial impact of openness decision as more severe in the early stages of the organization (i.e. start-up phase). Although survival tensions were not shown in the conceptual model, they were of significant explanatory value in this case. Consequently, they are included in the empirically revised model.

Background theories

There can be changes observed in the norms, strategies and assumptions of the organization that lead to certain changes in the platform openness. In addition, interviews suggested that societal risks led to both changed organizational and individual background theories. Furthermore, the responsibility and more specifically the duty of care of the organization can be observed to have changed as a result of some risks over the years. Regardless, findings also suggest that organizational maturity might affect responsibility. Various interviews suggested that organizational values changed and ultimately resulted in a changed responsibility. Besides values, beliefs and theories-in-use of the organization also show changes over time. Specifically, changed norms, strategies and assumptions led to restrictions in openness in various events throughout the case.

Based upon the findings a revised model was made. The picture below highlights the empirically enriched conceptual model. Whereas, the greyed out variables are newly added to the picture. Nonetheless, in order to test the propositions the findings and propositions (i.e. patterns) must be evaluated. Hence, the next chapter will test the validity of the propositions and if relevant provide alternative explanations.

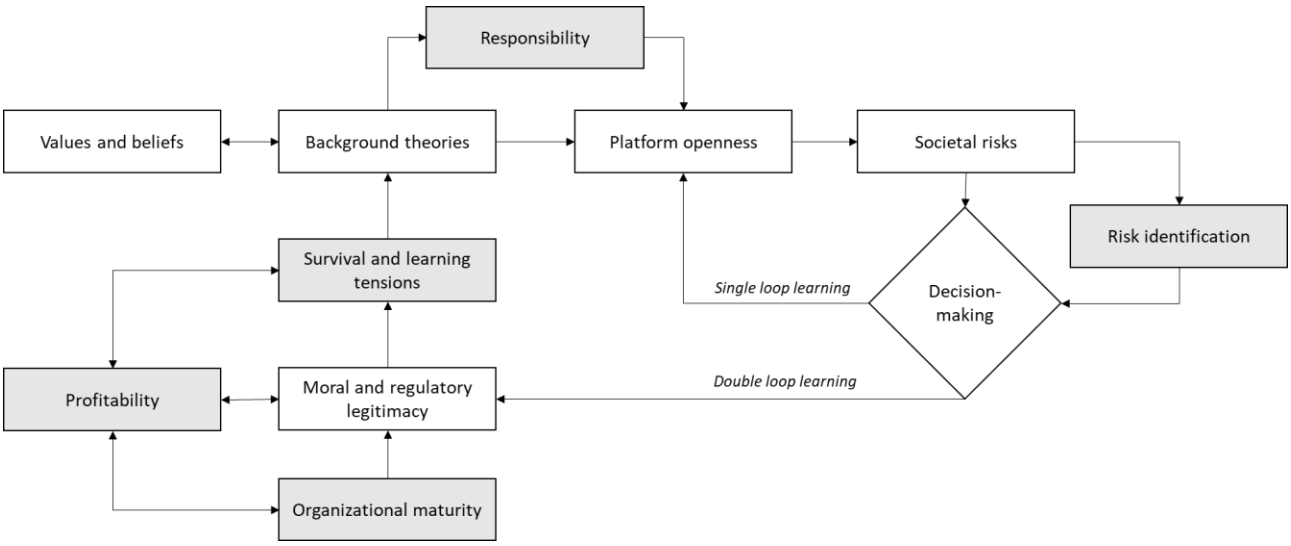

Figure 16 Empirically enriched conceptual model

5. Analysis of results

This chapter describes the findings alongside the propositions outlined in section 2.4.1. Following the pattern matching method of Yin (2018) the propositions hypothesized several patterns from theory on the phenomena of how openness would be adjusted upon learning about risks according to theory. Specifically, this chapter will explain the reasoning and assessment on what propositions seem true based on empirical findings. Accordingly, this chapter answers the fourth research question.

5.1 Assessment of propositions

In order to confirm or contest the proposed patterns, the empirically collected findings will be compared to the theoretically derived propositions (i.e. patterns) (Yin, 2018). This comparison requires an explanation of how a certain empirical event caused another event. The propositions suggest several causal connections to exist between theoretical concepts. Hence, in order to compare the empirical events with the propositions, an explanation of events is required. Furthermore as Gregor (2006, p. 617) states: "to ask for an explanation of an event is to ask for its cause". Yet, as Gregor argues, proving causality can be problematic. Especially in field research such as this case study where various contextual factors can affect causation. Nonetheless, there are several ways to reason about causality in research. Whereas often research uses regularity to derive universal laws or probability and finally even manipulation to prove event causation (Gregor, 2006; J. Kim, 1999). However, as is the case in this study, a case study does not always have the tools (data) to utilize such methods to argue about causality. Hence, leaving another form of reasoning about causality namely, counterfactual analysis (J. Kim, 1999).

Counterfactual analysis essentially utilizes the reasoning that if an event would not have occurred (contrary to fact) then the outcome would not have occurred either (Gregor, 2006). Thus causation can be inferred about the event being a necessary condition (i.e. cause) for the outcome. This analysis furthers the reasoning of causality than the if-then tests to test validity as suggested by Miles et al. (2014). For example if it is suggested that X causes Y then the counterfactual must also be valid. In other words, if X is not there or different then Y will not be observed or will be different.

Mahoney & Barrenechea (2019, p. 307), among other researchers, position counterfactual analysis "as an important tool of causal inference in small-N and case-study analysis" (See also Tetlock & Belkin, 1996). In their report, Mahoney & Barrenechea distinguish between four types of counterfactuals namely: necessary condition, SUIN condition, sufficient condition and INUS condition counterfactuals. Moreover, they argue that the first two of these types of counterfactuals are most useful in arguing on causality. This on account of the first two types suggest that a changed event can result in a changed outcome. Hence, being more useful in arguing on causality.

The first type of counterfactual is as the example provided earlier. If event X occurs then Y occurs. Goertz & Levy (2007) call this a necessary condition. Whereas a necessary condition counterfactual illustrates that a counterfactual absence of the antecedent (X) a different outcome (Y) occurs. Thus suggesting that the antecedent was necessary for the outcome. Mahoney & Barrenechea (2019) utilize the hypothesis of Moore (1966) that without bourgeoise there is no democracy. Hence, utilizing a counterfactual to position the bourgeoise as necessary for democracy to exist. Whereas the absence of a bourgeoise is then sufficient to lack a democracy. Assessing the validity of the counterfactual can provide support for inferring certain events as a necessary cause (Mahoney & Barrenechea, 2019).

The second type of counterfactual is a SUIN condition counterfactual. Whereas SUIN stands for "a sufficient but unnecessary part of a factor that is insufficient but necessary for an outcome" (Mahoney, 2008, p. 419). A SUIN cause is in itself insufficient to alter an outcome. This is best illustrated by the example of peace theory Mahoney (2008) uses to describe a SUIN condition. The theory states that nondemocracy is necessary for war. Moreover, Mahoney raises that conditions such as fraudulent elections and high levels of repression constitute nondemocracy. Therefore these conditions are SUIN causes of war (Mahoney, 2008). These conditions are neither necessary nor sufficient for war on themselves. However, the conditions do allow the outcome (of war) to occur.

Another example is provided by Seawright (2016). The outcome of a house fire requires the antecedent of an ignition to occur. Such ignition can occur by method of lighting a match. In itself the match is not sufficient for ignition as oxygen is also necessary. Furthermore, a match is also not necessary for ignition, as an electrical short can also cause ignition taken together with oxygen etc. (Seawright, 2016). Thus, lighting a match is a SUIN cause. A SUIN counterfactual lends itself not to reasoning about something being necessary. Instead, it provides a method to argue about how one specific changed antecedent (i.e. SUIN cause) might render a changed outcome (Mahoney & Barrenechea, 2019).

The two types of counterfactuals can prove useful in reasoning about the causality of events. Consequently, an understanding of the causality of events can support proving or disproving the outlined propositions. As will be done in the following chapters.

5.1.1 Pattern 1. Legitimacy theory

- Proposition 1A – A risk threatens or negatively affects the moral legitimacy of the platform sponsor.

As was mentioned in the findings chapter, one of the foremost findings was the fact that the decision making in the case was not primarily, or at all, motivated by safety risks. Even more so, evidence of privacy risks did not explain changes in openness over time significantly. Nonetheless, after the first few interviews it was observed that specifically other risks did seem to have an impact on decision making and by extend also platform openness. Therefore, the decision was made at the beginning of the data collection to broaden the scope of the proposition to include risks more broadly. This decision was made on account of the propositions still staying true to the original purpose of the research. Namely, how do societal values guide platform openness (See section 1.1 Problem definition). Moreover, the risks identified were almost all risks that threatened societal values. One such example is the risk of misleading consumers. This risk endangers the value of trust among other public values.

If the operationalization of Teixeira (2009) of a threat to moral legitimacy is used. Then impending or actualized negative assessment from key stakeholders negatively affects moral legitimacy. Furthermore, Scott (2001) defines moral legitimacy as the extent to which an organization adheres to the values of society. Besides these definitions, it is important to note that (moral) legitimacy does not necessarily convey what motivated an actor to protect legitimacy. For example protecting moral legitimacy might be a result of the values upkept by an organization. However, it might also be maintained in order to safeguard financial interests (i.e. continuity) (Suchman, 1995). Knowing this, the proposition can be assessed.

In the case of PayNow several risk such as web shops that misled consumers led to criticism from consumers and in some cases even from stakeholders such as CollectPay. More specifically, in the case it

was often referred to as damaging the reputation of the organization or posing a threat to the reputation. Yet does reputation convey moral legitimacy? The definition from the Cambridge Dictionary on reputation is: “the opinion that people in general have about someone or something […] based on past behaviour or character” (n.d.). Based on this definition this research defines reputation as reflecting perceived moral legitimacy of an organization. This relationship is defined as such because moral legitimacy also confers public opinion of an organization.

Consequently, if the risk of misleading consumers can harm, or already harmed, the organization reputation then it can be said that the risk did negatively affect moral legitimacy. Moreover, from several sources in the organization it was stated that employees, among one of them being the CEO, that when they learned of the practices they found them morally reprehensible and wanted them gone from the platform. Effectively questioning the morality of the practices.

Due to social desirability the truth of whether they actually found them morally reprehensible can be questioned. Regardless, if only taking into account the large amount of complaints received from consumers it can be said that moral legitimacy was negatively affected. According to the earlier mentioned operationalization of moral legitimacy this constitutes negative assessment of stakeholders.

Conversely, if the risk was not there, would the moral legitimacy not have been negatively affected? If the risk would not have been there, then the dubious web shops would not have misled organizations. Hence, leading to doing business in a morally right way. Furthermore, if the consumers would not feel misled then it could be argued that some of the complaints would disappear. Regardless it should be noted that a certain type of products seem to attract a certain type of consumers. Whereas, a certain type of consumers can also be more inclined to cause complaints. Finally, if dubious web shops did not adopt their way of doing business then there would also be no impact on reputation. Therefore, there seems to be some validity to the risk of misleading being a necessary condition for negatively affecting legitimacy.

Did privacy risks similarly affect the moral legitimacy of the organization? In a way it could be argued that the early questions from consumers on privacy raised the awareness of the organization on privacy. Subsequently, leading to questions in the organization on how privacy was managed. But there were no specific privacy risks in particular identified, hence it seemed as if the possibility of a privacy risk evaluated by consumer questioning the practices of the organization threatened the moral legitimacy of the organization. Nonetheless, when designing the credit check the platform did opt for a limited amount of data validation providers. Whereas this seemed to be trade-off where they waived the idea of a higher user acceptance rate in the face of privacy risks.

From a counterfactual perspective it could that if there was no privacy concerns then PayNow would have adopted more data validation providers. This seems valid on account of the sole reason provided for how PayNow selected data validation services being privacy risks for consumers. Yet, when arguing the counterfactual effect of consumer questions, issues with plausibility arise. Would customers have questioned the organization if consumers were not wary of privacy risks? Most likely not. Perhaps a more useful counterfactual in this case would be arguing for sufficiency. If the customers did not accept the way of data usage at PayNow then criticism seems plausible. In other words, if consumers would perceive a privacy risk at PayNow then a negative effect to moral legitimacy seems plausible.

- Proposition 1B – A risk threatens or negatively affects the regulatory legitimacy of the platform sponsor.

Did the risk of misleading consumers also affect regulatory legitimacy? From the perspective of the organization itself regulatory legitimacy is gained via compliance of applicable rules and regulations (Aldrich & Ruef, 2006). Furthermore, Zimmerman & Zeitz (2002) also operationalize regulatory legitimacy as the adherence to expectations set by governmental bodies.

