



Delft University of Technology

Document Version

Final published version

Licence

CC BY

Citation (APA)

de Reuver, M., & Brandwijk, N. (2026). Platform governance in the face of negative network externalities: a moral and regulatory legitimacy perspective. *European Journal of Information Systems*.
<https://doi.org/10.1080/0960085X.2026.2697811>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

In case the licence states "Dutch Copyright Act (Article 25fa)", this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.

Platform governance in the face of negative network externalities: a moral and regulatory legitimacy perspective

Mark de Reuver & Noah Brandwijk

To cite this article: Mark de Reuver & Noah Brandwijk (08 Jul 2026): Platform governance in the face of negative network externalities: a moral and regulatory legitimacy perspective, European Journal of Information Systems, DOI: [10.1080/0960085X.2026.2697811](https://doi.org/10.1080/0960085X.2026.2697811)

To link to this article: <https://doi.org/10.1080/0960085X.2026.2697811>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.



Published online: 08 Jul 2026.



Submit your article to this journal [↗](#)



Article views: 384



View related articles [↗](#)



View Crossmark data [↗](#)

RESEARCH ARTICLE

 OPEN ACCESS Check for updates

Platform governance in the face of negative network externalities: a moral and regulatory legitimacy perspective

Mark de Reuver  and Noah Brandwijk

Engineering Systems and Services, Delft University of Technology, Delft, The Netherlands

ABSTRACT

When participants on transaction platforms harm others (e.g. fraud, misconduct), it typically takes time before platform sponsors tighten their membership conditions. Although anecdotal evidence exists, platform governance literature does not cover the microlevel processes through which negative network externalities lead to actions to protect the platform. This paper employs an institutional legitimacy lens to theorise how governance processes unfold as platforms encounter negative network externalities. We study PayNow, a payment platform whose governance practices evolved over time as legitimacy pressures accumulated, leading to progressively stricter onboarding and fraud-prevention measures. The study provides exploratory insights into microlevel processes of materialising and spotting externalities, perceiving legitimacy challenges, questioning internal assumptions, trading off legitimacy and growth, and safeguarding the platform. We contribute to platform governance literature by illustrating how governance actions are driven by moral and regulatory legitimacy challenges that stem from diverse forms of negative network externalities.

ARTICLE HISTORY

Received 7 August 2023
Accepted 29 June 2026

KEYWORDS

Digital platforms; platform openness; platform governance; legitimacy; negative network externalities; ecosystem membership

1. Introduction

Businesses that own transaction platforms continuously have to adjust the conditions for buyers and sellers to join the platform (Broekhuizen et al., 2019; Tilson et al., 2010; Wareham et al., 2014). Platform literature suggests that permissive membership conditions help transaction platforms to grow (Ondrus et al., 2015). The underlying logic is that permissive conditions stimulate participants to join platforms, which increases the platform's value for prospective participants, creating a virtuous cycle (i.e., positive network externalities) (Rysman, 2009). Yet, permissive conditions also attract users who engage in harmful behaviour (e.g., fraud or misconduct) (Nash et al., 2017; Zuboff, 2015), thus creating *negative* network externalities (Afuah, 2013). While there is work suggesting that such harm reduces user satisfaction (Cennamo & Santaló, 2019; Wareham et al., 2014; Wessel et al., 2017), the role of negative network externalities is largely overlooked in platform governance literature (Gawer & Srnicek, 2021).

In several anecdotal examples, transaction platforms restrict membership conditions in response to negative network externalities. For example, Uber and Lyft increased screening of new drivers upon reports of sexual assault and dangerous driving (Garcia & O'Brien, 2019). Instagram implemented more stringent age-verification measures as criticism arose over child safety concerns (McMahon, 2022). While these

examples suggest that negative network externalities typically accumulate for some time before a platform sponsor acts, the processes through which platforms come to act on these externalities remain unclear.

To theorise the governance processes in the face of negative network externalities, we propose an institutional legitimacy perspective, which explains why organisations respond to accumulating external pressures (Suchman, 1995). Our core theoretical argument is that platform governance unfolds as a process in which platform sponsors perceive emerging negative network externalities as legitimacy challenges, which build up towards a certain threshold before they take measures to safeguard the platform. While legitimacy as a concept has recently gained considerable traction in platform literature (Ingram Bogusz et al., 2019; Tauscher & Rothe, 2021; Thomas & Ritala, 2021), it has not been applied to theorise the interplay of negative network externalities and actions to safeguard a platform.

This study provides exploratory insights into the governance processes through which platform sponsors deal with legitimacy challenges from negative network externalities. The core concepts used in this study are defined in Appendix A. We focus on transaction platforms because their open and interaction-intensive nature makes them especially vulnerable to immediate negative network externalities, such as fraud. We conduct a case study on payment platform PayNow. Its highly regulated fintech industry provides

a suitable context of regulatory pressures (e.g., financial and privacy regulations) and moral concerns (e.g., vulnerable consumers). PayNow specifically provides a rich example of a company taking various actions to safeguard the platform, for instance by restricting the membership of particular user groups.

In the case of PayNow, legitimacy challenges built up, for instance, through consumer complaints and internal reputational concerns. These legitimacy challenges pushed the platform sponsor to reconsider earlier trade-offs between growth and legitimacy and question internal assumptions on values such as duty of care and fairness. Ultimately, these processes led to actions to safeguard the platform through, for instance, stricter onboarding processes. Our findings show that the way these governance processes unfolded differed between the early and later stages of the platform, as negative network externalities grew and legitimacy was increasingly prioritised over growth and revenues.

The paper contributes to platform governance literature by uncovering the microlevel processes and thresholds through which platform sponsors interpret and respond to negative network externalities. This microlevel perspective complements macrolevel analyses of platform governance (Cennamo & Santaló, 2019; Wareham et al., 2014; Wessel et al., 2017), which describe governance challenges and outcomes, but leave open how platforms arrive at them. Understanding these internal processes matters for researchers seeking to theorise governance dynamics and for practitioners that need to know when and how to act on negative network externalities. In this way, we advance the understanding of platform governance dynamics (Broekhuizen et al., 2019; Gawer, 2014) and link governance actions to regulatory and moral legitimacy challenges caused by negative network externalities.

A background on negative network externalities, platform governance and legitimacy is provided in Section 2. The case study methodology is detailed in Section 3, and Section 4 presents the findings. Next, Section 5 discusses the findings, and Section 6 concludes the paper.

2. Background

2.1. Negative network externalities: behaviour-induced harms on platforms

Negative network externalities have long been considered only within the same user group of a platform. Examples include congestion in telecommunication networks (Asvanund et al., 2004; Liebowitz & Margolis, 1994) or an overload of sellers on marketplace platforms (Boudreau, 2010). In such classic cases, the number of participants exceeds the carrying capacity of the platform.

On today's transaction platforms, negative network externalities shift from same-side capacity-related issues to cross-side behaviour-induced harms. Because these platforms must remain open to generate positive network effects (Parker et al., 2017), they also become vulnerable to participant behaviours such as fraud, spam or misinformation (Cennamo & Santaló, 2019). While capacity-related problems have straightforward fixes (e.g., increasing platform capacity or limiting participation rates), heterogeneous behaviours such as fraud are harder to predict, model and control. An overview of heterogeneous network negative network externalities types is provided in Appendix B.

Although the trade-off between openness and control is a central theme in platform governance (e.g., Wessel et al., 2017; Eisenmann et al., 2009), negative network externalities have not been systematically linked. Much of the literature focuses on positive network externalities (e.g., Rietveld & Schilling, 2021) because they drive platform growth (e.g., Gawer & Cusumano, 2014). In addition to that, business and economic scholars tend to study growth more often than societal impacts. Another explanation is that negative outcomes such as misinformation and security risks, while not new phenomena, have gained increased scholarly and societal attention only in recent years (Van Dijck et al., 2023).

Related work hints at negative dynamics without labelling these as negative network externalities. McIntyre and Srinivasan (2017) suggest mitigating actions for platform sponsors to prevent low-quality, incompatible and badly supported complements from undermining value creation. Henfridsson and Bygstad (2013) discuss negative self-reinforcing mechanisms that lead to platform decline. Similarly, Hanseth et al. (2006) call for research on negative or unintended outcomes of platform evolutions, such as standardisation that causes fragmentation. These studies hint at negative dynamics but do not address how these result from participant actions or lead to governance interventions.

Closest to our argument is Afuah (2013), who suggests that network externalities arising from participant conduct (e.g., opportunistic behaviour) may harm trust in a network and damage the network's reputation. Building on this, we define negative network externalities as participant actions that harm others on the platform. In a transaction platform context, examples include spam, toxic behaviour, free-riding on shared resources and misconduct.

2.2. Platform governance: controlling membership conditions

Platform governance refers to allocating decision rights, control and ownership (Tiwana et al., 2010).

Governance mechanisms can be formal (e.g., rules, policies, procedures) and informal (e.g., norms) (Tiwana, 2014). While governance is typically exercised by platform sponsors, platform participants may resist and reshape interventions (Eaton et al., 2015). Platform governance facilitates value co-creation and enhances ecosystem relationships (Schrieck et al., 2016).