Technically the web shops that misled had everything in order according to the Dutch law on purchasing online. Regardless these same web shops were investigated for unfair trade practices later on. By extend, PayNow also had to provide them with evidence of these web shops due to them being one of the payment methods used by the web shops. Yet, PayNow already outed these web shops before the investigation by authorities took place. Thus leading to question whether it was regulatory legitimacy that motivated the organization, or whether this type of legitimacy was affected at all. In interviews it was found that the investigation by authorities was unexpected. Yet, PayNow did launch a compliance investigation into these parties before letting them go. Hence, inferring that regulatory legitimacy was indeed threatened by these parties that seemed to mislead consumers. Based on the compliance investigation it was found that the parties were actually in violation of applicable regulation. Alternatively, if there would not be a risk of misleading consumers then there would be no threat of regulatory interference. Hence making it plausible that regulatory legitimacy was threatened.

Another case was found with the decision to halt smartshops from joining the platform. As stated before, there was a chance the illegal products were sold or illegal quantities could be sold via the platform. In addition, there were already smartshops shut down based on them selling illegal products. This risk, although not materialized, was perceived as present by employees of the organization and threatened the regulatory legitimacy of the organization. Moreover, it also threatened regulatory legitimacy in another way, namely via the risk of voiding a purchase agreement if illegal goods were sold via the platform. Hence threatening the adherence to rules made by the purchase agreement.

Finally from a privacy perspective, threats to regulatory legitimacy resulted in changes to the espoused theories of the firm, but not much else. Although once they had a small privacy incident, they reported the incident even though it was not necessary to report to the authorities. When asked why they did this, it was said that it would be suspicious if they never had any incidents reported even though they handle such large amount of data. This can be explained by the operationalization of regulatory legitimacy by Zimmerman & Zeitz (2002). When this operationalization is considered perceived expectations could have been threatened if they never reported the incident.

If the incident did not threaten legitimacy, it could be suggested that then they would not have reported the incident. This assumes that a perceived impact to regulatory legitimacy could be reason for an authority to investigate. The motivation for reporting the incident is not compliance, as it was not necessary to report. Thus leaving no other seeming reasons other than meeting expectations. This seems valid on account of the incident not being publicly known. Hence, the public image or reputation of the organization was not publicly harmed in any way.

Nonetheless, it was also found in the case that both propositions do not always hold if risks in the broadest sense are considered. For example with the fraud risk affecting user-side openness of the platform. Consumer fraud affected primarily the profitability of the platform itself. Moreover, it can be argued that moral and regulatory legitimacy were not threatened. Therefore, both propositions seem to hold only if public values are endangered.

In addition, it should be noted that privacy seemed to be more anticipated on than other risks such as the risk from illegal products and misleading consumers. Two potential explanations might be recognizability of risk and the responsibility of the risk. First, as was mentioned in the findings, privacy seemed to gain much more awareness by media and consequently by consumers. Whereas, in several interviews it was questioned when something is misleading or that they were lacking the expertise to identify illegal products and/or packages. Thus one explanation could be the recognizability of the risks.

A second factor could be the responsibility of risk. With privacy it is and was clear who was responsible for the risks posed to the privacy of consumers. Yet, with the risks of misleading and illegal products, often it was ambiguous who was responsible for this in the network? This also led to the organisation asking whether the authorities were responsible for compliance, or web shops themselves.

Finally, an interesting finding that might also be of influence on the aspect of responsibility is maturity. Namely, organizational maturity. As could be inferred from various statements made in interviews, the legitimacy of a start-up might not be equally affected by the same risk as a more mature organization. Furthermore, it was also stated that once the organisation became more mature they were both more capable and felt more responsible for managing the aforementioned risks of misleading web shops. Hence suggesting that organizational maturity also affects whether a risk negatively affects the legitimacy of an organization. In other words, privacy risks could be better anticipated on due to it being clear who was legally and morally responsible for the risk.

5.1.2 Pattern 2. Organizational learning

- Proposition 2A – A threat or negative effect to legitimacy increases survival tension.

According to Suchman (1995) a negative effect to legitimacy can lead to issues in the continuity of an organization. Hence the connection was made to the more detailed concept of survival and learning tensions of Schein (1993). Whereas a survival tension is defined as a perceived threat to the current way of working or even more so, the current way things are. Organization themselves cannot perceive threats. However, the agents of organizational learning, people, can. Survival tensions were mentioned by several interviewees. Specifically, the criticism of costumers, criticism of stakeholders, threat of workload and threat of regulatory interference were identified. These threats all corroborate with examples of survival tensions provided by Schein (1993). As a result of risks such as introduced by misleading practices, privacy and illegal products. Thus, leading to suggest that negative effects on legitimacy incur survival tensions.

The mechanism seems to work as such that a risk such as misleading causes a negative effect to legitimacy. As Suchman (1995) theorized, companies that have issues with legitimacy encounter issues with continuity. In terms of survival tensions, a threat to the status quo. Yet, is criticism of stakeholders a necessary condition for a threat to the status quo? If there was no criticism would there be no survival tension? By extend, would there be a reason for change? This seems unlikely. More so when reasoned from the perspective of other results of some of the risks such as increasing workload. In itself the

absence of one effect of a threat or impact to legitimacy might be insufficient to alter an increase to survival tensions. Or in other words to induce a crisis that forms survival tensions. Moreover, criticism from consumers is not necessary for a crisis to occur. Yet it can enable crisis and thus survival tensions to occur. Other factors such as threat of an increasing workload might also cause a crisis. Hence, the effect of a negative effect to legitimacy might be interpreted as a SUIN cause for survival tension.

- Proposition 2B – Double-loop learning changes a platform sponsor's theories-in-use when survival tension outweighs learning tension.

Double-loop learning entails an actor questioning the current polices (i.e. theories-in-use) used to solve a certain problem (Argyris, 1977). Hence, changed theories-in-use would be indicative of double-loop learning. Argyris & Schön (1978) delineate that a crisis might incur double-loop learning. In other words, problems start cropping up when current policies do not adequately deal with the situation at hand. In order to explain the transition, or tipping-point, of single-loop to double-loop learning the concept of survival tensions is used.

In the case of the dubious web shops the complaints were not new. Yet, at one point in time the organization found web shops no longer acceptable. In other words, survival tensions were already present in this specific event. However, in one interview it was said that the owners of the web shops suddenly wanted to add more web shops to the platform. Upon which the perspective on these web shops turned negative. Thus suggesting a tipping point. The prospect of even higher survival tensions could have outweighed learning tensions at that time. Whereas learning tensions are tensions that prevent an organization from learning or changing their current way of working (Sun & Scott, 2003). Learning tensions identified were: the norms and values of the organization, financial benefits, receptivity of feedback of people and the current routines and processes of the organization.

Before that point, the web shops were tough to let go due to their high transaction volumes among other learning tensions. Yet after the decision to let these parties go, it could be suggested that there was a change in the theories-in-use of the organization. Argyris & Schön (1978) defined an organizations theories-in-use as the collective norms, strategies and assumptions of an organization. If the norms, strategies and assumptions before and after the event are taken into account. Then, several changes can be observed. Namely, the change in norms becoming: don't accept louche web shops. Secondly, the strategy changing from accept everyone to grow, into only accept clients that can enhance your reputation, in order to gain more reputable and bigger clients. Finally, the most striking change was found in the assumptions about these type of parties. Namely, that one of the reasons why they were not let go of earlier being the financial benefits they brought the organization. Here the assumption was still: these type of parties are profitable. After the 2018 event, this seemingly changed, because interviews also referred to these parties as providing consumers that had a low preparedness to pay. Thus it can be suggested that theory-in-use changed as a result of this.

This raises the question: would the strategy of the platform have changed without the survival tensions? Seeing as the norm "don't accept louche shops" originated from the identification of louche shops, this seems unlikely. Hence lending validity to the claim that survival tensions were necessary for the new strategy and norms.

A similar dynamic can be uncovered with the smartshops decision. When asked why the smartshops were let go, one of the reasons mentioned was the impossibility to monitor for illegal products and all

risks associated with that. Yet, it was also mentioned that these type of web shops brought in a less attractive type of customer segment. This event also resulted in different norms, but not necessarily a different strategy. From a survival tension point of view the threat of regulatory interference is what motivated the decision. If there was no risk of illegal products and thus no threat of regulatory interference, then there would have seemingly been no issue according to the interviews.

5.1.3 Pattern 3. Responsible innovation

- Proposition 3A – Double-loop learning changes the background theories of the platform sponsor.

Similar to theories-in-use, a change in background theories can possibly occur as a result of double-loop learning. Whereas these background theories exist out of an individual's belief and value system (Zwart et al., 2006). Beliefs confer a descriptive view from an agent how the world is, and values confer a normative view on how the world should be. However, due to the highly socially desirable nature of this research, what actors state that their values are, or were some time ago, might be skewed. Hence, this research aims to infer organizational beliefs and values from the actions and decisions that were made. Whereas beliefs and values are organizational if they appear so from collective rules. On account of the organization not having all rules formally codified, also informal rules are taken into account as long as they are collective in nature.

According to PayNow the decision in 2018 to let the dubious web shops go was made in the interest of the consumer, yet there was also a clear connection made to the reputation and thus the profitability of the platform. Although, the moral discussion came first according to the interviews, before the reputation discussion started. It is more clear that the theories-in-use changed on account of the actual evidence being there that norms changed in the organization. Yet, it is difficult to directly infer a conclusion on whether the values changed as a result of the survival tensions faced. This is primarily due to the fact that interviewees shared conflicting insights on their views of these parties. Whereas some said that they already knew the web shops were bad shops, but others stated that only after they wanted add new labels the risks were uncovered. Nonetheless, one thing was clear and that was that these web shops caused complaints for a longer time. In addition, it should be noted that complaints in itself are fairly normal, as there are always a myriad of legitimate reasons for complaints. Hence, they should not be taken as immediate cause for worries.

If the organization kicked the parties off the platform the moment they learned about the malpractices of these web shops then their values did not change. In fact, they remained the same. On the other hand if these parties were considered bad from the moment they caused a higher than usual load of complaints and upon closer investigation they viewed the parties as not allowable then it could be stated that values changed. Yet in both cases, for reasons of social desirability it is difficult to discern objectively whether a change occurred.

In another but less significant event, this is more clear. Some web shops held return addresses in a foreign country, making it very difficult or next to impossible for the consumer to return their products if they were unsatisfied with a product. This is not necessarily illegal to do, but PayNow restricted their terms of service to only allow web shops that held return addresses in the Netherlands. A decision that effectively limits openness, yet makes it more fair for consumers. Hence foregoing financial benefits in the face of protecting the consumer.

Regardless, this leaves the question on how to assess whether values actually changed? The answer might be found in observing the perceived duty of care PayNow feels like they have towards managing risks. Whereas the duty of care is defined as going beyond the obligation necessary to ensure that such risks are managed. From interviews it is gathered that PayNow viewed their duty of care more limited before the 2018 event than after. Specifically, even before the investigation by authorities PayNow started managing risks they previously viewed as not their responsibility. The most concrete example of this is found in earlier views stating that it was the authorities that should ensure to a certain extent that web shops adhere to consumer laws and rights. Yet, after 2018 this stance widened to include themselves making sure that web shops should comply to a set of conditions and methods of doing business PayNow held themselves to. This can be interpreted as a change in the background theory of the organization.

From a counterfactual perspective: if the risks did not lead to questioning then the responsibility would not have changed. This seems plausible on account of the questioning of leading to the internal compliance investigation. However, an alternative explanation that responsibility is a function of organizational maturity confounds with this view. Yet, when this logic is applied to the event of smartshops it can be seen that responsibility for risks outside the network actually decreased. Nonetheless, it can be argued that not having the responsibility for illegal products is a decision made in the interest of PayNow. Consequently, whether this was a result of changed values remains questionable.

In the case of privacy risks, the CTO did admit that privacy was less important in the beginning phases of organization (i.e. start-up phase). Whereas as time went on consumers started asking question about how their data was handled by the organization. Consequently leading to the organization questioning how they actually are utilizing data safely and with privacy in mind. This is validated by the fact that the privacy statement from 2014 and 2020 almost show no change in processing activities. Hence, it can be inferred that the organization had the value of privacy in mind from the beginning. Nonetheless was there a change in values as a result of privacy risk? According to the interviews: yes. Whereas before it was suggested in an interview with the CTO that the credit check might have used data in more than one way. If they did not impose limitation on the usage of data themselves. Furthermore, again this seems validated by the lack of changes in the processing activities from the privacy statement.

Yet the counterfactual remains difficult to validate as it entails: no questioning from consumers would result in no privacy concerns. This counterfactual is inherently problematic, because it assumes that only the questioning resulted in privacy concern as a necessary condition. As was noted before privacy awareness was raised in recent years, leading to society as a whole becoming more aware. Hence, it can only be suggested that consumer questioning is sufficient to raise privacy concerns. Consequently, it cannot be ruled out that the absence of consumer questions would have led to a different outcome.

Nonetheless, a change in organizational beliefs did seemingly happen. Grin & de Graaf (1996a) conceptualized beliefs (belief systems) as an actor's descriptive view of the world. According to Grin & de Graaf these beliefs shape the objectives and strategies of actors. In other words an actor's belief system could be argued to generate the problem formulation that leads to the objectives of an actor. Grin & de Graaf (1996a, p. 301) provide an example assumption of a belief system: "for the realization a sustainable society, material and energy cycles need to be closed". The central problem here is open material and energy cycles. According to Argyris & Schön (1978) an actor's theories-in-use are adjusted

based upon how well it 'solves' a problem. Hence, it could be suggested that a changed problem formulation and changed theories-in-use are indicative of a changed belief system.

As such the question arises: did the organizational beliefs change? In the case of the dubious web shops a shared view was the assumption that accepting all parties they could get was necessary to grow. It was observed that this assumption did indeed change. Whereas, after ousting the dubious web shops the platform decision-makers viewed these parties as no longer necessary. This not only indicates a change in theories-in-use, but also in descriptive theories of how the world works (i.e. beliefs). Whereas on an abstract level it could be stated that first these parties were viewed as beneficial and afterwards they no longer were. A similar interaction can be observed in the case of smart shops. Before the decision to restrict openness, they were viewed as beneficial. Yet, after identifying the risk it could be stated that these parties were deemed as no longer beneficial to growth.

Regardless, of whether beliefs changed, the proposition specifically states background theories as a whole. Thus, aforementioned events and conditions of social desirability make confirming the proposition difficult, unless the broader duty of care is accepted as indicative of values.

- Proposition 3B – The changed background theories of the platform sponsor affect the platform openness.

Platform openness had changed over time, due to several risks identified. Whereas, this was stronger in the case of risks such as misleading, illegal products and fraud than privacy. The definition of openness used is: the degree of ease for external actors to use services of the platform or build on the platform (Evans et al., 2006, p. 12). In addition using the dimensions of openness as defined by Ondrus et al. (2015) and the definition of access openness (Karhu et al., 2018), to operationalize openness. Using these notions the following changes in openness can be identified.

Firstly, a change in supplier openness. The web shops allowed to the platforms has restricted over time due to changes in the due diligence of the organization, but also other norms in the organization. This illustrates that the theories-in-use have changed. Yet, does this also entail that background theories have changed?

Confirming whether organizational values changed remains difficult. Yet, as argued above changed theories-in-use seem indicative of changed organizational beliefs. Before the risks were identified, a descriptive theory on growth of the platform could have been: a higher degree of openness leads to a higher degree of growth. After the risk it seemed clear that this theory did not always hold. Especially, if you need a good reputation to get better clients. As is exemplified by the case that no more 'bad' web shops are accepted after learning about the risks. Other changes are also the smart shops that are no longer accepted on the platform due to the risks associated with the products being sold.

If the responsibility of the platform did not widen, then the openness would not have changed. One specific way this is illustrated is by the fact that if the platform still thought that it was the authorities' job to take care of risks harming consumers, then they would not have interfered with the dubious web shops. Instead the openness could remain the same, as an authority should take 'bad' parties of the market according to that view.

Secondly, the user side openness has also changed over time. Namely due to the fraud risks associated with some web shops and more specifically the assumptions that changed about certain segments of

web shops such as the fraud sensitivity of certain product groups that led to a stricter credit check and by extend thus user openness on the platform. Similarly from a perspective of beliefs, some beliefs changed on which products were more fraud sensitive. Suggesting that if the beliefs on the fraud sensitivity did not change, then user openness would not have changed.

Finally, due to privacy concerns the openness toward the data validation provider was also limited to parties that held privacy in high regard. Which is an example of a value that affects the provider openness of platform. On account of more data validation services used, the more users can join the platform. As argued before, a seeming trade-off has been made with foregoing financial benefits in the face of privacy. Hence, if privacy was not of concern, then there was no reason for provider openness to change. Similarly to proposition 3A background theories as a whole are difficult due to confirm due to social desirability. Yet, it can still be argued that the organizational belief system did change.

5.2 Summary of propositions

This chapter summarizes whether the propositions have been met. In the case support was found for the propositions involving legitimacy. Whereas both privacy and other types of risks were found to negatively affect regulatory legitimacy. However, the identification of fraud risks did not seem to threaten legitimacy. Therefore, a risk only threatens legitimacy only if public values are threatened.

Furthermore, it was found that the effect of a threat or negative effect to legitimacy resulted in an increase of survival tensions. Yet, it was also found that these effects were SUIN causes of survival tensions. In other words they were a sufficient but unnecessary part of the causation of survival tensions. This suggests that survival tensions can be increased by other phenomena and enabling conditions as well. This is also seen with the risk of fraud. This risk adds to survival tensions, yet it does not pose a threat to legitimacy.

The crisis incurred by survival tensions was found in the case to lead to questioning of practices. Ultimately this led in several events to changed strategies, assumptions and norms. However, due to the social desirable nature of the research and the remaining alternative explanations it was not confirmed whether questioning led to changed values. Yet, the theories of action, or in other words the beliefs of the organization, did change. Hence propositions 3A and B are marked as not met.

Specifically, background theories as a whole did not necessarily change. However, a nuanced proposition that remains is that the belief system of an organization does change as a result of double-loop learning. In addition, using the concept of theories of action, support was found for theories-in-use of the organization resulting in a changed platform openness. Specifically it was found that privacy risks led to a reduced provider openness and other risks led to a reduced supplier and user openness. The table below summarizes these findings.

Proposition nr:	**Proposition:**	**Support found for proposition:**	**No support found for proposition:**
1. Legitimacy theory			
1A	A risk threatens or negatively affects the moral legitimacy of the platform sponsor.	X	
1B	A risk threatens or negatively affects the regulatory legitimacy of the platform sponsor	X	

Proposition nr:	Proposition:	Support found for proposition:	No support found for proposition:
2. Organizational learning			
2A	A threat or negative effect to legitimacy increases survival tension	X	
2B	Double-loop learning changes a platform sponsor's theories-in-use when survival tension outweighs learning tension	X	
3. Responsible innovation			
3A	Double-loop learning changes the background theories of the platform sponsor		X
3B	The changed background theories of the platform sponsor affect the platform openness		X

Table 7 Summary of proposition support

6. Discussion

This chapter answers the main research question in the first paragraph. In addition, this chapter describes the limitations, alongside the practical and theoretical implications of the study. Furthermore, practical recommendations for the case company are made and future research suggestions are provided.

6.1 Conclusion

A platform needs to have sufficient market potential, represented by the number of users who can join a platform. Platform openness affects the ease of actors joining the platform. Hence, in order to increase the chances of platform success, platforms want to maximize market potential and consequently also platform openness. This is problematic because architectural configurations with the highest market potential do not necessarily represent the most favourable configurations for societal values. Although there is anecdotal evidence of safety and privacy risks resulting in adjusted platform openness, there is little literature explaining the drivers and the process of adjusting due to risks posed to societal values. Hence, this thesis aims to build an initial theory on the process of how digital platforms adjust their platform openness upon learning about risks for societal values. Accordingly, the following research question was formulated:

- *How does a digital platform sponsor adjust openness upon learning about privacy and safety risks?*

Originally, the anecdotal evidence available pointed toward safety and privacy risks as potential risks that affected openness. Yet, this case uncovered a more broad spectrum of risks that affect societal values. Hence, instead of focusing solely on privacy and safety other risks were also investigated.

RQ1 – What theories in available literature explain how platform openness is adjusted upon learning about privacy and safety risks?

Available literature on platform openness and digital platforms explain how platform openness evolves due to financial and innovation dynamics. Furthermore, the concept of generativity explains why risks can appear unprompted for a platform. Nonetheless, literature on platform openness does not provide an explanation for why a platform would change due to the emergence of societal risks or how platform openness would adjust over time upon learning about this. Existing literature on legitimacy theory, organizational learning and responsible innovation provide a potential solution to this knowledge gap.

Theory on legitimacy provides an explanation for why a platform would want to change their practices due to societal risks. Specifically, legitimacy theory conceptualizes that an organization's actions are desirable within a system of public norms, values and beliefs. Furthermore, the process of organizational change (i.e. learning) is explained via established descriptive theories on organizational learning. Whereas primarily the concept of double-loop learning is used to explain the process of organizational change.

In contrast to legitimacy theory, theory on responsible innovation provides an explanation for why an organization changes without a threat to legitimacy. Legitimacy theory suggests that a risk that is not known to the public, might not motivate an organization to act. Hence, theory on responsible innovation fills this gap by providing an alternative understanding of how the values and beliefs of agents can motivate change without a risk present. Analogous to real-life an agent might be motivated to show certain behaviour due to an extrinsic reward (e.g. threat to legitimacy). Yet, behaviour can also be

triggered by an intrinsic motivator (e.g. values/beliefs). Moreover, the concept of second order learning also explains how these values and beliefs can change themselves. The model derived from above theories provides a theory on how platform openness is adjusted upon learning about privacy and safety risks.

RQ2 – How do platform sponsors adjust openness upon learning about safety risks?
In the case a process was observed where societal risks formed a threat to legitimacy. Concurrently, this threat led to survival tensions and ultimately double-loop learning. This learning affected the theories-in-use of the platform. Nonetheless, changing background theories were difficult to discern as explained below.

As mentioned, safety risks were not a prominent risk. Instead, it was found that risks of misleading, fraud and illegal products were more present in the case. It was found that misleading practices by web shops and illegal products resulted in potential risks for consumers. Hence incurring not only a regulatory obligation to protect these consumers, but also the morality of the issues motivated the platform under study to change. In other words, these risks affected moral and regulatory legitimacy.

Survival and learning tensions explain in greater detail the 'crisis' that is induced by a threat to legitimacy. Specifically, the concept explains a tipping point in the events leading to the case platform restricting openness. The effects observed due to the risks were criticism of consumers/stakeholders, the threat of an increasing workload and the threat of regulatory interference. Resistance to change was also observed in the form of existing norms and values, financial benefits, the existing routines and a lowered receptivity of feedback of decision-makers. This resistance is conceptualized in literature as learning tensions.

In the case it was found that the theories-in-use of the organization did indeed change upon identifying a risk. Specifically, based on documents and interviews it was found that strategies, assumptions and norms did change as an effect of certain risks. According to the interviews a change in values and beliefs could also be observed. Yet, alternative explanations such as financial gains and the socially desirable nature of the research conflict with this view. Nonetheless, a change in the responsibility of the platform was observed as a result of risks. By taking responsibility for risks in the ecosystem the platform adjusted openness for those actors that brought about these risks. The risks of misleading web shops and illegal products caused changes on the supplier-side over the years. Whereas fraud risks resulted in both an effect on supply-side and user-side openness.

RQ3 – How do platform sponsors adjust openness upon learning about privacy risks?
In the case of privacy risks, a similar process as the other risks was observed. Likewise a threat to moral and regulatory legitimacy was observed. Although in the case of privacy risks it was better anticipated upon than the earlier outlined risks. Two possible reasons were found during the case study.

First, responsibility of a privacy risk is more clear than other risks. As can be seen with risks 'external' to the organization (e.g. misleading) discussion arises on who is responsible. Secondly, privacy risks are more recognizable than other risks such as the risk of misleading consumers. It is less clear to people when something can be considered misleading or just clever marketing. Conversely, issues with privacy can be identified more easily. A third contextual factor might also be the increasing attention to privacy over the years. Ultimately this also led to the introduction of the GDPR.

Privacy risks motivated change due to the tension introduced by the threat of regulatory interference, the threat of criticism but also the need to do better. An example of how privacy risks affected the background theories in the organization is reflected by the case decision on data validation. In the case, the platform knowingly chose only a small selection of data validation providers to share data with. This is interesting on account of this decision not necessarily being made in the best interest of raising a platform's market potential. Instead it could be suggested that having more data validators as providers, and thus sharing more data could increase the acceptance rate of users even more. Hence, privacy risks led to restricting provider openness in the case observed.

RQ4 – How does the conceptual model explain how privacy and safety risks affect platform openness?
Both sub-questions suggest that societal values also influence digital platform openness. In order to validate these findings, the final sub-research question compares the conceptual model to the empirical findings.

Ultimately, support was found for most of the propositions derived from the conceptual model. The propositions on legitimacy were met from a theoretical perspective. Suggesting that societal risks do indeed negatively affect the moral and regulatory legitimacy of the organization. Moreover, a threat to legitimacy, seemed to incur a threat to the status quo which resulted in changed theories-in-use. Accordingly, openness was adjusted as a result of risks that threatened public values. Regardless, propositions on changed background theories (i.e. values) were difficult to rule out due to alternative explanations.