Transaction platforms typically need governance mechanisms in the form of standardised membership conditions (e.g., Adner, 2017; Jacobides et al., 2018). Existing literature emphasises the benefits of lenient membership conditions: accelerated adoption (Van Angeren et al., 2016; Venkatraman & Lee, 2004), increased diversity of offerings (Tiwana, 2014), and strengthened third-party motivation to contribute (Goldbach et al., 2014; Schaarschmidt et al., 2019). The downsides of excessive leniency have largely been considered in terms of choice overload (Boudreau, 2010, see Section 2.1) and reputational loss due to low-quality offerings (Cennamo & Santaló, 2019), both of which call for moderating the level of openness.

In addition to macrolevel analyses on the trade-offs involving openness versus control, we focus on the microlevel governance processes of spotting emerging externalities, revisiting internal assumptions and safeguarding the platform. We conceptualise the governance actions through which platform sponsors restrict membership conditions (e.g., by tightening onboarding requirements for a specific user group) as ‘securing’ the platform. We borrow this term from Ghazawneh and Henfridsson (2013) as an umbrella concept encompassing safeguards that restrict or control platform access, such as curating transactions (Cusumano et al., 2019) or setting conditions for participation of sellers on a platform (Eisenmann et al., 2009).

2.3. Moral and regulatory legitimacy as a theoretical lens

To explain why platform sponsors react to negative network externalities, we adopt an institutional legitimacy perspective. Rather than developing a new theory, we draw on established accounts of how legitimacy pressures shape organisational action (Suchman, 1995). Legitimacy refers to ‘a generalised 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’ (Suchman, 1995, p. 574).

A core idea in Suchman’s (1995) foundational work on institutional legitimacy is that legitimacy challenges build gradually, driven by accumulating pressures such as regulatory scrutiny or customer dissatisfaction. Only once a threshold is reached, is the

organisation compelled to preserve or repair legitimacy. In the platform context, negative network externalities can accumulate and challenge legitimacy until a threshold is reached that prompts corrective governance measures.

We anchor our lens in two widely used, complementary frameworks. First, Suchman (1995) distinguishes pragmatic, cognitive and moral forms. Pragmatic legitimacy rests on self-interested evaluations of whether an organisation delivers benefits. In platforms, this corresponds to platform adoption, growth and positive network externalities, which have been well theorised (e.g., Rysman, 2009). Cognitive legitimacy reflects that outsiders take an organisation for granted and it gradually evolves over time, making it less relevant for explaining short-term governance responses. In contrast, moral legitimacy concerns normative evaluations about whether the organisation ‘does the right thing’, making it highly relevant for negative network externalities such as fraud, misconduct and harm.

Second, building on Suchman (1995), Scott (2001) anchors legitimacy in three institutional pillars: regulative, normative and cultural-cognitive. Moral legitimacy aligns with the normative pillar, while cultural-cognitive legitimacy relates to shared understandings that change only gradually. The regulative pillar, however, reflects conformity with formal laws, rules and governmental oversight, which is relevant as negative network externalities attract regulatory scrutiny.

Both moral and regulatory legitimacy represent the sociopolitical pressures on platforms (Aldrich & Ruef, 2006). Moral legitimacy is evaluated by the public and societal stakeholders, while regulatory legitimacy is granted by state and institutional authorities (Teixeira, 2009). They are not mutually exclusive: regulatory processes extend well beyond what is considered morally right or wrong (Aldrich & Ruef, 2006, p. 186).

Platform research has historically treated legitimacy primarily as a precondition for growth and scaling. Early studies focused on how platforms must gain legitimacy to attract users (Ansari et al., 2016; Autio & Thomas, 2016), build ecosystems (Iansiti & Levien, 2004) and function as platform leaders (Cusumano & Gawer, 2002). Governance-related strategies for legitimacy similarly focus on ways for platforms to grow, such as partnering with reputable actors (Taeuscher & Rothe, 2021), relinquishing technical control (Khanagha et al., 2020), decentralisation (Singal, 2021) and continuous adaptation (Garud et al., 2022). Studies also show how legitimacy crises lead to actions by platform sponsors (Casini, 2018), such as communication (Peng et al., 2019).

Only more recently, as platforms have become contested by public criticism and regulatory oversight, have scholars turned to moral and regulatory

legitimacy as central concerns (Taeuscher & Rothe, 2021; Uzunca et al., 2018). Few scholars explicitly analyse how negative network externalities create acute pressures that prompt sponsors to safeguard their platforms (Uzunca et al., 2018). This gap partly reflects that platform research has been dominated by questions of market adoption and scaling, with less attention to governance once platforms are established. Addressing this gap, we focus on moral and regulatory legitimacy because they are the forms that generate acute pressure to act when harms accumulate. This perspective allows us to theorise governance not merely as a growth enabler but as a corrective and preventive response to threats to a platform's licence to operate.

3. Methodology

The case study method is suitable for our research purposes for several reasons. First, as we theorise the microlevel processes of governance responses, longitudinal data is required. Second, negative network externalities and legitimacy challenges are highly context-specific, requiring an in-depth understanding that cannot be separated from the real-life context (Yin, 2018). Third, while we aim to theorise in an exploratory fashion, we use the concepts from Section 2 as a foundation, which is a common practice in case study research (Eisenhardt, 1989). The remainder of this section discusses case selection (3.1), theoretical boundary conditions of the case (3.2), data collection (3.3) and data analysis approach (3.4).

3.1. Case selection

We adopt an embedded case study design (Yin, 2018) to investigate events in which a platform sponsor adapted its membership conditions. Our focal case is PayNow: a digital platform sponsor based in the Netherlands, providing payment solutions for webshops and consumers. As their platform mediates between two user groups through digital technologies, it fits our definition of a transaction platform (see Appendix A).

PayNow was selected for three reasons. First, the platform applies a moderate level of membership conditions. Webshops have to pass an approval procedure, while consumers are subjected to a credit check. This makes PayNow neither completely open nor fully closed, providing a fertile ground for examining governance processes. Second, informal discussions with PayNow's IT manager revealed that the company decided to stop serving particular webshops, as they sold products in a way that was unacceptable to the PayNow directors. Hence, we expected to find more instances of PayNow adjusting its membership conditions upon learning about negative network

externalities. Third, after its launch in 2010, the platform grew significantly. This growth enabled the study into how governance processes change over the course of developing and growing the platform.

3.2. Theoretical boundary conditions

Our case is a fintech platform, situated in the financial payment service sector during the period 2013–2018. Fintech platforms face particular regulatory standards concerning anti-money laundering, capital, security and privacy (Jagtiani & John, 2018; Lee & Shin, 2018). Regulatory legitimacy pressures can emerge even before formal rules are enforced, as organisations anticipate looming regulatory requirements (cf. Suchman, 1995). In our case, two major EU regulations were announced in 2016 and came into force in 2018: the revised Payment Service Directive (PSD2) (2018) and the General Data Protection Regulation (GDPR). The announcement of these regulations increased expectations for payment providers to prevent fraud (Polasik et al., 2020) and protect user data (Lee & Shin, 2018). The announcement of the GDPR also increased societal attention to the moral issues surrounding privacy. A relevant boundary condition is thus that regulatory and moral standards intensified during the study period, which may have amplified legitimacy pressures compared to less regulated platform contexts.

3.3. Data collection

We use interviews as a main data source, complemented by internal documentation to triangulate findings on governance outcomes (Miles et al., 2014). Documents were especially used to capture the outcomes of formalised governance actions (e.g., updated terms and conditions), while interviews were most suitable to understand the governance processes leading to those changes. The key informant initially provided twelve documents. During the interviews, additional documents were requested when mentioned by respondents, allowing us to retrieve different versions of the platform's terms of use and internal reports on strategy changes. This enabled us to track how formal membership conditions evolved over time (Appendix C).

We selected a diverse set of interviewees from strategic and operational levels. They either (1) decided upon generic platform membership policies, (2) were in charge of admitting or rejecting participants, or (3) onboarded new participants to the platform. Interviewees were identified through talks with the key informant. Saturation was achieved when no new aspects or events emerged in the final interviews and

documents. Appendix D provides an overview of interviewees and the duration of each interview.

Interviews were conducted in 2020 via video calls, lasting 47 minutes on average. Eleven interviews were recorded (with informed consent) and transcribed. Interviewees verified transcripts, upon which recordings were destroyed. Each transcript is between ten and twenty pages.

Interviews were semi-structured, tailored to the interviewee's expertise. We started with generic questions on how respondents identified, judged and remediated negative network externalities. Negative network externalities were explained to be issues or risks external to the company, such as privacy, fraud or safety. Respondents were asked how these issues and risks affected the initial business model design.

Next, interviewees were asked to recall specific instances in which they identified a potential externality. By going into specific instances, we intended to collect authentic information on the lived experience of participants (Schultze & Avital, 2011). Interviewees were asked what had happened and how this affected the organisation. To steer the discussion towards governance, helping questions were asked about how the externality affected decisions regarding which suppliers, customers and developers were allowed on the platform and what these parties were allowed to do.

After discussing specific instances, interviewees were asked about their general approach to assessing externalities, how this changed over time, and the extent to which they find PayNow to be responsible for externalities. Follow-up questions were asked to pinpoint the timing of events and changes in PayNow's approach. Finally, to understand the role of legitimacy challenges in general, questions were asked about the impact of the contextual environment, for instance, reputation, stakeholders, critique from customers and stakeholders, competition, peer expectations and regulatory standards.