One alternative explanation arises from the finding that a platform's legitimacy is influenced by an organization's maturity. Consequently, a more mature platform has a higher responsibility in the ecosystem. This suggests that a different organizational maturity might affect what societal risks actually affect the platform and thus how openness is adjusted. However, privacy risks were seemingly taken into account regardless of the maturity of the organization. In addition, restrictions to openness were not observed without a risk affecting public values. Hence, evidence supports that maturity affects an organization's responsibility and by extend openness, but does not explain all changes to openness.

Another alternative explanation is that instead of values, financial gains moderated platform openness. An example is the decision to oust certain web shops on account of them being morally reprehensible and hurting the reputation of the platform. Due to the effect of social desirability, it remains questionable whether certain actions were performed due to moral reasons. Moreover, a good reputation is beneficial to attracting new clients. However, there were instances where the platform forewent financial benefits in the face of values such as privacy. An alternative explanation could still be that this was motivated to protect the organization from fines or reputational damage (i.e. loss of clients). Therefore, the evidence cannot rule out this explanation and future research is necessary.

Main RQ – How does a digital platform sponsor adjust openness upon learning about privacy and safety risks?
An initial theory of how a digital platform sponsor adjust openness upon learning about societal risks is found. Whereas this process is characterized by the interaction between the platform and its ecosystem. In this case society and other stakeholders were instrumental in identifying risks. Accordingly the case findings suggest that threats to societal values might also affect openness on account of a threat to legitimacy affecting the status quo and profitability of the platform. Nonetheless, it remains questionable whether a platform's organization value system actually change as a result of risks. In sum, findings support that theories-in-use of the organization change due to societal risks, resulting in different norms, assumptions and strategies and ultimately an adjusted platform openness.

6.2 Limitations

Due to the design and context of this research several limitations can be derived. These limitations are outlined below. First, primary limitations such as social desirability are discussed. Secondly, the inherent recall bias of this research is addressed. Finally, the quality of research is assessed according to the concepts of construct validity, internal validity, external validity and reliability.

First, due to the nature of the subject that is being researched (e.g. handling of risks) there was a high risk of respondents providing socially desirable answers. Moreover, due to the potentially sensitive nature of the research data collection could be skewed toward answers far from the truth. However, there have been several precautions taken to reduce the potential of socially desirable answers. Firstly, the report and all personal details pertaining toward the company, its partners/stakeholders and interviewees have been anonymized. This has been done to reduce the perceived risk of speaking freely. Second, the data sources selected for interviews and content analysis have not been chosen by the case study company. Instead, the researcher made a list of documents and people that seemed relevant for the case study. Furthermore, the interviewees covered a large part of the organization and interviewed people in roles of customer service employees up to middle and upper management. Although the nature of the research might motivate respondents to provide socially desirable answers, the researcher also has reason to believe that there are also respondents that answered freely. Nonetheless, some questions of the research went into how and why the company dealt with certain risks. A decision to do something about a risk could be financially driven, but it could reflect better on the company if it was a moral decision. Hence, the values and beliefs were difficult to derive directly from interviewees themselves. Finally the case company requested reviewing this report before finalisation. Although the changes made due to review were factual corrections, it can be deduced that the parties were on some level concerned about the outcome of the report.

Secondly, the research investigates changes to platform openness over time due to risks. Moreover, the research primarily uses interviews to gather insights how an organization deals with this. Hence, this might introduce recall bias to the research. In other words, depending on people recalling certain events might result in a lower accuracy or less than complete recollection of events (Sekaran & Bougie, 2016). In order to mitigate the effect of this bias to a manageable extent data source triangulation has been utilized. Both interviews and documentation surrounding certain events were used to validate findings and verify their completeness. Nonetheless, in some cases there was no documentation available surrounding a certain decision. Consequently, some findings are possibly subject to recall bias in the research. As is documented in research on organizational learning, documentation highlights the espoused theory of an organization. In other words, the activities that an organization *says* they do. While this does not necessarily show what they actually do (i.e. theories-in-use).

Quality of research

According to Yin et al. (2018) there are several tests for judging the quality of social science research. These tests relate to the construct validity, internal validity, external validity and reliability of the study.

Construct validity

Sekaran & Bougie (2016) define construct validity as the fit of the data collected with theoretical concepts defined. Yin et al. (2018) elaborate on this by stating that a case study should correct operationalize measures of concepts in a case study. Moreover, Yin notes that this can be quickly become lacking in a case study. As a result vaguely operationalized measures can lead to questions on

what is actually measured or whether the concept was measured, if at all. Yin et al. (2018) recommends to define the concepts used in the study and clearly operationalize the measures used.

In this case study, a selection of well-established, longstanding theories have been used to define how organizations learn, what platform openness is etc. Definitions of concepts are outlined in section 2.3 Definitions and subsequent concepts are outlined in the section 2.4.2 Description of propositions. Accordingly each proposition has operationalized measures defined often based on existent literature that operationalize similarly. Yet, some concepts such as belief and value systems require the interpretation of the research and require inferences to be made based on none other than the data collected. Hence, rendering these measures vulnerable to a certain degree of subjectivity of the researcher. In order to lower the impact of this judgment, the researcher has attempted to describe the exact decision rules used to interpret certain findings.

Internal validity

Internal validity is the degree of confidence in the causality of relationships identified or propositioned in the study (Sekaran & Bougie, 2016). In the domain of case studies internal validity is not at the level of an experiment. This research can be characterized as both explanatory as well as exploratory in nature. This can be stated on account of the study aiming to confirm certain events led to certain conceptual mechanisms. In contrast, new relationships discovered are also included. Yin (2018) suggests various tactics for ensuring that confidence in the inferences made is raised. These tactics are: pattern matching, explanation building, addressing rival explanations and building logic models.

First, as outlined in the design of the research pattern matching was used as the analytical strategy of this research to strengthen internal validity by using theory to 'predict' empirical events (Yin, 2018). If predicted patterns match empirical patterns then conclusions can be made about the relationships of the events. However, this also relies on the execution of another tactic. Namely, addressing rival explanations. If a causal relationship between X and Y is suggested but actually Z could also have caused it then there exists a threat to internal validity. Hence, this study includes some rival explanations that the research could think in the findings sections. In addition, using counterfactual analysis the researcher has attempt to raise the internal validity. Thus, ruling out to certain degree of conclusiveness what inferences can be made about certain events. An important side-note to consider is that pattern matching was only used for a selection of pre-defined propositions. Inferences made about relationships between other/new found variables are solely inferred from interviews and documents gathered. In addition, not all propositions could be resolved with high confidence. An example of this are background theories and the inferences made in this.

Secondly, explanation building in order to build theory was utilized in the format of an iterative structure (Yin, 2018). In order to do this the findings were first introduced with a piece of narrative on the context of an event and shown the diachronicity of the case. Then the event was analysed more conceptually by discussing what happened in the case against a theoretically relevant statement (e.g. What caused this change in the trade-off and what caused the organization to let go of the web shops in the first place?). Hence this structure aims to follow a chronological structure to highlight the sequence of actions through an event, and sometimes also compare this to other events. One example of this is the event around the dubious web shops and another event on smartshops.

Finally, some network/relationship diagrams were positioned at the end of some sections to elaborate on the intermediate processes or outcomes of certain events that happened within the case. Yin (2018)

recommends using so-called logic models as developed by Wholey (1979) to highlight the sequence of events. Thereby showcasing the cause-effect patterns between specific events (Peterson & Bickman, 1992; Yin, 2018). This aims to prevent making causal inferences on relationships that do not exists. Instead of using logic models, this research used existing functionality of Atlas.ti's network diagrams to identify relationships between existing codes on an event level. This decision was made on account of this enabling the researcher to review quotations of codes in interviews and documents and validate relationships inferred.

External validity

Sekaran & Bougie (2016) define external validity as the generalizability of results to other settings. As raised by Yin (2018) a case study may not reach statistical generalization, but analytical generalization is possible. An important aspect of this research that already limits the statistical generalization is the setting of the case. The findings found that the regulatory environment has an effect on the platform openness of the organization. Although this case represents a company in the Dutch payment service sector, not all regulation applicable to a payment service provider applies to this organization. Hence, the regulatory pressure might be greater in a different case in the same sector. Accordingly, it may be that regulatory legitimacy may play a larger factor in affecting platform openness than is portrayed in this research. Hence, the actual impact on openness and risks found may have limited external validity.

However, the mechanisms (i.e. propositions) developed do largely corroborate with empirical findings. Hence, an overlap with the theoretical mechanisms of legitimacy and organizational learning and empirical findings is found. Due to the nature of pattern matching, theoretical mechanisms were explicitly compared with empirically found processes. Accordingly, is there some level of analytical generalization reached in this study?

Yin et al. (2018, p. 73) argues that analytic generalization "may be based on either (a) corroborating, modifying, rejecting, or otherwise advancing theoretical concepts that you referenced in designing your case study or (b) new concepts that arose upon the completion of your case study". Further outlined in section 6.6 theoretical implications, theory used to build propositions led to advancing theory by combining existing theory into a new perspective, while also conforming these propositions in a context that it was not earlier used for. Based on this definition of analytical generalization it could be stated that by confirming the propositions from theory this study corroborates existing theory. Consequently, some level of analytical generalization is reached and adds to the external validity of the study.

Reliability

Yin (2018) defines that reliability entails the possibility to repeat a study and minimizing bias and errors in this process while receiving the same findings. In order to uphold this section 3.4 Case study protocol outlined the exact protocol used to collect and analyse data. While other procedures such as case selection is also highlighted. In addition a case study database is upheld in the form of an Atlas.ti project which also contains analytical memos which discuss coding decisions made. Furthermore, in the beginning of section 4 Results. There is also an example table provided which describes the coding process in order to provide the reader with an account of how decisions on merging, removing and coding were made. Moreover, since a fair portion of the findings are based on interviews the interview protocol used is also included in appendix A. One threat to reliability might be a lack of convergence from multiple observers or coders of the data (Miles et al., 2014). As the coding and interpretation of data occurred via one researcher reliability might be affected.

6.3 Practical implications

The theory developed has practical implications in the sense that it can guide platform sponsors to think about their responsibility, or duty of care, and how participatory forms of engaging with stakeholders and the public can help to better avoid harm occurring form risks that affect society.

Furthermore, this research also provides an initial conceptualization of a what a responsible digital platform could be. In addition, the study also provides practical issues that were dealt with as a result of value conflicts and the decisions and trade-offs that need to be made as a result of being or becoming a more responsible platform. This is important as the negative effects of open platforms also need to be taken into account.

Moreover, the main practical implication of this study may be as a problem formulation of open platforms. Especially with the continued rise of open digital platforms this becomes more important. As digital platforms such as in the Internet of Things domain become increasingly pervasive in society, these platforms also have access to increasingly more physical parts of life (e.g. vehicles) and data (e.g. medical data). Hence, the societal implications of digital platform openness need to be better understood in order for platforms to open up responsibly. Not only digital platform sponsors can learn from this, but also policymakers. Whereas this case shows that a laissez faire approach to open platforms may give rise to future emergent societal risks.

Finally, this research provides an empirical account of how a platform sponsor learnt to deal with the emergence of certain societal risks. Other platform sponsor can learn from these accounts. Specifically, a platform sponsor may pay attention to the methods of risk identification. As these methods define primarily how equipped a platform is to identify societal risks.

6.4 Practical recommendations

In complex networks with many different agents, it can be difficult to define who is responsible for certain risks. This is also referred to in some context as the Problem of Many Hands (See Van de Poel (2015). In some cases responsibility is bestowed upon the actor which has the ability to foresee some risk of occurring (Van De Poel et al., 2015). Similar to this case, one institutional actor bestowed the responsibility of watching out for external risks upon the platform due to their ability to spot early signs of harm occurring (e.g. consumer rights being harmed by web shops). Hence, this case also allows some findings to be framed as a lessons or recommendations for platform to become more responsible. In other words, the findings of this case allow some recommendations for becoming a responsible platform to be formulated.

Participatory governance of the platform

Due to the generative nature of digital platforms it theoretically becomes very difficult to fully anticipate risks. Yet, as found in this case a well-working identification mechanism is key to uncovering risk. As found in the various types of risks identified in the case, the public played a crucial role in this. This highlights the importance of setting up opportunities to 'listen' to society. This may be in the format of customer service like in the platform, but also in the format of looking at online forums and observing customer complaints and satisfaction. In essence by listening to the public, this creates a form of participatory governance. Whereas participatory governance efforts have been known to increase the responsiveness of institutions (Speer, 2012), it can also increase the responsiveness in reacting to new risks by a platform.