3.4. Data analysis

To systematically analyse how governance approaches evolved in response to legitimacy challenges and negative network externalities, we combine thematic analysis using the 'Gioia' methodology (Gioia et al., 2013) with processual analysis using temporal bracketing (Langley, 1999). While few IS studies have combined these particular methods (e.g., Fürstenau et al., 2019; Ofte & Sandberg, 2023), doing so allows a firm rooting in the data while tracing the dynamic interplay of microlevel governance processes over time.

We first applied the Gioia methodology to identify the main microlevel governance processes. The resulting aggregate dimensions are expressed as gerunds (e.g., spotting potential externalities), reflecting their processual nature. Next, we conducted temporal

bracketing to explore how the interactions between these processes evolved over time. For instance, while the Gioia analysis identified *spotting potential externalities* and *questioning internal assumptions* as key themes, temporal bracketing revealed that their relationship changed: in early phases, the former did not lead to the latter, but in later phases, their interaction became a driver of governance adaptation. By conducting the Gioia analysis prior to temporal bracketing (similar as in Rinta-Kahila et al., 2022), we ensured that the governance processes were grounded in our empirical data before establishing their temporal relevance.

Figure 1 provides an overview of the steps completed within each analysis method.

3.4.1. Gioia approach

To guide the initial coding process, we developed 91 preliminary codes based on concepts of legitimacy building, moral and regulatory legitimacy, and governance conditions for consumers, providers and complementors. The preliminary codes served as a starting point rather than a final structure, allowing flexibility for new insights to emerge from the data. This approach aligns with qualitative best practices, where theoretical concepts inform but do not constrain the analysis (e.g., Gioia et al., 2013; Saldaña, 2013).

As a first sub-step, we conducted open coding to capture themes beyond the preliminary codes, expanding the coding scheme to 253 codes. Coding was done by the second author and checked by the first author. Some quotations were assigned multiple

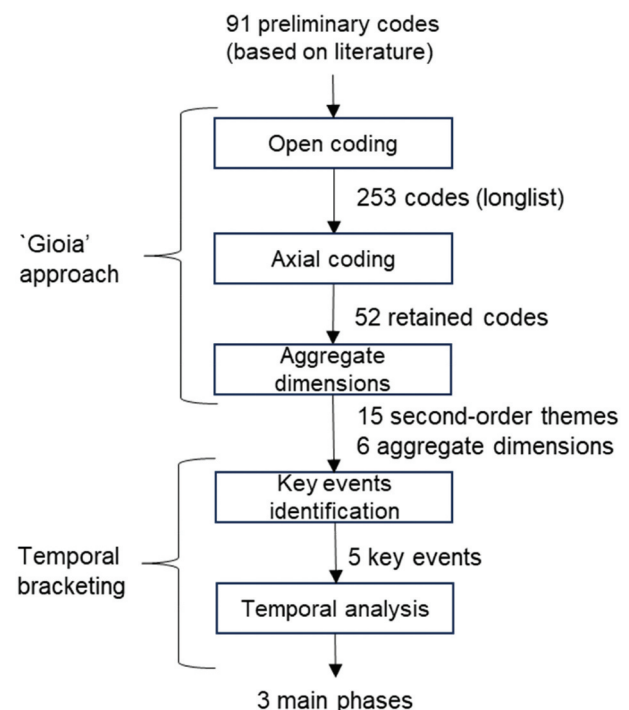


Figure 1. Analysis approach.

codes to reflect their complexity. For instance, the quotation ‘But if you suddenly receive ten calls about webshop X [...] At some point it will simply stand out’ was assigned codes ‘Clustering of complaints’ and ‘Criticism from customers’. The approach allows descriptive labels that remain close to the informants’ language, which helps to incorporate the multiplicity of perspectives within PayNow.

In a second sub-step, we applied axial coding to refine the structure, merging overlapping or redundant codes and removing infrequently mentioned ones. This process reduced the coding scheme to 52 retained codes. Throughout, we documented our decisions using analytical memos (Saldaña, 2013), which helped track the evolution of themes and ensure transparency.

In the final sub-step, codes were further developed into aggregate dimensions (Gioia et al., 2013). Although often applied to theory development, the ‘Gioia’ approach was used here to explore the micro-level governance processes that relate to key concepts (e.g., legitimacy, negative network externalities). To identify causal and conditional relationships (i.e., “if-then” relations) among the codes (Saldaña, 2013), network diagrams were constructed to visualise connections. For instance, we examined how concerns over negative network externalities (e.g., fraudulent sellers) interacted with internal assumptions. These relationships were verified by re-reading coded quotations and reviewing full transcripts where necessary. This sub-step yielded a set of six aggregate dimensions that disentangle the microlevel processes, for instance distinguishing between observing negative network externalities, perceiving legitimacy challenges, questioning internal assumptions and making trade-offs.

To ensure robustness, the third sub-step was reiterated by the first author, who reviewed all codes and categories, returning to the original quotations. Following the reiteration, the labels of most first-order concepts were expanded to be more descriptive. Further, second-order themes were refined. For instance, the broadly formulated theme ‘Maturity’ was relabelled as ‘Startup/scale-up’. Aggregated dimensions were also reformulated as gerunds to reflect their role in the process of governance adaptations.

Figure 2 provides an overview of the codes, categories and aggregate dimensions.

3.4.2. Temporal bracketing

Temporal bracketing began by identifying key events that could serve as units of analysis, representing episodes where platform access conditions were modified (e.g., policy updates, enforcement actions). For each event, we reviewed the relevant codes and aggregate dimensions to understand their interactions. For

example, we examined how the observation of negative network externalities (e.g., fraud reports) interacted with legitimacy perceptions (e.g., receptivity to feedback) and internal assumptions (e.g., importance of fairness) to shape governance responses (e.g., code of conduct). An overview of these events, along with associated evidence and codes, is provided in Appendix E. Appendix F summarises negative network externalities, legitimacy challenges, and changes in membership conditions for each event.

Next, we mapped these events onto a timeline (see Appendix G) and inductively grouped them into three phases, each characterised by distinct patterns of interaction among microprocesses. For instance, Phase 1 was marked by the emergence of awareness around negative network externalities, but these observations did not yet challenge internal assumptions or prompt governance action. In contrast, Phase 3 saw proactive governance actions, where spotting externalities directly informed policy adjustments and trade-off decisions. To define the phases, we zoomed in on interviewee responses to questions such as: “Can you describe how the organisation’s approach to [theme] evolved?” and “When did you first notice a shift in [process]?”, and follow-up questions such as “Was this different before?” and “What triggered this change?”. In this way, the phase definitions were empirically grounded in informant accounts, aligning with Langley’s (1999) suggestion of endogenous processual analysis.

Following Langley (1999), we view the phase transitions as gradual and endogenous, driven by internal dynamics rather than external shocks. While regulatory changes and external audits occurred during the study period, interviewees consistently reported that these did not trigger abrupt changes in the way they dealt with platform governance. For example, one interviewee noted: “The realisation that people were reading about privacy became important as early as 2013/2014, well before GDPR” (IN10). Instead, shifts emerged from cumulative internal changes, such as the maturing of the organisation or growing awareness of societal concerns.

While comparing the phases, we found that interviewees used terms such as early stages, maturation and professionalisation to describe how the organisation changed. For instance, interviewees commented that, since around 2016, they had gone through stages of ‘professionalisation’ (IN3), introducing the new roles of compliance and privacy officers. The later phases also show increased financial stability with less dependence on short-term revenues to survive, which indicates that typical start-up stage vulnerabilities had diminished. Following Langley (1999), we do not strictly delineate early versus mature stages but use these terms to capture the company’s gradual professionalisation and internal capability development,