Questioning practices
In the case it was found that some identified risks caused discussion. Discussion that questioned existing norms, strategies and even assumptions. Eventually these discussion were the foundation of some changes to be adopted. This questioning forms the conceptual foundation of what is called double-loop learning in this research. Yet, how does this questioning actually make its way in the organization (i.e. is the knowledge internalized)? In the case it was found that questions were raised in team meetings and discussions between colleagues form different departments. As a result discussions did not disappear over time. Hence an open culture which allows for questioning of existing practices and maybe even promotes questioning can function to enable this type of behaviour.

Responsibility as a result of double-loop learning
Doorn (2010) argues that a possible result of double-loop learning might result in a shift between the relationships of actors in a network. Similarly in this case, a shift between the relationships of suppliers and the platform was observed as a result of double-loop learning. Whereas the platform adopted more of a supervisory role over web shops than before. The case also highlights that reputation is a significant factor in both the competitive advantage of the platform, as well as ability of the platform the accept a higher class of clientele. In essence, by taking responsibility to ensure that risks caused by external parties were taken care of, negative reviews could be avoided, and even led to a strategy of getting better clients through being a more responsible platform. Hence, it can be beneficial for a platform's reputation to take up responsibility.

6.5 Link with Master programme Management of Technology

This study is fitting to the researchers Master programme, Management of Technology. This study researched the balancing act of how a platform can be responsible while still upholding the market potential of a digital platforms. Whereas a platforms' market potential directly affects the competitiveness and profitability of the platform. This study investigates not only societal dynamics, but also service/platform governance and the functioning of the knowledge processes in learning about risks. The case study researched a technologically-driven phenomena named digital platforms and how this technology is affected by societal risks. Specially this research studied one digital platform from the perspective of the platform utilizing interviews and collected documents to provide an outside account of how an organization utilizes its digital payment platform to manage risks brought about by the inherent generativity of innovations such as digital platforms. Finally, utilizing scientific methods this balancing act is researched and provides not only an initial theory of how digital platform openness is adjusted due to societal values but also provides a practical account on how platforms can manage risks to societal values.

6.6 Theoretical implications

Based on this research there are several theoretical implications that can be derived. This paragraph outlined these implications per theoretical field. First, before the implications are described, the general value of this study is explained. Secondly, there are four important implications for theory on digital platform openness. Thirdly, two concepts were found to have new implications in future research on digital platform openness. Finally, this study describes implications for theory on organizational learning and provides a starting-point for research on responsible platforms.

First, the study provides an initial theory outlining how a platform sponsor adjusts openness upon learning about societal risks. More specifically, a theory has been developed that builds upon earlier

established and prominent theories from the respective fields of organizational learning, legitimacy theory and responsible innovation. The theory explains how, why and when a platform sponsor adjusts openness when learning about risks. This research has added to existing literature on platform openness in the sense that currently primarily innovation and financial dynamics explained how openness was designed and subsequently evolved. Yet, as this research suggests, societal values also play a role in determining and adjusting platform openness. Specifically in this case user, supplier and provider openness. Moreover, this theory furthers the understanding of the governance of digital platforms by providing an preliminary description of the reflexive relationship between platform openness and risks as a result of a platform's generativity.

Secondly, this research combines previously unconnected streams of literature on platform openness and organizational learning to understand platform evolution. As raised by Gawer (2014), previous platform literature does not explain how or why platforms evolve over time. Gawer provided an integrative framework on how digital platforms evolve due to innovation dynamics. This research provides a new perspective from the organizational sciences on how a digital platform evolved over time due to organizational learning. Whereas Gawer provides exogenous drivers for change, this research provides endogenous drivers of change in the platform (i.e. survival tensions). Hence, this furthers understanding on how digital platforms evolve over time. As such, future research investigating platform evolution should consider endogenous drivers of change alongside the earlier referred exogenous drivers.

Furthermore, this research provides an alternative perspective to contemporary literature on platform openness. Whereas contemporary literature on platform openness provides drivers from an economic and innovation perspective on why a platform sponsor is motivated to open up or restrict openness. Contemporary literature captures trade-offs in opening up from these perspectives (e.g. De Reuver et al., 2015; Wessel et al., 2017). Nonetheless, this does not capture the trade-offs a platform sponsor faces between openness and societal values. This research provides an initial understanding of how societal values such as privacy and fairness are affected by openness and subsequently captures these trade-offs made by a platform sponsor. Besides drivers of openness, this research also captures the consequences of openness on societal values. Therefore, this research might be a starting point into research investigating negative externalities of open platforms. Instead, it is observed that the state-of-the-art literature still mainly focusses on the positive effects of openness.

In general there are few studies who consider the effect of risks on platform openness. Previous research on platform openness that does consider risk suggested that certain risks such as privacy and security affect openness (e.g. Mosterd, 2019; Schreieck et al., 2017). Yet, no research has studied the phenomenon on how platform openness is adjusted upon learning about risk. This research provides a preliminary description of this process of adjustment from the perspective of a platform sponsor. As such this research moves beyond recent studies that focus on factors that affect platform openness. In addition, other risks than security and privacy have also been uncovered. Furthermore, the aforementioned studies only mention risks as a factor affecting openness. Whereas this research provides a more descriptive account on how risks affect openness rather than listing factors. Thereby providing an early process which can be used or adapted in future research. Specifically, the theory developed provides a theoretical foundation for future studies to understand how risks affect platform openness.

Moreover, literature defines openness as a unidirectional process, instead it appears bidirectional and reflexive in nature. This research found that risks can be anticipated and subsequently affect openness. Yet, risks are also not always foreseeable in the design of a platform. Hence, openness can be adjusted upon learning about these risks. Furthermore, after platform launch, a platform can encounter new risks due to having a certain degree of openness. This is also illustrated in the case whereas a specific openness allowed certain risks to occur. Hence, highlighting the reflexive and bidirectional nature of risks and platform openness. Subsequently, future research on the drivers of openness should also consider how consequences of openness can ultimately affect openness reflexively.

Two concepts have been found useful in understanding the process of adjusting platform openness. One interesting finding from this research is the notion that organizational maturity affects platform openness. Based on a literature research on platform openness this was not a prominently covered relationship. Hence, this study adds to existing literature on platform openness by relating organizational maturity to openness. In literature an organization's maturity is sometimes linked to its legitimacy (See Stinchcombe, 1965; Zimmerman & Zeitz, 2002). If the indirect link of a platform's legitimacy and its openness is accepted then future studies should consider organizational maturity as a moderator affecting drivers of openness.

The second concept is legitimacy. This study has been one of the first studies to consider the concept of organizational legitimacy as a driver of opening or restricting platform openness. Specifically moral and regulatory legitimacy can help explain why openness is adjusted. Findings that factors such as reputation, values and regulatory pressures (e.g. expectations of authorities) can shape decision-making on platform openness. Hence suggesting that future research on platform openness should consider moral and regulatory legitimacy as drivers for adjusting platform openness.

From a perspective of organizational learning this research has incorporated theory on organizational learning and legitimacy theory in order to provide a new perspective on what triggers organizational learning. Sun & Scott (2003, p. 205) state that one major issue with organizational learning theory is that: "The learning process is well described by Argyris and Schön. However, the triggers that spur the learning process are not addressed". In an attempt to overcome this issue, legitimacy theory was incorporated as a theory that provides an understanding of the trigger of organization learning (i.e. why/motivation). Furthermore, as is derived from empirical findings how risks are identified via efforts of the public also shed light on how risks are identified by a platform. Hence, providing theory on organizational learning a different perspective on how organizational learning is triggered by threats to an organization's legitimacy.

Finally, this study provides a call for research in the conceptualization of responsible platforms. This study provides an empirical account on how platform openness can challenge existing societal values. In addition this research also highlights how a platform's generativity can enable unforeseen risks for society to occur. Subsequently, this study can be viewed as an initial problem formulation for a larger problem inherent to open platforms. Namely, the realization of unforeseen risks in a society where platforms are becoming increasingly pervasive. Whereas solely methods of anticipation might come up short in identifying risks prior to a platform's launch. Hence, future research is necessary in order to learn how to manage these unforeseeable risks responsibly. A potential starting-point for research is outlined in the future research section.

6.7 Future research

Although this research answers one question in research, it also brings about new questions for future research. Firstly, this chapter provides three potential avenues of research to test alternative explanations and overcome limitations inherent to this study. Secondly, an early problem formulation and call to research on responsible platforms is provided.

Firstly, one such opportunity for future research may be a longitudinal case study to better observe changes in theories-in-use, and more specifically changes in belief and values systems and prevent recall bias. This research had difficulty in claiming that societal risks led to changed value and belief systems. Hence longitudinal research might uncover trade-offs previously unknown due to social desirability. Whereas a researcher could observe the decision-making unaffected by respondents making the reality/history look better than it is. A researcher could record the exact views and values of respondents across various timeframes (e.g. years apart). Furthermore, in order to infer organizational values and beliefs, the researcher could capture organizational decision over a specific timeframe him/herself. Specifically, unchanged beliefs or values (negative evidence) after learning about societal risks could point toward ruling out that organizational values change as a result of risks posed to a platform.

Secondly, on the topic of case research, cross-case analysis in different types of digital platforms and different industries can add to this research. Firstly, the case studied may be classified as a subset of a digital platform (i.e. payment service provider). Yet, there are many other types of digital platforms which could influence which risks are faced and how risks shape (different) dimensions of platform openness. For example emerging Internet of Things platforms could have very different types of risks affecting different openness levels more prominently than is observed in this case. These cases could lead to very different dimensions of openness to be affected than observed in this study.

Thirdly, one alternative explanation that was difficult to disprove in this research related to financial dynamics. Did values and beliefs affect openness or did financial incentives shape decisions to restrict openness? Upon first sight restricting openness might seems counterintuitive if one's goal is to increase the profitability of the platform. Yet, upon closer investigation it can be suggested that financial gains might still motivate decision-making. Firstly, when the dubious web shops were let go further reputational damage and future legal fees were prevented. Whereas reputational damage could entail a loss of high-end clients according to some interviews. Secondly, the decision to limit openness towards smart shops could have been made to prevent future legal fees. Therefore, future research should be conducted on the effect of financial incentives on decision-making for openness. This research can disprove that solely financial incentives motivate platform sponsor decision-making in adjusting openness. Possible research designs include case studies of non-profit, community- or government-owned digital platforms. Whereas profitability can be of lower or no priority in these cases.

Finally, this research provides an empirical account of the negative externalities of open platform and how they can harm public values. Due to the generative nature of open platforms some of these externalities may hardly be foreseen. Hence, current methods of anticipation may fall short of dealing with the uncertainty brought about by generativity. As a result, open platforms are sure to give rise to more societal risks in the future. Therefore, different approaches are necessary to reduce the impact of these risks or reduce the uncertainty in anticipating on these risks.

Earlier research by Van de Poel (2017) on unforeseen risks argues that social experiments are a possible avenue to reduce uncertainty. He argues that responsible social experiments may be necessary to be able to anticipate on new risks. Van de Poel (2017) equates introducing new technology in society to a social experiment of sorts. However, often there is much uncertainty about the potential benefits and disadvantages of a new technology. Yet, Van de Poel argues that in order to reduce this uncertainty social experimentation may be necessary. Similarly he also notes that this might raise ethical concerns and put undue risks on society. Van de Poel remarks that methods of anticipation might still prove useful, but anticipating 'unknown unknowns' is something anticipation does not solve. Hence, learning-by-doing from a new technology embedded in society might be useful in reducing uncertainties (van de Poel, 2017). Nonetheless, Van de Poel reasons that this form of learning might also put an undue burden on society if undesirable effects occur. Therefore, he proposes learning-by-experimentation. Whereas a new technology is introduced under certain conditions to society.

Such a responsible experiment might reduce epistemic, normative and institutional uncertainty (van de Poel, 2017). Yet, due to a platform's generativity this approach might not account for reducing the uncertainty involving the occurrence of undesirable unknown unknowns. In addition, due to a platforms generativity new users might introduce yet unforeseen risks after small-scale experimentation. Hence more research is necessary in order conceptualize what a responsible platform should look like. A possible avenue is provided by Stilgoe et al. (2013). Whereas Stilgoe et al. argue that the responsiveness of a system is required in situations of changing circumstances. Accepting unknown unknowns and focusing on how platforms should better respond might be more effective in reducing the potential impact on society. Therefore, researching how platforms can be more responsive may be worthwhile in pursuing what a responsible open platform should look like.

References

Adam, B., & Groves, C. (2011). Futures Tended: Care and Future-Oriented Responsibility. *Bulletin of Science, Technology & Society*, *31*(1), 17–27. https://doi.org/10.1177/0270467610391237

AFM. (2019). *A survey of trends and risks on the financial markets*.

Aldrich, H. E., & Ruef, M. (2006). Organizations evolving, second edition. In *Organizations Evolving, Second Edition*. https://doi.org/10.4135/9781446212509

Anvaari, M., & Jansen, S. (2010). Evaluating architectural openness in mobile software platforms. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/1842752.1842775

Archel, P., Husillos, J., Larrinaga, C., & Spence, C. (2009). Social disclosure, legitimacy theory and the role of the state. *Accounting, Auditing and Accountability Journal*, *22*(8), 1284–1307. https://doi.org/10.1108/09513570910999319

Argyris, C. (1976). Single-Loop and Double-Loop Models in Research on Decision Making. *Administrative Science Quarterly*, *21*(3), 363–375.

Argyris, C. (1977). Double loop learning in organizations. *Harvard Business Review*, *55*(5), 115–125. Retrieved from https://hbr-org.tudelft.idm.oclc.org/1977/09/double-loop-learning-in-organizations

Argyris, C. (2002). Teaching Smart People How to Learn. *Reflections: The SoL Journal*. https://doi.org/10.1162/152417302762251291

Argyris, C., & Schon, D. (1978). Organizational learning: A theory of action approach. In *Reading, MA: Addision Wesley*.

Argyris, C., & Schon, D. A. (1974). Theory in Practice: Increasing Professional Effectiveness. *Administrative Science Quarterly*. https://doi.org/10.2307/2391706

Baldwin, C. Y., & Woodard, C. J. (2009). The Architecture of Platforms: A Unified View. Harvard Business School Finance Working Paper No. 09-034. *SSRN Electronic Journal*, *2*(November 2018). https://doi.org/10.2139/ssrn.1265155

Beddewela, E., & Fairbrass, J. (2016). Seeking Legitimacy Through CSR: Institutional Pressures and Corporate Responses of Multinationals in Sri Lanka. *Journal of Business Ethics*, *136*(3), 503–522. https://doi.org/10.1007/s10551-014-2478-z

Benlian, A., Hilkert, D., & Hess, T. (2015). How open is this platform? The meaning and measurement of platform openness from the complementors' perspective. *Journal of Information Technology*, *30*(3), 209–228. https://doi.org/10.1057/jit.2015.6

Bergman, M., Lyytinen, K., & Mark, G. (2007). Boundary objects in design: An ecological view of design artifacts. *Journal of the Association for Information Systems*. https://doi.org/10.17705/1jais.00144

Berzon, A., Shifflett, S., & Scheck, J. (2019, August 23). Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products - WSJ. *The Wall Street Journal*. Retrieved from https://www-wsj-com.tudelft.idm.oclc.org/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990

Boland, R. J., Lyytinen, K., & Yoo, Y. (2007). Wakes of Innovation in Project Networks: The Case of Digital

3-D Representations in Architecture, Engineering, and Construction. *Organization Science*, *18*(4), 631–647.

Bolt, W., & Butler, B. (2017). E-commerce drukt de prijzen. *Economisch Statistische Berichten*, *102*(4753S), 14–17.

Boudon, R. (1981). *The logic of social action : an introduction to sociological analysis*. London: Routledge & Kegan Paul.

Boudreau, K. (2010). Open Platform Strategies and Innovation: Granting Access vs. Devolving Control. *Management Science*, *56*(10), 1849–1872. https://doi.org/10.1287/mnsc.1100.1215

Boudreau, K., & Hagiu, A. (2009). Platform rules: Multi-sided platforms as regulators. In *Platforms, Markets and Innovation* (pp. 163–191). https://doi.org/10.4337/9781849803311.00014

Brodsky, L., & Oakes, L. (2017). Data sharing and open banking. *McKinsey on Payments July*.

Broekhuizen, T. L. J., Emrich, O., Gijsenberg, M. J., Broekhuis, M., Donkers, B., & Sloot, L. M. (2019). Digital platform openness: Drivers, dimensions and outcomes. *Journal of Business Research*, *In press*. https://doi.org/10.1016/j.jbusres.2019.07.001

Cambridge English Dictionary. (n.d.). REPUTATION. Retrieved May 14, 2020, from https://dictionary.cambridge.org/dictionary/english/reputation

Capgemini. (2019). *World Payments Report 2019*. Retrieved from www.worldpaymentsreport.com

CBS. (2016, January 20). Stormachtige ontwikkeling webverkopen. Retrieved March 2, 2020, from https://www.cbs.nl/nl-nl/nieuws/2016/03/stormachtige-ontwikkeling-webverkopen

Chiva, R., & Alegre, J. (2009). Organizational learning capability and job satisfaction: An empirical assessment in the ceramic tile industry. *British Journal of Management*. https://doi.org/10.1111/j.1467-8551.2008.00586.x

Chu, C. I., Chatterjee, B., & Brown, A. (2013). The current status of greenhouse gas reporting by Chinese companies: A test of legitimacy theory. *Managerial Auditing Journal*, *28*(2), 114–139. https://doi.org/10.1108/02686901311284531

Clark, K. B. (1985). The interaction of design hierarchies and market concepts in technological evolution. *Research Policy*, *14*(5), 235–251. https://doi.org/10.1016/0048-7333(85)90007-1

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*. https://doi.org/10.1007/BF00988593

Coutu, D. L. (2002). The anxiety of learning. *Harvard Business Review*, *80*(3), 100–101. Retrieved from https://hbr-org.tudelft.idm.oclc.org/2002/03/the-anxiety-of-learning

Crossan, M. M., Lane, H. W., & White, R. E. (1999). An Organizational Learning Framework: From Intuition to Institution. *The Academy of Management Review*, *24*(3), 522. https://doi.org/10.2307/259140

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/20650322

Dapp, T. (2014). Fintech – The digital (r)evolution. *Deutsche Bank Research*. Retrieved from

www.dbresearch.com

de Bijl, P., & van Leuvensteijn, M. (2017). De invloed van fintech op publieke belangen in het betalingsverkeer. *Economisch Statistische Berichten*, *102*(4753S), 37–42.

De Reuver, M., Sørensen, C., & Basole, R. C. (2018). The digital platform: A research agenda. *Journal of Information Technology*, *33*(2), 124–135. https://doi.org/10.1057/s41265-016-0033-3

De Reuver, M., Verschuur, E., Nikayin, F., Cerpa, N., & Bouwman, H. (2015). Collective action for mobile payment platforms: A case study on collaboration issues between banks and telecom operators. *Electronic Commerce Research and Applications*, *14*(5), 331–344. https://doi.org/10.1016/j.elerap.2014.08.004

DeCew, J. (2018). Privacy. In *Stanford Encyclopedia of Philosophy* (Spring 201). Retrieved from https://plato.stanford.edu/entries/privacy/#RedVsCoh

Deegan, C. (2006). Legitimacy theory. In Z. Hoque (Ed.), *Methodological Issues in Accounting Research: Theories, Methods and Issues* (pp. 161–181). London: Spiramus.

den Butter, F. A. G., & Mallekoote, P. M. (2017). Het publiek belang van innovaties in het betalingsverkeer. *Economisch Statistische Berichten*, *102*(4753S), 19–23.

Doorn, N. (2010). A procedural approach to distributing responsibilities in R&D networks. *Poiesis Und Praxis*. https://doi.org/10.1007/s10202-010-0086-2

Easterby-Smith, M., Crossan, M., & Nicolini, D. (2000). Organizational Learning: Debates Past, Present And Future. *Journal of Management Studies*, *37*(6), 783–796. https://doi.org/10.1111/1467-6486.00203

Eisenhardt, K. M. (1989). Building Theories from Case Study Research Published. *The Academy of Management Review*, *14*(4), 532–550.

Eisenmann, T. R., Parker, G., & Van Alstyne, M. (2009). Opening platforms: How, when and why? In *Platforms, Markets and Innovation* (pp. 131–162). https://doi.org/10.4337/9781849803311.00013

Eisenmann, T. R., Parker, G., & Van Alstyne, M. W. (2008). Opening Platforms: How, When and Why? In *Harvard Business School Working Paper*. https://doi.org/10.2139/ssrn.1264012

European Parliament and Council. (2015). Directive 2015/2366 (Payment Service Directive 2). *Official Journal of the European Union*.

European Parliament and Council. (2016). Directive 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*. https://doi.org/L:2016:119:TOC

Evans, D. S. (2003). The Antitrust Economics of Two-Sided Markets. *SSRN Electronic Journal*, *20*(2). https://doi.org/10.2139/ssrn.332022

Evans, D. S., Hagiu, A., & Schmalensee, R. (2006). *Invisible Engines: How Software Platforms Drive Innovation and Transform Industries*. MIT.

Evans, D. S., & Schmalensee, R. (2010). Failure to launch: Critical mass in platform businesses. *Review of Network Economics*, *9*(4), 0–33. https://doi.org/10.2202/1446-9022.1256

Friedman, B., & Kahn, P. H. (2002). Human Values, Ethics, and Design. In A. Sears & J. A. Jacko (Eds.), *The Human-Computer Interaction Handbook* (pp. 1209–1233).

https://doi.org/10.1201/9781410606723-48

Friedman, B., Kahn, P. H., & Borning, A. (2009). Value Sensitive Design and Information Systems. In *The Handbook of Information and Computer Ethics*. https://doi.org/10.1002/9780470281819.ch4

Friese, S. (2012). Qualitative Data Analysis with ATLAS.ti. *Qualitative Research*. https://doi.org/10.1177/1468794113475420

Garcia, A., & O'Brien, S. (2019, December 7). Uber releases safety report revealing 5,981 incidents of sexual assault. Retrieved March 19, 2020, from CNN website: https://edition.cnn.com/2019/12/05/tech/uber-safety-report/index.html

Gawer, A. (2014). Bridging differing perspectives on technological platforms: Toward an integrative framework. *Research Policy*, *43*(7), 1239–1249. https://doi.org/10.1016/j.respol.2014.03.006

Ghazawneh, A., & Henfridsson, O. (2010). Governing third-party development through platform boundary resources. *ICIS 2010 Proceedings - Thirty First International Conference on Information Systems*.

Ghazawneh, A., & Henfridsson, O. (2013). Balancing platform control and external contribution in third-party development: The boundary resources model. *Information Systems Journal*, *23*(2), 173–192. https://doi.org/10.1111/j.1365-2575.2012.00406.x

Goertz, G., & Levy, J. S. (2007). Explaining war and peace: Case studies and necessary condition counterfactuals. In *Explaining War and Peace: Case Studies and Necessary Condition Counterfactuals*. https://doi.org/10.4324/9780203089101

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Retrieved March 19, 2020, from WIRED website: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611–642.

Grin, J., & Van de Graaf, H. (1996a). Implementation as communicative action: An interpretive understanding of interactions between policy actors and target groups. *Policy Sciences*. https://doi.org/10.1007/BF00138406

Grin, J., & Van de Graaf, H. (1996b). Technology Assessment as Learning. *Science, Technology, & Human Values*, *21*(1), 72–99. https://doi.org/10.1177/016224399602100104

Guo, H., Tang, J., & Su, Z. (2014). To be different, or to be the same? The interactive effect of organizational regulatory legitimacy and entrepreneurial orientation on new venture performance. *Asia Pacific Journal of Management*, *31*(3), 665–685. https://doi.org/10.1007/s10490-013-9361-9

Hagiu, A., & Wright, J. (2015). Multi-sided platforms. *International Journal of Industrial Organization*, *43*, 162–174. https://doi.org/10.1016/j.ijindorg.2015.03.003

Hanseth, O., & Ciborra, C. (2007). Risk, complexity and ICT. *Risk, Complexity and ICT*. https://doi.org/10.4337/9781847207005

Hansson, S. O. (2009). Risk and Safety in Technology. In *Philosophy of Technology and Engineering Sciences* (pp. 1069–1102). https://doi.org/10.1016/B978-0-444-51667-1.50043-4

Henfridsson, O., & Lindgren, R. (2010). User involvement in developing mobile and temporarily interconnected systems. *Information Systems Journal*. https://doi.org/10.1111/j.1365-2575.2009.00337.x

Hoffmann-Riem, H., & Wynne, B. (2002, March 14). In risk assessment, one has to admit ignorance. *Nature*, Vol. 416, p. 123. https://doi.org/10.1038/416123a

Houser, K., & Voss, W. G. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3212210

Jesson, J., Matheson, L., & Lacey, F. M. (2011). *Doing your literature review - Traditional and systematic techniques*.