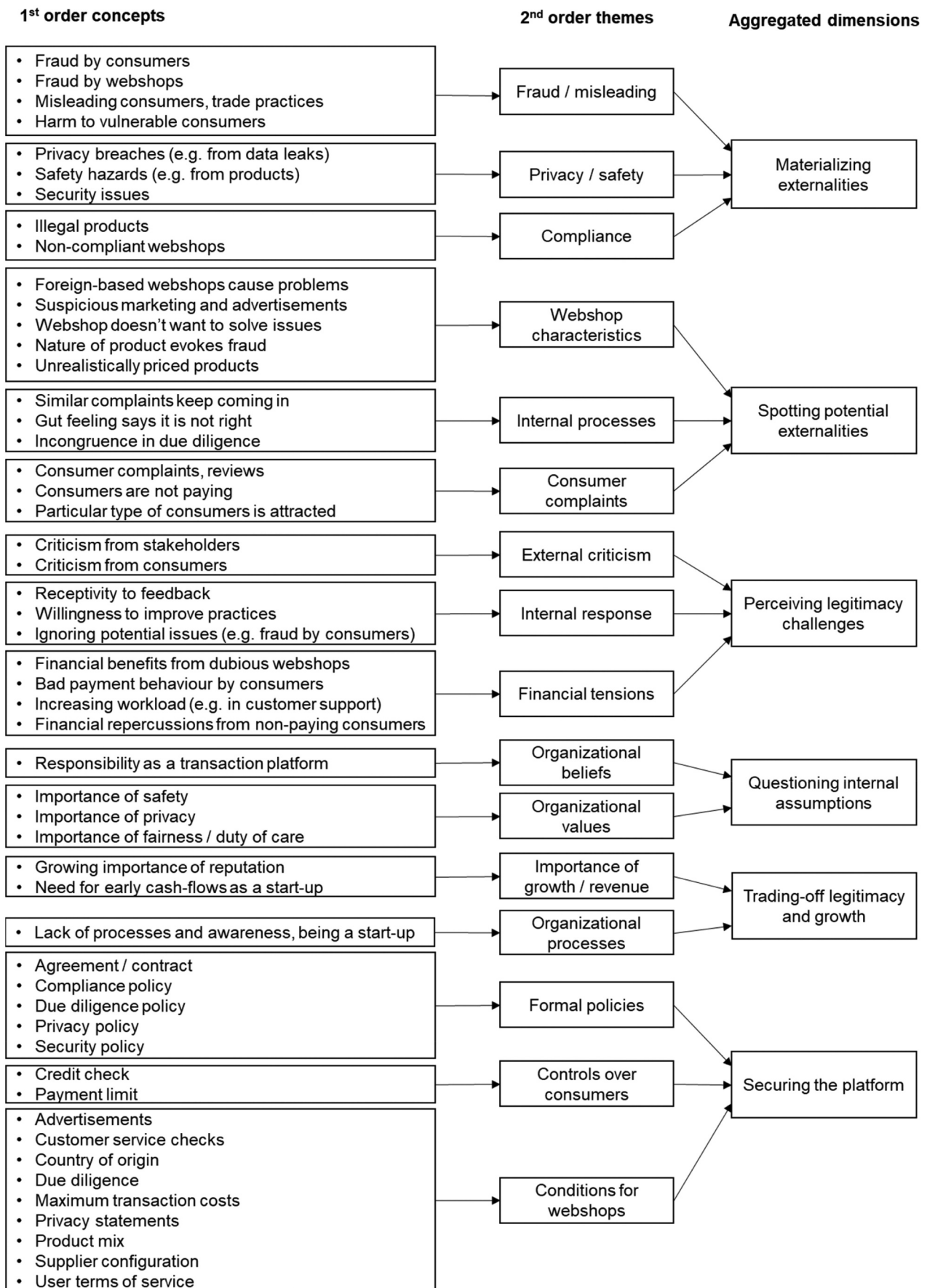


Figure 2. Coding structure and aggregated dimensions.

which shaped how governance processes responded to emerging negative network externalities.

4. Findings

4.1. Phase 1: selective legitimacy responses to negative network externalities (2013–2016)

In the first phase, PayNow prioritised growth and revenue generation over legitimacy. Therefore, negative network externalities (e.g., fraudulent return processes) were spotted but rarely prompted governance responses to secure the platform. One notable exception was the appointment of a privacy officer, although this action did not come at the expense of growth or revenue.

4.1.1. Materialising and spotting externalities

In *Event 1*, negative network externalities materialised as fraudulent webshops used foreign return addresses to make returns impractical and costly for consumers (interview: IN3). For instance, some webshops required consumers to return goods to China. PayNow had no return address policy at the time (IN1). PayNow noticed consumers were increasingly failing to fulfil their payment obligations, thus spotting this as a potential negative network externality (IN3).

Privacy-related externalities were spotted as a potential risk, even though they did not materialise (*Event 4*). Overall, PayNow had always taken care to minimise data collection in view of privacy: 'We always collected everything [data] we needed and not much more than that. Practically no adjustments have been made to this in recent years'. (IN2). Yet, for consumer identity validation services from third parties, PayNow did share more personal data (e.g., name and address) than was technically needed. Doing so resulted in a lower tariff and was thought to benefit consumers, assuming the shared data is not further enriched by the external parties: 'From the moment that your data is in a [third-party] database, others can validate [you], that then gives you only the opportunity to use services that you otherwise couldn't use'. (IN2). However, consumers started to ask customer service about their privacy, which made PayNow aware of potential negative network externalities. Looking back at these changes, an interviewee commented: 'Then we also get the first people who reported to customer service. And asked what data do you actually have? So how is such a credit check utilised? And how do you actually do that, how do you analyse me?' (IN10). This led to a revelation on the side of the decision-makers: 'And then actually for the first time we thought, yes, what is our role in this?' (IN10). Notably, no large-scale privacy breaches happened at third-party service providers, suggesting that negative network externalities did *not* actually materialise.

4.1.2. Building up legitimacy challenges, questioning assumptions and trade-offs

In the return address policy example (*Event 1*), regulatory legitimacy challenges did not emerge, as Dutch law does not require a domestic return address (IN1). In terms of moral legitimacy, PayNow's position was that they should remain neutral: 'I don't think that we should want to play a police officer. To go a random webshop and tell them: you are doing something right or wrong'. (IN11). These assumptions were not questioned internally, as PayNow prioritised growth over legitimacy concerns, as an interviewee commented: 'That's because in the past we were simply dependent [on foreign webshops]'. (IN3).

In contrast, in the privacy example (*Event 4*), moral legitimacy challenges did build up considerably. Internally, awareness of potential privacy risks increased as the company worked extensively with personal data (IN11). Externally, interviewees point to changing societal values on privacy as voiced on television and fora, legal scholar opinions and competitor practices (IN1). One interviewee explains how internal and external norms interacted: '[In the early days,] we mainly looked into: how can we make a business out of this? And in the recent years it is more like: what are you allowed to do? And what can you do? So there has been a real change in thinking. Both in society and at the company [...]. It is simply society who asks for [privacy measures], for our company that is therefore important. [...]' (IN10). These concerns also personally resonated with this interviewee: 'I personally don't want my data to be available because I have seen what can happen to data at other businesses, and how often data is sold behind your back. For me, it's like: I don't want that happening in my company'. (IN10). In this way, changing societal values created moral legitimacy pressures that led to internal discussions on assumptions.

The internal debate affected how PayNow made trade-offs between negative network externalities (i.e., potential privacy risks) and growth-related goals: 'So you see that the privacy regulation and privacy/safety can sometimes stand in the way of the ambitions of a company'. (IN1).

Regulatory legitimacy did not majorly affect the privacy-related changes in conditions for third-party validation services. Privacy was already on the company's agenda in 2013, well before the GDPR was introduced (IN10). When the regulation was announced, some products were re-evaluated for compliance (IN10) but nothing major had to be changed (IN11).

4.1.3. Securing the platform

In the case of the return address policies, no major actions were taken to secure the platform, as negative

network externalities from fraudulent sellers did not outweigh growth and financial gains. Such actions only happened in Phase 2, where *Event 1* continues to unfold.

In contrast, privacy-related policies were tightened in response to internal debate and trade-offs between legitimacy and growth (*Event 4*). A privacy officer was appointed to check compliance with privacy authority guidelines (IN10). More importantly, PayNow retained a selected set of third-party providers for identity validation (IN2, IN3), with the strict requirement that consumer data 'may only be added to their own validation service and may not be used to enrich data for other parties' (IN2). In this way, PayNow unilaterally tightened the conditions for third parties as a governance response.

While *Event 1* suggests that financial growth is prioritised over legitimacy concerns, *Event 4* shows a gradual shift towards catering for legitimacy. From the discussions with interviewees, it is clear that, during this time period, privacy issues resonated more within the organisation than fraud-related ethical considerations.

4.2. Phase 2: legitimacy responses to escalating negative network externalities (2016–2017)

As the second phase starts, negative network externalities intensify, especially from foreign and dubious webshops. Unlike *Phase 1*, where growth dominated decision-making, PayNow started to question long-held assumptions about their responsibility as a platform. Consequently, legitimacy challenges started to weigh more heavily, leading to incremental changes to platform membership conditions.

4.2.1. Materialising and spotting externalities

Negative network externalities continued to materialise and escalate, as PayNow became more sensitive to the risks posed by certain product categories and merchants. In the return address policy case (*Event 1*), PayNow increasingly spotted negative network externalities as employees started to realise that foreign-based webshops in particular were causing problems with consumer payment (IN3).

New sources of negative network externalities also started to materialise. For instance, smart shops had started to sell psychoactive substances (*Event 5*). PayNow observed that smart shop products attracted a particular type of consumer with worse payment behaviour (IN4, IN6). Similarly to *Event 1*, this worse payment behaviour was a trigger to ask questions: 'Why don't those consumers pay? Are they being lured by that webshop, or is it that the products are not good? Or is there more to it?' (IN1). Besides having worse payment behaviour, customer service employees also noticed consumers who buy from

smartshops are difficult to reason with on the phone: 'It attracts a certain type of people. I'm not sure if that is immoral. But it is practically not doable'. (IN4). PayNow started to observe suspicious marketing and advertisements, and employees doubted whether these complied with the regulation (IN6).

4.2.2. Accumulating legitimacy challenges, questioning assumptions and trade-offs

Across this phase, PayNow's growing financial stability allowed for reassessing the trade-offs between growth and legitimacy challenges. Moral challenges started to weigh more heavily as reputation was becoming more important than growth and financial gains. For instance, PayNow no longer wanted to serve dubious webshops that were rejected by its competitors: 'Of course, we do not want to be noted as a party that services rejected customers of our competitors. That if you do not pass the due diligence at [competitor 1, competitor 2], you can still knock on PayNow's door to become a customer there. We also do not need that anymore now, I think. We have a very healthy sales volume. Reputation has to do with that too. We have certain things we want to expose both internally and externally, and noncompliant shops of course do not fit that'. (IN4)

Even though legitimacy concerns still barely played a role in the return address policy case, PayNow did change its internal assessment of duty of care and fairness. Moral legitimacy concerns did not fundamentally change. However, because of increasingly bad payment behaviour by consumers, financial gains were fading (IN11), and thus the trade-off in favour of legitimacy concerns became easier to make. Consequently, the platform sponsor changed its internal assumptions, deciding that foreign return addresses violated the value of fairness and duty of care towards consumers (IN1).