Karhu, K., Gustafsson, R., & Lyytinen, K. (2018). Exploiting and defending open digital platforms with boundary resources: Android's five platform forks. *Information Systems Research*, *29*(2), 479–497. https://doi.org/10.1287/isre.2018.0786

Kasasbeh, E. A., Harada, Y., & Noor, I. M. (2017). Factors Influencing Competitive Advantage in Banking Sector: A Systematic Literature Review. *Research Journal of Business Management*, *11*(2), 67–73. https://doi.org/10.3923/rjbm.2017.67.73

Katz, M. L., & Shapiro, C. (1985, June 1). Network externalities, competition, and compatibility. *American Economic Review*, Vol. 75, pp. 424–440. https://doi.org/10.2307/1814809

Kim, J. (1999). Causation. In R. Audi (Ed.), *The Cambridge Dictionary of Philosophy 2nd edition* (pp. 125–127). Cambridge, UK: Cambridge University Press.

Kim, L. (1998). Crisis Construction and Organizational Learning: Capability Building in Catching-up at Hyundai Motor. *Organization Science*. https://doi.org/10.1287/orsc.9.4.506

Lawrence, S., & Fernando, S. (2014). *A theoretical framework for CSR practices: integrating legitimacy theory, stakeholder theory and intitutional work*. (January), 149–178.

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*. https://doi.org/10.1016/j.bushor.2017.09.003

Lee, R. D., & Mudge, A. R. (2006). *Reasonable Security: The FTC's Focus on Personal Privacy Initiatives Highlights the Importance of Integrated Information Security Programs*. *1*(7), 643–658.

Lewin, K. (1947). *Understanding Lewin's change management model*. Retrieved from https://www.mindtools.com/pages/article/newPPM_94.htm

Mahoney, J. (2008). Toward a unified theory of causality. *Comparative Political Studies*. https://doi.org/10.1177/0010414007313115

Mahoney, J., & Barrenechea, R. (2019). The logic of counterfactual analysis in case-study explanation. *British Journal of Sociology*, *70*(1), 306–338. https://doi.org/10.1111/1468-4446.12340

McCammon, L. A., Saldaña, J., Hines, A., & Omasta, M. (2012). Lifelong impact: Adult perceptions of their high school speech and/or theatre participation. *Youth Theatre Journal*. https://doi.org/10.1080/08929092.2012.678223

Miles, M., Huberman, A., & Saldaña, J. (2014). An expanded sourcebook: Qualitative data analysis (2nd Edition). In M. B. Miles & A. M. Huberman (Eds.), *Sage Publications* (2nd Editio). https://doi.org/10.1016/0149-7189(96)88232-2

Moore, B. (1966). *Social Origins of Dictatorship and Democracy: Lord and Peasant in the Making of the Modern World*. Boston, MA: Beacon Press.

Mosterd, L. (2019). *The Openness between Platforms. What Changes in an IoT Context?*

Nordmann, A. (2014). Responsible innovation, the art and craft of anticipation. *Journal of Responsible Innovation*, *1*(1), 87–98. https://doi.org/10.1080/23299460.2014.882064

Ondrus, J., Gannamaneni, A., & Lyytinen, K. (2015). The impact of openness on the market potential of multi-sided platforms: A case study of mobile payment platforms. *Journal of Information Technology*, *30*(3), 260–275. https://doi.org/10.1057/jit.2015.7

Parnas, D. L. (1972). On the criteria to be used in decomposing systems into modules. *Communications of the ACM*, *15*(12), 1053–1058. https://doi.org/10.1145/361598.361623

Peterson, K. A., & Bickman, L. (1992). Using program theory in quality assessments of children's mental health services. In H. T. Chen & P. Rossi (Eds.), *Using theory to improve program and policy evaluations* (pp. 165–176). New York: Greenwood.

Philippon, T. (2016). THE FINTECH OPPORTUNITY. *Annual Conference of the BIS*, 1–25.

Poel, I. van de, & Royakkers, L. M. M. (2011). *Ethics, Technology, and Engineering : an Introduction*. Wiley-Blackwell.

Puschmann, T. (2017). Fintech. *Business and Information Systems Engineering*, *59*(1), 69–76. https://doi.org/10.1007/s12599-017-0464-6

Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association*. https://doi.org/10.1162/154247603322493212

ROFIEG. (2019). *30 Recommendations on regulation, innovation and finance - Final Report to the European Commission - December 2019*.

Romanova, I., & Kudinska, M. (2018). Banking and fintech: A challenge or opportunity? *Contemporary Studies in Economic and Financial Analysis*, *98*, 21–35. https://doi.org/10.1108/S1569-375920160000098002

Rysman, M. (2009). The economics of two-sided markets. *Journal of Economic Perspectives*, *23*(3), 125–143. https://doi.org/10.1257/jep.23.3.125

Rysman, M., & Schuh, S. (2017). New innovations in payments. *Innovation Policy and the Economy*, *17*(1), 27–48. https://doi.org/10.1086/688843

Saghiri, S., Wilding, R., Mena, C., & Bourlakis, M. (2017). Toward a three-dimensional framework for omni-channel. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2017.03.025

Saldaña, J. (2013). *The Coding Manual for Qualitative Researchers* (Second Edi). SAGE Publications Ltd.

Schein, E. H. (1993). How Can Organizations Learn Faster? The Challenge of Entering the Green Room. *MIT Sloan Management Review*, *34*(2). https://doi.org/10.1017/CBO9781107415324.004

Schoeman, F. (1984). Philosophical Dimensions of Privacy. In *Philosophical Dimensions of Privacy* (Vol. 21). https://doi.org/10.1017/cbo9780511625138

Schön, D. A. (1984). The reflective practitioner: How professionals think in action. In *The Reflective Practitioner: How Professionals Think in Action*. https://doi.org/10.4324/9781315237473

Schot, J., & Rip, A. (1997). The Past and Future of Constructive Technology Assessment. *Technological Forecasting and Social Change*. https://doi.org/10.1016/s0040-1625(96)00180-1

Schreieck, M., Hein, A., Wiesche, M., & Krcmar, H. (2017). The challenge of governing digital platform ecosystems. In *Digital Marketplaces Unleashed* (pp. 527–538). https://doi.org/10.1007/978-3-662-49275-8_47

Scott, W. R. (2001). *Institutions and organizations* (2nd editio). Thousand Oaks, CA: Sage Publications.

Seawright, J. (2016). Multi-Method Social Science: Combining Qualitative and Quantitative Tools. *Strategies for Social Inquiry*. https://doi.org/10.1017/CBO9781316160831

Sekaran, U., & Bougie, R. (2016). *Research methods for business: a skill-building approach* (7th ed.). Wiley.

Singer, I., Batch, D., Tannock, V., & Wiebusch, P. (2018). *Open banking, privacy at the epicentre*. Retrieved from http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2017-003584&language=EN

Smith, H. W. (1981). *Strategies of social research : the methodological imagination*. Prentice-Hall.

Sosna, M., Trevinyo-Rodríguez, R. N., & Velamuri, S. R. (2010). Business model innovation through trial-and-error learning: The naturhouse case. *Long Range Planning*. https://doi.org/10.1016/j.lrp.2010.02.003

Speer, J. (2012). Participatory Governance Reform: A Good Strategy for Increasing Government Responsiveness and Improving Public Services? *World Development*, *40*(12), 2379–2398. https://doi.org/10.1016/j.worlddev.2012.05.034

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy*, *42*(9), 1568–1580. https://doi.org/10.1016/j.respol.2013.05.008

Stinchcombe, A. (1965). Social structure and organizations. In J. March (Ed.), *Handbook of organizations* (pp. 142–193). Chicago: Rand McNally.

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of Management Review*. https://doi.org/10.5465/amr.1995.9508080331

Sun, P. Y. T., & Scott, J. L. (2003). Exploring the divide – organizational learning and learning organization. *The Learning Organization*, *10*(4), 202–215. https://doi.org/10.1108/09696470310476972

Taebi, B. (2017). Bridging the Gap between Social Acceptance and Ethical Acceptability. *Risk Analysis*, *37*(10), 1817–1827. https://doi.org/10.1111/risa.12734

Teixeira, A. (2009). *Swimming with dolphins: a study on legitimacy processes in the southern California tuna industry* (University of North Carolina). https://doi.org/10.17615/81zz-az92

Tetlock, P. E., & Belkin, A. (1996). Counterfactual Thought Experiments in World Politics. *Counterfactual*

Thought Experiments in World Politics.

Tilling, M. V., & Tilt, C. A. (2010). The edge of legitimacy. *Accounting, Auditing & Accountability Journal*. https://doi.org/10.1108/09513571011010600

Tiwana, A. (2014). *Platform Ecosystems Aligning Architecture, Governance, and Strategy Library of Congress Cataloging-in-Publication Data*. Elsevier Inc.

Tost, L. P. (2011). Legitimacy Judgments. *Academy of Management Review*, *36*(4), 686–710.

Valinsky, J. (2020, January 14). Tinder adds a panic button for dates that go wrong. Retrieved March 19, 2020, from CNN website: https://edition.cnn.com/2020/01/23/tech/tinder-panic-button-safety-tools/index.html

Van Alstyne, M. W., Parker, G. G., & Choudary, S. P. (2016). Pipelines, Platforms, and the New Rules of Strategy: Scale now trumps differentiation. *Hardvard Business Review*. https://doi.org/https://hbr.org/2016/04/pipelines-platforms-and-the-new-rules-of-strategy

van de Poel, I. (2009). Values in Engineering Design. In *Philosophy of Technology and Engineering Sciences* (pp. 973–1006). https://doi.org/10.1016/B978-0-444-51667-1.50040-9

van de Poel, I. (2016). A Coherentist View on the Relation Between Social Acceptance and Moral Acceptability of Technology. In M. Franssen, P. Vermaas, & K. P. Meijers (Eds.), *Philosophy of Technology after the Empirical Turn* (pp. 177–193). https://doi.org/10.1007/978-3-319-33717-3_11

van de Poel, I. (2017). Society as a Laboratory to Experiment with New Technologies. In *Embedding New Technologies into Society* (pp. 61–87). https://doi.org/10.1201/9781315379593-4

Van De Poel, I., & Fahlquist, J. N. (2012). Risk and responsibility. In *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk* (pp. 877–907). https://doi.org/10.1007/978-94-007-1433-5_35

Van De Poel, I., Royakkers, L., Zwart, S. D., de Lima, T., Doorn, N., & Fahlquist, J. N. (2015). Moral responsibility and the problem of many hands. In *Moral Responsibility and the Problem of Many Hands*. https://doi.org/10.4324/9781315734217

van de Poel, I., & Zwart, S. D. (2010). Reflective equilibrium in R & D networks. *Science Technology and Human Values*, *35*(2), 174–199. https://doi.org/10.1177/0162243909340272

van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2019). Privacy and Information Technology. In *Stanford Encyclopedia of Philosophy* (Winter 201). Edward N. Zalta (ed.).

van der Cruijsen, C., Hernandez, L., & Jonker, N. (2017). In love with the debit card but still married to cash. *Applied Economics*, *49*(30), 2989–3004. https://doi.org/10.1080/00036846.2016.1251568

Vaughan, D. (1992). Theory elaboration: The heuristics of case analysis. In *What is a case?: Exploring the foundations of social inquiry*.

Von Hippel, E., & Katz, R. (2002). Shifting innovation to users via toolkits. *Management Science*, *48*(7), 821–833. https://doi.org/10.1287/mnsc.48.7.821.2817

Wessel, M., Thies, F., & Benlian, A. (2017). Opening the floodgates: The implications of increasing platform openness in crowdfunding. *Journal of Information Technology*, *32*(4), 344–360. https://doi.org/10.1057/s41265-017-0040-z

West, J. (2003). How open is open enough? Melding proprietary and open source platform strategies. *Research Policy*. https://doi.org/10.1016/S0048-7333(03)00052-0

West, J. (2007). The economic realities of open standards: Black, white, and many shades of gray. In *Standards and Public Policy* (pp. 87–122). https://doi.org/10.1017/CBO9780511493249.004

Westra, L., & Shrader-Frechette, K. S. (1997). *Technology and values / edited by Kristin Shrader-Frechette and Laura Westra*. Rowman & Littlefield Publishers Lanham, Md.

Wheelwright, S. C., & Clark, K. B. (1992). Creating project plans to focus product development. *Harvard Business Review*, *70*(2), 70–82. Retrieved from https://hbr-org.tudelft.idm.oclc.org/1992/03/creating-project-plans-to-focus-product-development

Wholey, J. (1979). *Evaluation: Performance and promise.* Washington, DC: The Urban Institute.

Williams, B. (1981). Moral Luck. In *Moral Luck*. https://doi.org/10.1017/cbo9781139165860

Wolf, C. J. (1986). *Markets or Governments: Choosing Between Imperfect Alternatives*.

Woutersen, M., Tiesjema, B., Jeurissen, S., de Bruijn, A., Herremans, J., & Hegger, I. (2017). *Producten op de grensvlakken Warenwet-Wet op de medische hulpmiddelen-Biocidenverordening*. Rijksinstituut voor Volksgezondheid en Milieu RIVM.