In the case of the smart shops (*Event 5*), PayNow faced both severe regulatory and moral legitimacy concerns that led to internal debates on its position as a transaction platform. The moral challenges started to weigh more heavily, as reputation was becoming more important. Regulatory legitimacy pressures did increase, however, as PayNow perceived regulations to be vague and subject to change (IN4, IN6), making it difficult to keep up with and scrutinise the suspicious offerings of smart shops. Interviewees refer to the smart shop case as a 'grey area' legally.¹ These regulatory legitimacy concerns were reinforced as an external collection agency did a due diligence check on a smart shop and identified illegal products (IN4, IN9).

The regulatory concerns affected PayNow's internal assumptions. Initially, PayNow felt responsible for fair sales processes rather than the actual products being sold: 'Does this fulfil the law or what we want? That is

not our task at all [...] In principle, if the law allows it, then who is PayNow to put moral question marks to it?' (IN4). With the unclear and shifting regulations, this assumption was challenged, expanding the scope of duty of care to the products being sold by webshops. Manually checking products was considered unfeasible though, costing too much time in relation to the sales volume (IN4).

Moral legitimacy concerns also accumulated, as PayNow started to realise what activities could be done with smart shop products. 'From the moment that it can be used for [large-scale illegal activities], I feel you should ask yourself whether it is ethical to further illegal money-streams or at least sustain them'. (IN6). Moral legitimacy concerns also grew through critique from internal stakeholders, such as customer service employees. In this sense, bad payment behaviour by consumers played a role in this example as well, but this time creating moral legitimacy concerns rather than causing significant financial harms (IN4, IN6).

4.2.3. Securing the platform

PayNow took responsive actions to secure the platform in this phase by adjusting its membership conditions and policies. For the return address issue (*Event 1*), PayNow introduced a new requirement for local return addresses in its compliance policy and supplier conditions, even though it was not legally mandated (document: D4). This action stemmed from a shift in internal assumptions about what duty of care towards consumers means, but also from a changing trade-off between growth and legitimacy as PayNow became less dependent on dubious webshops.

The smart shop case (*Event 5*) led to a more decisive change, as PayNow changed its product mix requirements and due diligence process in such a way that smart shops stopped using the platform (IN6). Both moral and regulatory legitimacy concerns played a role. Moral concerns triggered fierce internal debate over the assumptions of the company. 'One was pro and the other didn't agree. Yes, I think everyone had an opinion on that. [Account managers] see, of course, many orders coming in [...] But well, the other people don't want a lot of hassle again'. (IN8). Regulatory legitimacy pressures played a role as PayNow found it would be virtually impossible to ensure that every order made via the platform is compliant (IN4; IN6; IN9) due to rapid changes in regulation (IN6) and offerings by smart shops (IN4).

4.3. Phase 3: proactively securing for legitimacy gains (2017–2018)

In the final phase, legitimacy clearly takes priority over growth and revenues, as PayNow starts focusing on

long-term outcomes. The phase further exhibits increasingly proactive governance mechanisms to secure the platform, such as a strategy for stricter onboarding that materialised at the end of 2017.

4.3.1. Materialising and spotting externalities

In this phase, PayNow was increasingly able to identify negative network externalities through financial impacts as well as internal and external criticism. Two events dominate this period, with new sources of negative externalities that both relate to fraud.

Consumer fraud (*Event 3*) was spotted as consumers refused to pay or complained about invoices, especially for high-value products such as smartphones and barber equipment (IN5, IN9, IN11). For instance, consumers ordered goods using a neighbour's address and obtained the package without paying, while the neighbour would understandably refuse to pay an invoice for a product that they never ordered (IN8). PayNow realised the size of the fraud only after they took on the insurance of payment defaults, which was previously outsourced. In the words of one interviewee, the fraud became tangible and concrete for the first time: 'Then we suddenly had to look into fraud and that turned out to be a bigger problem than we initially thought. We knew it would be a problem but we just underestimated all of that'. (IN5).

Around the same period, an increasing and disproportionate number of consumer complaints were received regarding a select group of webshops selling nutritional supplements (*Event 2*; IN1, IN5, IN7, IN8, IN9). These were advertised as 'free' to try, but once consumers opened the sample packages, they were obliged to pay. This practice led to complaints directed at PayNow (IN1). The number of complaints was disproportionate to other clients (IN5) well before 2018. Over time, the complaints started to cluster noticeably around individual webshops (IN5; IN7; IN8; IN9): 'Half [of all the complaints] were just about the [dubious webshops]. 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). Complaints kept coming in, also after PayNow contacted the webshops to resolve the issues (IN7).

4.3.2. Accumulating legitimacy challenges, questioning assumptions and trade-offs

The negative network externalities created financial risks as well as moral legitimacy concerns related to reputation and internal and external criticism. PayNow's financial stability allowed it to resolve the trade-off of growth and morality, prioritising moral legitimacy over profitability.

In the case of consumer fraud (*Event 3*), moral legitimacy challenges grew and led PayNow to

question its assumptions about their responsibility as a transaction platform: 'We started to look more, are they selling products that attract much fraud. Previously, we never did that because it was never our problem'. (IN5). Reputational concerns emerged as well: 'From the moment that we accept orders unthinkingly and they then remain uninsured and that the products purchased through one of our customers are privately resold before payment is made. Yes, then it is, of course, a small step towards the media to indicate that we are negligent in conducting thorough creditworthiness checks'. (IN7). Some employees even advocated for preventing fraud to differentiate themselves from competitors. Interviewees did point out that it was not only a matter of moral and reputational concern, as taking over the insurance of payment defaults meant that they also started to suffer direct financial repercussions (IN5).

In the dubious webshops case (*Event 2*), PayNow had to forego its initial intention to remain neutral on merchant compliance. Initially, moral legitimacy concerns grew through criticism from consumers through reviews, complaint sites, emails and calls. PayNow even became a topic of discussion on a widely used public complaint forum. 'There were so many complaints on the Internet at one point, we really had to do something about that to repair our reputation. And that was a very good argument, of course, in that whole decision to stop doing business with them'. (IN2). Other external stakeholders provided similar criticism. For instance, partner CollectPay directly contacted non-paying consumers and received many complaints (IN2).

Internal criticism emerged too, especially from the customer service, legal and support departments owing to their increasing workload (IN1). 'I think [the complaints] certainly played a part in the decision. Because it was negative from all sides. Also from service desk employees'. (IN8). The criticism was not shared by all departments and individuals, though. As one interviewee recalled, the sales department maintained that it was not their job to care if webshops acted legally.

Interviewees explain that PayNow directors did not agree on whether to act, as they still had different views on their responsibility as a transaction platform. To resolve the disagreement, they commissioned an internal due diligence and compliance investigation: 'The trigger was disagreement within the board about a specific customer'. (IN1). This investigation showed evidence of misleading consumers and pointed out that there could be legal and reputational repercussions. As the compliance officer noted to the directors: 'Please note that you have a reputation risk here by being associated with this party [...]' (IN1). At this point, the directors started to question their assumptions, with a debate on whether they should continue

to accept any webshop and risk similar problems, and then possibly lose the business and prospects of large and benevolent webshops (IN1, IN2, D3). In the end, the directors agreed to give the dubious webshops the choice of complying or leaving the platform (IN1).

The trade-off between growth and legitimacy changed. The dubious webshops had already been part of the platform for several years (IN9), and some interviewees argued that the webshops had brought in high-volume orders and a large part of the revenue in the early days of PayNow. Yet, the internal investigation suggested that, if sales were now to be ruled illegal, they would also have a negative financial impact on the organisation. Further, financial gains from morally dubious webshops were becoming less important, given that the platform had a financially secure position by 2018 (IN2).

The growing importance of reputation also plays a role. Employees argued that if PayNow wanted to garner a higher class of webshops, they should not be associated with disreputable parties (IN1, IN2). The reduced reputation of the platform could negatively impact future profitability (IN7). '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. [...] Yes, and that's a bit more than we might have thought beforehand. That our responsibility is a bit wider or bigger [...] Then your responsibility can be bigger than just [acting as] a serving hatch'. (IN11).

Questioning of internal assumptions took place continuously. '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 [the webshops], who are we to do that? [...] That was the approach for a long time'. (IN2).

A change in moral perspective is apparent from this quote: 'Anyway, it was more of an ethical issue. A webshop like this [...] is not the way you should do business. And if we are like: you as a webshop do not do business the way we would, that we would find responsible. Yes, why should we want to do business with you? [...] 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 heading for deception. But when is something a deception? And then comes the ethical aspect. And at some point, that, fortunately, grew in importance'. (IN2). While PayNow previously did not consider it their responsibility to tell others how to run their business, this eventually changed. (IN2)

4.3.3. Securing the platform

Securing the platform was done more proactively in this phase. To battle consumer fraud, PayNow replaced their generic credit checks with more

sophisticated risk assessments, including the price and tradability of goods. Large orders (i.e., over a few thousand euros) are now checked manually (IN5). Sometimes, PayNow does not accept webshops because the types of goods they sell attract too much fraud (IN9).

For dubious webshops, PayNow implemented a stricter onboarding process, including a specific compliance officer role and due diligence procedure. This stricter process was the outcome of a longer process in which PayNow made changes and the webshops responded, sometimes actively resisting the governance interventions. Early on, PayNow approached the webshops multiple times and confronted them with their behaviour. PayNow also increased the transaction costs for the dubious webshops (IN2). Although the webshops maintained that all was legally correct, they reluctantly changed their websites. As one interviewee said in frustration: 'They were treating symptoms but never had the intention of actually changing their methods'. (IN2). While PayNow directors were still debating what to do, dubious webshops even tried to add many new labels for their shops and products to the platform, which increased the fears at PayNow of having to process even more complaints (IN5).

Comparing the versions of the due diligence process (D2) shows that PayNow started to evaluate whether the merchant complied with their terms of service, such as correctly providing information to consumers and handling purchases. This decision was made to prevent new parties that misled consumers from being taken on and to prevent trouble. 'We want all webshops that do business with us to meet several conditions. And those parties that did not comply, while they had a chance to comply, did then put all the effort there [once it was required of them]. And then we said goodbye'. (IN2). Later, after the authorities had investigated PayNow, further changes were made to the due diligence procedure of checking information provided to consumers (D2). The compliance check task was also moved from the sales department to the customer service department to avoid conflicts of interest, whereby sales goals would be prioritised over due diligence. A checklist was introduced to collect website information and to verify whether the webshop has a correct listing with the Chamber of Commerce. According to some interviewees, these changes resulted in an even stricter process (IN1, IN2).

4.4. Cross-phase analysis

Moral legitimacy concerns consistently influenced governance practices across the phases, see Table 1. Employees and external stakeholders viewed negative network externalities as morally reprehensible and damaging to the platform's reputation.

Regulatory legitimacy played a role in the background as actions were often taken proactively before formal intervention. In the second phase, the legal ambiguity around selling certain product categories played a role in the background, indirectly leading to stricter conditions on product mix. Only in the third phase did regulatory legitimacy concerns play a direct role, which may explain why the governance responses were more formalised than before (e.g., due diligence checks).

Microlevel governance processes had to deal with negative network externalities, legitimacy concerns and other goals across all phases, but the way that trade-offs were made changed profoundly. Negative network externalities and legitimacy concerns (calling for stricter governance) increasingly outweighed goals of revenues and growth (calling for leniency). Moral standards shifted over time, resulting from internal debate about fairness, duty of care and the responsibility of transaction platforms for third-party behaviour. While this pattern is clear from our results, financial harm caused by negative network externalities (e.g., through non-paying consumers) also remained important.

5. Discussion

5.1. Negative network externalities as triggers of platform governance

Our study unpacks how negative network externalities trigger governance responses, and thus specifies how organisations deal with negative feedback loops that generative platforms may cause (Hanseth et al., 2006; Henfridsson & Bygstad, 2013). In doing so, we go beyond existing literature that largely focuses on how platform governance results in positive network effects (Parker et al., 2017) and value co-creation (Schrieck et al., 2016).

Our study uncovers societally-driven negative network externalities that create legitimacy challenges, unlike prior studies that focus on low-quality and inferior offerings (e.g., Helfat & Raubitschek, 2018). The externalities we uncovered do not carry the same weight, as is often assumed (Liebowitz & Margolis, 1994). We show that different types of externalities (e.g., fraud, privacy violations) produce diverse governance responses. Differentiating the types of negative network externalities is necessary to explain why platforms adopt different governance responses to ostensibly similar levels of pressure.

The heterogeneity of negative network externalities draws out the limitations of existing approaches that use proxies such as losses of attractiveness (Wessel et al., 2017) and satisfaction (Cennamo & Santaló, 2019) or quantitative models of rivalry or choice overload (Boudreau, 2010), which treat negative network externalities as homogeneous and thus obscure the different governance responses that distinct types of externalities call for.

Table 1. Cross-phase analysis.

Aggregated dimensions	Phase 1: Selective legitimacy responses (2013–2016)	Phase 2: Responding to escalating legitimacy challenges (2016–2017)	Phase 3: Proactively securing for legitimacy gains (2017–2018)
Materialising and spotting negative network externalities	Triggers: - Fraudulent webshops requiring costly foreign returns (Event 1) - Consumers failing to pay invoices raised alarms - Consumers started asking about privacy and data use (Event 4), but no major privacy breaches occurred Responses: - Spotted payment issues but largely ignored them to protect growth - Appointed a privacy officer (rare exception) and limited third-party identity validation providers	Triggers: - Worsening payment behaviour from foreign webshops (Event 1) - New issues from smart shops selling psychoactive substances (Event 5): poor payment behaviour and hard-to-handle consumers Responses: - Began systematically spotting and discussing problematic merchants/product categories - Started to question merchant quality when payment performance declined	Triggers: - Consumer fraud became financially visible after PayNow took over payment default insurance (Event 3) - Clustered complaints about 'free trial' webshops misleading consumers (Event 2) Responses: - Monitored complaint volumes per webshop
Perceiving legitimacy challenges	Triggers: - Moral legitimacy concerns about privacy rose due to societal debate and consumer questions - No major regulatory pressure on return addresses (Dutch law did not require domestic returns) Responses: - Limited debate; growth focus overrode fraud concerns - Growing moral awareness on privacy, seeing it as part of firm's role	Triggers: - Competitor rejections of dubious merchants - Smart shops created moral and regulatory concerns (unclear legality) Responses: - Perceived that continuing to host dubious webshops might harm image	Triggers: - Public complaints, partner complaints, and customer service overload (Event 2) - Internal debate about platform's responsibility intensified Responses: - Directors commissioned internal due diligence and compliance investigation to resolve debate - Reputation explicitly prioritised over short-term revenues
Internal Assumptions and Trade-Offs	Triggers: - Growth dependency on foreign webshops led to assumption that PayNow should remain neutral and not 'police' merchants Responses: - Maintained priority on growth (except for privacy issues)	Triggers: - Financial dependency on dubious webshops declined; reputation became more important - Payment losses reduced financial benefits from foreign merchants Responses: - Changed assumption: foreign return addresses violate fairness/duty of care - Expanded perceived duty of care to include product-level responsibility (smart shops)	Triggers: - Fraud and complaints threatened both reputation and profitability Responses: - Dropped neutrality assumption: now actively screened merchants - Directors agreed that only compliant and responsible webshops should remain - Trade-off resolved in favour of long-term legitimacy even at cost of short-term revenues
Securing the Platform	Responses: - Minimal action on return addresses (no local return policy introduced yet) (Event 1) - Appointed privacy officer and limited the third parties that received consumer data (tightened conditions slightly) (Event 4)	Responses: - Introduced local return address requirement in compliance policy (Event 1) - Adjusted membership conditions and product mix to exclude smart shops (Event 5)	Responses: - Replaced generic credit checks with risk-based assessments and manual review of large orders (Event 3) - Implemented stricter onboarding & compliance processes (Event 2) - Added compliance officer role, moved compliance checks out of sales department to avoid conflicts, created due diligence checklist to collect webshop information and listing, direct conversations with dubious webshops, increased transaction costs for dubious webshops, and removed non-compliant webshops

5.2. Micro-processes of platform governance: thresholds and assumption-questioning

Our insights into the endogenous microlevel processes of governance adaptations complement those focusing on exogenous drivers (Gawer, 2014). Distinguishing these processes is important, as they do not necessarily co-occur. For instance, materialising negative network externalities are not always spotted, while platform sponsors act not only on materialised negative network externalities but also on potential ones. The processes and negative network externalities are co-constitutive, as platform sponsors observe the negative network externalities that their existing membership conditions allow, leading to slowly accumulating

legitimacy challenges, internal discussions and ultimately changes in the same membership conditions. Finally, threshold models are more suitable to understanding the processes as it typically took the platform sponsor a prolonged period of time to act upon materialising negative network externalities.

In explaining the governance processes, we show that an institutional legitimacy lens is helpful. When legitimacy pressures accumulate beyond a certain threshold, the platform sponsor takes governance actions to safeguard the platform. The level of these thresholds depends on how platform sponsors trade off losses of legitimacy against competing goals such as growth and financial stability.

Table 2. Future research directions.

Research questions	Why it matters for IS literature and theory
How do negative network externalities constrain or condition the realisation of positive network externalities?	• Advances understanding of interactions between positive and negative externalities, integrating economics and institutional views
How does the weight of negative network externalities evolve during the platform life cycle?	• Reconciles economics-dominated discourse on positive impacts of platforms and critical discourses on the societal implications
Through what microlevel processes do platform sponsors spot, trade off and act upon negative network externalities?	• Deepen insight into the microlevel mechanisms of platform governance
How do these microlevel platform governance processes and thresholds differ between industries?	• Contextualisation and comparative theorisation of governance under varying societal and regulatory expectations (e.g., finance vs healthcare)
How do governance transitions unfold as legitimacy pressures emerge across different platform types?	• Enhances theories of <i>platform evolution</i> by conceptualising governance as a dynamic, path-dependent process rather than a static choice
How do securing dynamics for platform governance differ between transaction and innovation platforms?	• Builds comparative insights across platform types, strengthening the generality of IS theories on governance and legitimacy
How do AI-driven governance tools (e.g., automated fraud detection) affect the ways in which negative network externalities lead to internal debates and governance actions?	• Extends platform governance theories by examining the unintended consequences of algorithmic control, especially the loss of human oversight and reflective practice
How do platform participants actively resist governance interventions?	• Extends IS theory by introducing user agency and resistance into governance studies, helping to explain unintended consequences of governance choices
How does participant resistance affect the microlevel processes of platform governance adaptations?	