Yin, R. (2018). Case Study Research and Applications: Design and Methods. In *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications, Inc.

Yoffie, D. B., & Kwak, M. (2006). With friends like these: The art of managing complementors. *Harvard Business Review*.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research*, *21*(4), 724–735. https://doi.org/10.1287/isre.1100.0322

Zimmerman, M. A., & Zeitz, G. J. (2002). Beyond survival: Achieving new venture growth by building legitimacy. *Academy of Management Review*, Vol. 27, pp. 414–431. https://doi.org/10.5465/AMR.2002.7389921

Zittrain, J. (2009). Law and technology - The end of the generative internet. *Communications of the ACM*, *52*(1), 18–20. https://doi.org/10.1145/1435417.1435426

Zwart, S. D., Van De Poel, I., Van Mil, H., & Brumsen, M. (2006). A network approach for distinguishing ethical issues in research and development. *Science and Engineering Ethics*, *12*(4), 663–684. https://doi.org/10.1007/s11948-006-0063-2

Appendix A: Interview protocol

The following interview protocol was used to conduct the interviews with the interviewees for the case. A Dutch translation was used instead of the English version if the interviewee could converse in Dutch.

Protocol question:	**Interview questions:**	**Explanation**	**Propositions:**					
Introduction	*Introduce researcher* *Introduce research goal* *Check and read informed consent* *Ask for permission to audio record interview* *Ask for function and experience within PayNow*		*1A*	*1B*	*2A*	*2B*	*3A*	*3B*
Research question 2: How do platform sponsors adjust openness due to safety risks? **Research question 3: How do platform sponsors adjust openness due to privacy risks?**								
How does the organization learn about safety and privacy risks?	1. What do you consider to be a safety or privacy risk? * OR if applicable misleading, fraud or unfair trade practices or illegal products 1.1 How does the organization identify safety and privacy risks? 1.2 How do you judge a safety and privacy risk? 1.3 How do you remediate/act on a safety and privacy risk?	The first question is asked in order to understand the context of how the organization perceives and identifies safety/privacy risks. Furthermore, understanding how a person judges a risk says something about their beliefs and values (van de Poel & Zwart, 2010). These questions also aim to gather the context on how the organization detects and remediates privacy and safety risks. This is indicatory of the single-loop learning process because it highlights the *normal* process of the organization (Argyris, 1976).						
How do safety and privacy risks affect platform openness?	2. [if applicable] How did safety and privacy concerns affect the initial design of the business model when PayNow started? 2.1 Did you ever identify a safety and privacy risk?	The first question aims to establish the baseline of how privacy and safety affected the initial design of the business. Accordingly, the second question aims to identify how the organization reacted (in decisions and actions) upon identifying a risk. This allows to construct a					X	X

	2.2 Can you tell me what happened as result of identifying this safety or privacy risk? 3. How did this affect the organization?	process on how the organization changes due to a privacy or safety risk. Based on the levels of openness by Ondrus et al. (2015) the impact on what kind of openness is questioned. Furthermore, the questions specifically measure access openness as defined by Karhu et al. (2018). Theory on organizational learning state that the theory-in-use of an organization can be observed from the actions and decisions of the organization (Argyris & Schon, 1978). Hence, the theories of action of an organization can be constructed from the decisions and actions an organization takes after identifying a safety or privacy risk.						
	Checklist of answers: - Which suppliers (web shops) to allow on the platform? - What suppliers can or cannot do on the platform (e.g. how much can they interact with the end customer)? - Which customers (web shop customers) to allow on the platform? - What customers can or cannot do on the platform (e.g. leave reviews or choose certain options)? - How to be compatible with other technology (e.g. WooCommerce)? - What can other developers do and explicitly cannot do via the platform/API/plugin? - What platform to be compatible with?							
Why do safety and privacy risks affect platform openness?	4. Why and when do you address safety/privacy risks? 4.1 (How) did this change over time? 5. In what cases does PayNow consider itself responsible in	Double-loop learning affects an individual's background theories (Grin & Van de Graaf, 1996a). By extend an individual's background theories are part of the organizational background theories (Argyris & Schon, 1978). Background theories exist out of an individual's					X	X

	addressing safety or privacy risks?	belief and value systems (Zwart et al., 2006). These background theories, or theories of action, dictate how an organization behaves and what the norms, strategy and routines of an organization are (Argyris & Schon, 1978). Hence the two question aim to capture the beliefs (descriptive views) and values (normative views) of an individual. Whereas this describes the background theories of the individual.						
What role does (moral or regulatory) legitimacy play in adjusting openness?	6. How did the context (e.g. internal policy) play a role in deciding to address safety/privacy risks? *Checklist for answers (proposition):* - Reputation (1); - Stakeholders (1); - Criticism of customers and stakeholders (1); - Competition (2); - Internal policy/strategy (2); - Peers and expectations (2); - Regulation, rules and standards (1).	Theory on legitimacy theory explains why a threat to legitimacy could trigger certain behaviour from organizations (Suchman, 1995). More specifically a threat to legitimacy is likened to a threat to the organizational continuity. Whereas Argyris & Schön (1978) state that certain conditions such as a crisis are needed to induce double-loop learning. The concept of survival and learning tensions (Schein, 1993; Sun & Scott, 2003) further explain the mechanism of how a perceived organizational threat (i.e. crisis) can induce (double-loop) learning. The threat of or actual criticism by an opinion leader, civil society groups and/or stakeholders can damage/threaten moral legitimacy (Teixeira, 2009). Regulatory legitimacy is threatened if an organization might be or is not compliant with relevant regulations, rules or standards (Aldrich & Ruef, 2006; Guo et al., 2014). Therefore these questions check how the two forms of legitimacy appear as the reason for why double-loop learning occurs.	X	X	X	X		

		In addition, the questions on stakeholders, internal policy, competition, peers and expectations describe the learning and survival tensions in the organization (Sun & Scott, 2003). For example, a competitor getting ahead drives survival tension. In contrast, internal norms such as internal policy could hamper survival tension (i.e. learning tensions). Finally, these questions can be used to infer what to this affected the actions and decisions of the organization.						
Closure	*Ask whether interviewee has anything to add* *Finish interview* *Thank interviewee for time* *State that a transcript will be sent for verification purposes*							

Appendix B: Initial code list

Legend:

- Uppercase codes are highest-categories;
- Sub-categories are denoted by : after a capitalized category;
- Lowercase words are codes.

Codes:
DECISION-MAKING
Decision-making: group
Decision-making: individual
Decision-making: organization
DOUBLE-LOOP LEARNING
Double-loop learning: espoused theory
Double-loop learning: espoused theory: agreement/contract
Double-loop learning: espoused theory: policy
Double-loop learning: moderators
Double-loop learning: moderators: culture, structure and systems
Double-loop learning: moderators: external context
Double-loop learning: moderators: knowledge embeddedness
Double-loop learning: moderators: learning retention
Double-loop learning: moderators: network dynamics
Double-loop learning: moderators: organizational structure
Double-loop learning: moderators: power dynamics
Double-loop learning: moderators: strategy
Double-loop learning: theories-in-use
Double-loop learning: theories-in-use: action/decision
Double-loop learning: theories-in-use: assumption
Double-loop learning: theories-in-use: belief
Double-loop learning: theories-in-use: norm
Double-loop learning: theories-in-use: organizational belief
Double-loop learning: theories-in-use: organizational value
Double-loop learning: theories-in-use: privacy value
Double-loop learning: theories-in-use: role responsibilities
Double-loop learning: theories-in-use: safety value
Double-loop learning: theories-in-use: strategy
Double-loop learning: theories-in-use: value
KNOWLEDGE
Knowledge: combination
Knowledge: externalization
Knowledge: internalization
Knowledge: socialization
LEGITIMACY
Legitimacy: building
Legitimacy: maintaining
Legitimacy: maintaining: monitoring change

Legitimacy: maintaining: monitoring operations
Legitimacy: moral impact
Legitimacy: moral threat
Legitimacy: regulatory impact
Legitimacy: regulatory threat
Legitimacy: repairing
Legitimacy: repairing: act calmly
Legitimacy: repairing: normalization
Legitimacy: repairing: restructuring
PLATFORM OPENNESS
Platform openness: complementary
Platform openness: provider
Platform openness: sponsor
Platform openness: supplier
Platform openness: technology
Platform openness: technology: boundary resource
Platform openness: technology: service provider
Platform openness: user
RISK
Risk: privacy
Risk: privacy classification
Risk: safety
Risk: safety classification
SINGLE-LOOP LEARNING
Single-loop learning: espoused theory
Single-loop learning: espoused theory: agreement/contract
Single-loop learning: espoused theory: policy
Single-loop learning: espoused theory: strategy
Single-loop learning: theories-in-use
Single-loop learning: theories-in-use: action/process
Single-loop learning: theories-in-use: norm
Single-loop learning: theories-in-use: results/assumption
Single-loop learning: theories-in-use: strategy
TENSION
Tension: learning
Tension: learning: group-think
Tension: learning: norms, values, language
Tension: learning: politics and resistance
Tension: learning: receptivity of feedback
Tension: learning: routines/processes
Tension: learning: unilateral control
Tension: learning: valid information production
Tension: survival
Tension: survival: criticism of customers
Tension: survival: criticism of stakeholders
Tension: survival: curiosity/personal satisfaction

Tension: survival: insufficient process/technology
Tension: survival: self-improvement
Tension: survival: threat of competitor
Tension: survival: threat of job loss
Tension: survival: threat of workload
Tension: survival: threat to promotion

Appendix C: Final code list

Codes:
ADJUSTING PLATFORM OPENNESS
CHANGING BACKGROUND THEORIES
Clustering of complaints
Common sense
Corporate social responsibility
Criticism of customers
Criticism of stakeholders
Customer complaints
Data as a commodity
Data leakage
Duty of care
Earlier experience
Espoused theory
Espoused theory: agreement/contract
Espoused theory: compliance policy
Espoused theory: due diligence policy
Espoused theory: privacy statement/policy
Espoused theory: security policy
Existing routines/processes
Financial benefits
Foreign web shop
GDPR enforcement
Incongruencies in due diligence
Incorrect establishment of purchase
Insufficient process/technology
Learning tension
LEGITIMACY AND ORG. MATURITY
Legitimacy building
Legitimacy maintaining
Legitimacy maintaining: monitoring change
Legitimacy maintaining: monitoring operations
Legitimacy repairing
Legitimacy repairing: normalization
Legitimacy repairing: restructuring
LEGITIMACY THREAT INCREASES SURVIVAL TENSION
Legitimacy: moral threat: reputation
Misalignment of values / unknowing
Moral legitimacy
Moral legitimacy: impact
Moral legitimacy: threat
Moral legitimacy: threat: consumer trust
Nature of the product
Negotiating

Norms, values
Opening
Organizational maturity
Partner complaints
Payment percentage
Platform openness
Platform openness: provider
Platform openness: provider: complementor
Platform openness: provider: provider openness
Platform openness: supplier
Platform openness: supplier: control of advertisements
Platform openness: supplier: control of customer service
Platform openness: supplier: country of origin
Platform openness: supplier: due diligence
Platform openness: supplier: max transaction costs
Platform openness: supplier: privacy statement
Platform openness: supplier: product mix
Platform openness: supplier: supplier configuration
Platform openness: supplier: user terms of service
Platform openness: technology
Platform openness: technology: boundary resource
Platform openness: user
Platform openness: user: credit check
Platform openness: user: payment limit
Price of products
Privacy awareness
Profitability of platform
QUESTIONING
Receptivity of feedback
Regulatory ambiguity
Regulatory legitimacy
Regulatory legitimacy: impact
Regulatory legitimacy: impact: investigation
Regulatory legitimacy: threat
Responsibility
Restricting
Risk
Risk appetite
Risk identification
RISK THREATENING MORAL LEGITIMACY
RISK THREATENING REGULATORY LEGITIMACY
Risk: financial
Risk: fraud
Risk: fraud: consumer
Risk: fraud: web shop
Risk: illegal products

Risk: misleading consumers / trade practices
Risk: non-compliance web shop
Risk: privacy
Risk: regulatory/legal risk
Risk: reputation
Risk: safety
Risk: security
Risk: vulnerable group affected
Self-improvement
Social dynamics
Survival tension
Theories-in-use
Theories-in-use: belief
Theories-in-use: norm
Theories-in-use: organizational belief
Theories-in-use: organizational value
Theories-in-use: privacy value
Theories-in-use: results/assumption
Theories-in-use: role responsibilities
Theories-in-use: safety value
Theories-in-use: strategy
Theories-in-use: value
Theories-in-use: value: fairness
Third-party supplier openness
Third-party user openness
Threat of competitor
Threat of regulatory interference
Threat of workload
Type of consumer segment
Type of web shop
Usage of personal data
Web shop marketing
Web shop negligence