Internal processes are involved as well, as the platform sponsor questions its assumptions and values in light of the perceived legitimacy challenges, whereas adjusted assumptions and values (e.g., over what duty of care means for a transaction platform) may accelerate the decision to act and safeguard the platform.

Moral legitimacy concerns grew due to changing societal expectations and internal debates about fairness and duty of care, which pushed the platform sponsor to act. In this sense, we provide evidence that governance processes are triggered proactively before regulatory legitimacy challenges accumulate or externalities materialise. This proactive tightening of membership conditions challenges the assumption that platform governance primarily evolves towards greater openness (Staykova & Damsgaard, 2015; Tan et al., 2015).

Our case provides novel ways in which platform participants affect platform governance. In platform literature, the idea is readily established that platform participants do so actively, for instance, through shared decision rights (Selander et al., 2013) or by creating their boundary resources (Eaton et al., 2015; Van der Geest & Van Angeren, 2023). Our study suggests three more indirect ways. First, we show that platform participants may behave in such ways that they create negative network externalities, which call upon the platform sponsor to act. Second, we show that platform participants can affect legitimacy perceptions by voicing complaints or giving feedback, which in turn motivates changes in platform governance. Third, we find that platform participants may resist governance (e.g., calls to change fraudulent practices), which intensifies the negative network externalities (more fraud) and triggers follow-up governance actions (actively ousting fraudulent webshops).

5.3. Legitimacy of platform governance: societal pressure and internal deliberation

Our study extends legitimacy theory by unpacking the microlevel processes through which platform sponsors respond to emerging legitimacy challenges. While Suchman's (1995) framework conceptualises the accumulation of legitimacy pressures at a macro level, it does not specify the internal organisational processes through which actors detect, interpret, debate, and act upon emerging legitimacy challenges. Our study shows that legitimacy pressures accumulate through ongoing processes that gradually shift organisational assumptions about responsibility and duty of care.

Questions about whether platform sponsors are responsible for the behaviour of platform users have been raised previously (Cusumano et al., 2019). We contribute to this debate through a legitimacy lens, by showing that the platform sponsor took more responsibility over time and exerted more stringent governance in response to uncovered network externalities. Besides the growing importance of reputation for long-term viability, the payment platform sector became more professional in dealing with normative issues. Consequently, decision-makers gave greater weight to moral and regulatory legitimacy concerns, redefining their duty of care and justifying stricter governance. The sense of responsibility thus depends on established market categories that provide clear and stable benchmarks for what is deemed acceptable (Cattani et al., 2017; Taeuscher & Rothe, 2024).

We also show how societal actors influence platform governance by proactively creating or amplifying legitimacy challenges. The potentially negative impact of platforms on users, public values and social life is increasingly apparent in literature (Van Dijck, 2014; Van Dijck et al., 2018, 2023). Existing work shows that negative network externalities can affect platform legitimacy (Uzunca et al., 2018). Our study adds to

this by showing the process through which legitimacy challenges from societal actors accumulate and drive platform sponsors to safeguard their platforms. Policymakers aiming to address negative network externalities by regulating platform membership conditions (Heimburg & Wiesche, 2023) may seek to actively create legitimacy challenges to effectuate change. Even when regulations are stable, perceptions about regulatory legitimacy change and affect governance decisions. Likewise, public awareness campaigns could be used to intensify moral legitimacy pressures on platforms to adopt more ethical practices.

Our study shows that negative network externalities affecting moral legitimacy trigger reputational concerns and internal questions about the platform's duty of care, which lead to governance changes focused on reputation and ethical standards. Those affecting regulatory legitimacy prompt compliance-oriented governance responses. In this way, distinguishing moral and regulatory dimensions of legitimacy helps in understanding the processes that produce different governance responses.

5.4. Implications for practice

Platform sponsors that proactively spot and address negative network externalities may prevent losses of legitimacy. By implementing governance mechanisms such as stricter onboarding processes, fraud checks and compliance roles, transaction platforms can build safeguards on their platforms. Especially in industries where users can easily switch to competing platforms, legitimacy is essential to retain users. Further, early governance interventions reduce the risk of potentially more costly corrective actions. Proactive governance, even before formal requirements arise, can pre-empt crises and signal responsibility to stakeholders.

Governance actions are advisable if moral and regulatory challenges outweigh (short-term) opportunities for growth and revenue generation. Governance responses typically reduce the opportunities to create positive network externalities. As growth and revenues are typically more important for younger platforms, they may tolerate greater negative network externalities before taking action. Further, the costs of governance enforcement should be traded off against the risks of not taking action.

If left unaddressed, negative network externalities can escalate substantially. For instance, misinformation on social media platforms has led to massive regulatory scrutiny and user distrust. But also isolated incidents with big ramifications, such as unsafe drivers on a ride-hailing platform, can create major societal and moral legitimacy pressures.

Actions such as actively tracking user complaints, media coverage and public forums help to spot

emerging negative network externalities early. Within the organisation, customer-facing roles (e.g., helpdesk employees) in particular should have a voice, and filling compliance roles with employees who are incentivised to boost usage and growth (e.g., account managers) should be avoided. Opening up the organisation to regulators, interest groups and users will also help to spot issues and co-create governance solutions. Rather than seeing governance as a one-off task, continuous adjustments and enforcement are needed.

Regulatory intervention can accelerate responses to negative network externalities, because even the mere possibility of regulatory action may influence internal debates. The implications outlined above should therefore not be misinterpreted as a plea for self-regulation, given that growth and revenue generation, which apply to any starting company, are even greater in the face of positive network externalities and platform competition. Earlier regulatory interventions might therefore counterbalance these growth incentives and accelerate responses to negative network externalities.

Our findings also connect to broader debates on how governments engage with platforms. Governments not only regulate to mitigate harm but also aim to capture value generated through network effects. This perspective adds nuance to the observation that regulatory legitimacy pressures shape governance changes on transaction platforms. Regulatory scrutiny may have been motivated not only by consumer protection but also by the interest in ensuring value creation within the payment ecosystem in alignment with broader fiscal, competitive or strategic goals. In this way, negative network externalities create not only legitimacy challenges for platforms but also opportunities for governments to assert control over how value from network effects is distributed.

Beyond asserting control over value distribution, policymakers can also leverage legitimacy pressures more directly to drive platform accountability. By amplifying moral and regulatory legitimacy challenges (e.g., through public awareness campaigns, media scrutiny, or dialogues), policymakers can put pressure on platforms to take governance actions. For example, highlighting consumer harm or ethical lapses in public discourse can accelerate governance adjustments. Regulators should also consider flexible frameworks that allow platforms to experiment with governance innovations, while setting clear benchmarks for duty of care and compliance, especially as these notions were still contested at the early stage of the platform.

5.5. Contributions to IS literature and future research

One set of questions revolves around the interaction of positive and negative network externalities, see Table

2. In our case, the platform sponsor perceived that not complying with societal expectations negatively impacted the willingness of participants to remain active on the platform. This calls for research into how negative network externalities constrain or condition the realisation of positive network externalities, integrating economics and institutional views on platforms. Future research should explicitly examine temporal and life-cycle dynamics, as negative network externalities often grow more influential as platforms scale up and face legitimacy pressures. Such integration of positive and negative implications of transaction platforms could help reconcile the separate research streams that take an economics versus a critical approach.

The microlevel platform governance processes provide a basis for further theorising that challenges the view of platform governance as a one-off choice. Such process theories could incorporate the idea of thresholds for governance change, as introduced in this paper, to understand the punctuated process of governance adaptations. While our study is contextualised in the financial industry, the theoretical mechanisms could be transferred to other settings with high societal expectations, such as healthcare or education. Comparative studies between transaction and innovation platforms could deepen these insights by testing whether similar governance dynamics occur across different types of platforms.

The case study period ended as algorithmic control and AI-driven governance were just emerging (e.g., Wiener et al., 2023). While such tools may increase effectiveness in rule enforcement, they also raise concerns. If human oversight is reduced, the kind of reflective questioning of assumptions that we found to be vital in our case may become less likely. Thus, future IS research should examine not only how AI-driven governance safeguard platforms but also whether it limits opportunities for organisational learning and reflexivity, thereby creating another source of feedback loops in the microlevel processes of governance adaptation.

Finally, our study primarily focused on the perspective of the platform sponsor. However, interviewees noted that complementors often resisted governance interventions or only superficially complied through cosmetic adjustments to their offerings. This points to the need for research that takes into account participant agency and explores how resistance shapes the effectiveness of governance mechanisms.

5.6. Limitations and transferability

Several methodological limitations apply to our study. First, interviewees may give socially desirable answers as we study how negative network externalities are handled. As negative network externalities are by

definition socially undesirable and concern sensitive topics (e.g., fraud, privacy violations), this risk may be greater in this particular study. Yet, we observe that interviewees were generally open in discussing how they chose not to deal with externalities in the past, and how their normative assumptions changed over time. Such openness may have been stimulated by our assurance to respondents of the anonymisation of the case and personal details. Second, recall bias may have played a role, as we asked interviewees to reflect on past events. Especially internal debates about assumptions and norms may be easier to recall if they happened recently. Sometimes, interviewees admitted not being able to fully recall what happened in the early days of the platform or commented that the events unfolded before they were hired. For mitigation, we used documents to understand the context of the events and referred to these in the interviews. Third, although interviewees were diverse and saturation was attained, more interviews might lead to additional findings. Interviewing other stakeholders (e.g., consumers) could show whether legitimacy concerns are grounded in reality. While the data provides rich insights into the sponsor's internal decision-making process, it does not capture the perspectives of demand or supply side actors, such as consumers or complementors. As a result, the study examines perceived legitimacy challenges rather than the actual effects of governance mechanisms on external stakeholders. This focus aligns with the study's theoretical lens, which emphasises the role of organisational perceptions in driving governance decisions (Suchman, 1995). Future research could triangulate platform sponsor data with external stakeholder perspectives to provide a more comprehensive view of how governance mechanisms influence legitimacy and ecosystem stability. Fourth, as in any single case study, our findings may not generalise to other transaction platforms, which may have had different reasons for changing their governance in the study period. Fifth, exact turning points between the phases could not be established in the temporal bracketing analysis, as phases flowed more gradually into each other. Phase transitions were inferred from observed changes in how the platform sponsor dealt with negative network externalities rather than external drivers. Future research may provide more precise understanding of how early and mature phases affect decision-making about governance responses, especially if done through (naturalistic) experiments.

Our findings are valid within the boundary conditions of the case. Here, especially the announced introduction of European regulations on privacy and fraud monitoring increased regulatory scrutiny around the end of the study period. Also relevant is the Dutch civil law context, which only seeks to compensate actual damages without allowing for high claims for non-

material damages or deterrent purposes (as opposed to, for instance, the US).

As our case is situated in the fintech industry, its regulatory context may play a role. Unlike platforms in emerging sectors, such as social media or ridesharing, where regulatory standards are still evolving, fintech platforms must operate within well-defined regulatory frameworks. Hence, platform sponsors can anticipate what regulatory norms and beliefs are desirable. Although negative externalities mainly stemmed from observing the malicious behaviour of sellers (e.g., misleading policies) and consumer complaints, the regulatory context of the fintech industry likely made PayNow more sensitive to those issues that could remain tolerable in other sectors. Especially the regulatory aspects of legitimacy challenges are amplified by potential legal repercussions, which never directly materialised in any of the studied events but remained in the background, thereby necessitating proactive governance interventions. Future research could benefit from comparing governance responses across platforms in regulated versus less-regulated or less-stable industries to better understand how the interplay between regulatory compliance and legitimacy concerns influences governance decisions.

Our findings might be transferable to understanding the governance mechanisms of open innovation platforms. Similar to transaction platforms, open innovation platforms face negative network externalities such as malware and must navigate trade-offs between financial gains and legitimacy. Other parts of our findings specifically apply to transaction platforms. In contrast to innovation platforms, transaction platforms only facilitate interactions and provide no basis for generative innovation, which could explain why a platform sponsor may perceive less responsibility for the content of interactions. Unlike innovation platforms, transaction platforms do not provide the technical architecture for third parties to create or modify boundary resources (e.g., jailbreaking on iOS; Eaton et al., 2015). This form of infrastructural resistance therefore limits the transferability of our findings to innovation platform contexts.

6. Conclusions

When platform sponsors face negative network externalities, platform governance unfolds as a process driven by accumulating moral and regulatory legitimacy pressures. This study shows that platform sponsors respond to negative network externalities through microlevel processes of spotting externalities, revisiting internal assumptions and safeguarding the platform. These microlevel processes become increasingly proactive as platforms mature and legitimacy concerns outweigh growth incentives. An institutional legitimacy lens helps in

understanding these dynamics. This study extends platform governance theory beyond its traditional focus on positive network effects and openness, towards a more fine-grained process understanding of how platforms maintain and safeguard legitimacy over time.

Note

1. Under certain conditions, smart shop products are legal in the Netherlands. Yet, there is a thin line between what is legal and illegal, depending, for instance, on the weight of the sold product or whether certain products are bought in combination.

Acknowledgement

The authors thank Ibo van de Poel for his valuable feedback on the empirical study and the case organization's key informant for continuous support throughout the research process. The authors thank the Editor and the anonymous reviewers for their constructive comments and insightful suggestions.

Author contributions

CRedit: **Mark de Reuver**: Conceptualization, Methodology, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing; **Noah Brandwijk**: Conceptualization, Investigation, Methodology, Project administration, Visualization, Writing – original draft, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Mark de Reuver  <http://orcid.org/0000-0002-6302-7185>

References

- Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. *Journal of Management*, 43(1), 39–58. <https://doi.org/10.1177/0149206316678451>
- Afuah, A. (2013). Are network effects really all about size? The role of structure and conduct. *Strategic Management Journal*, 34(3), 257–273. <https://doi.org/10.1002/smj.2013>
- Aldrich, H. E., & Ruef, M. (2006). *Organizations evolving* (Second ed.). Sage Publications. <https://doi.org/10.4135/9781446212509>
- Ansari, S. (S.), Garud, R., & Kumaraswamy, A. (2016). The disruptor's dilemma: TiVo and the U.S. television ecosystem. *Strategic Management Journal*, 37(9), 1829–1853. <https://doi.org/10.1002/smj.2442>
- Asvanund, A., Clay, K., Krishnan, R., & Smith, M. D. (2004). An empirical analysis of network externalities in peer-to-peer music-sharing networks. *Information Systems Research*, 15(2), 155–174. <https://doi.org/10.1287/isre.1040.0020>

- Autio, E., & Thomas, L. D. W. (2016). Tilting the playing field: Towards an endogenous strategic action theory of ecosystem creation. In S. Nambisan (Ed.), *Open innovation, innovation ecosystems, and entrepreneurship: Multidisciplinary perspectives* (1–4, pp. 111–140). World Scientific Publishing. https://doi.org/10.1142/9789813149083_0005
- 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>
- Broekhuizen, T. L. J., Emrich, O., Gijsenberg, M. J., Broekhuis, M., Donkers, B., & Sloot, L. M. (2019). Digital platform openness: Drivers, dimensions and outcomes. *The Journal of Business Research*, In press. <https://doi.org/10.1016/j.jbusres.2019.07.001>
- Casini, L. (2018). Googling democracy? New technologies and the law of global governance: Afterword to Eyal Benvenisti's foreword. *The European Journal of International Law*, 29(4), 1071–1077. <https://doi.org/10.1093/ejil/chy072>
- Cattani, G., Ferriani, S., & Lanza, A. (2017). Deconstructing the outsider puzzle: The legitimation journey of novelty. *Organization Science*, 28(6), 965–992. <https://doi.org/10.1287/orsc.2017.1161>
- Cennamo, C., & Santaló, J. (2019). Generativity tension and value creation in platform ecosystems. *Organization Science*, 30(3), 617–641. <https://doi.org/10.1287/orsc.2018.1270>
- Cusumano, M. A., & Gawer, A. (2002). The elements of platform leadership. *MIT Sloan Management Review*, 43(3), 51. <https://doi.org/10.1109/EMR.2003.1201437>
- Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). *The business of platforms: Strategy in the age of digital competition, innovation, and power*. Harper Business.
- Eaton, B., Elaluf-Calderwood, S., Sorensen, C., & Yoo, Y. (2015). Distributed tuning of boundary resources: The case of Apple's iOS service system. *MIS Quarterly: Management Information Systems*, 39(1), 217–243. <https://doi.org/10.25300/MISQ/2015/39.1.10>
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532–550. <https://doi.org/10.5465/amr.1989.4308385>
- Eisenmann, T. R., Parker, G., & Van Alstyne, M. (2009). Opening platforms: How, when and why? In A. Gawer (Ed.), *Platforms, Markets and Innovation*, 131–162. Edward Elgar. <https://doi.org/10.4337/9781849803311.00013>
- Fürstenau, D., Baiyere, A., & Klierer, N. (2019). A dynamic model of embeddedness in digital infrastructures. *Information Systems Research*, 30(4), 1319–1342.
- Garcia, A., & O'Brien, S. (2019, December 7). Uber releases safety report revealing 5, 981 incidents of sexual assault. CNN. <https://edition.cnn.com/2019/12/05/tech/uber-safety-report/index.html>
- Garud, R., Kumaraswamy, A., Roberts, A., & Xu, L. (2022). Liminal movement by digital platform-based sharing economy ventures: The case of Uber Technologies. *Strategic Management Journal*, 43(3), 447–475. <https://doi.org/10.1002/smj.3148>
- 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>
- Gawer, A., & Cusumano, M. A. (2014). Industry platforms and ecosystem innovation. *Journal of Product Innovation Management*, 31(3), 417–433. <https://doi.org/10.1111/jpim.12105>
- Gawer, A., & Srnicek, N. (2021). *Online platforms: Economic and societal effects*. European Parliament. <https://data.europa.eu/doi/10.2861/844602>
- 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>
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research. *Organizational Research Methods*, 16(1), 15–31. <https://doi.org/10.1177/1094428112452151>
- Goldbach, T., Kemper, V., & Benlian, A. (2014). Mobile application quality and platform stickiness under formal vs. self-control-evidence from an experimental study.
- Gu, X., Cao, J., & Fang, Y. (2025). Review manipulation and filtering on digital platforms. *Information Systems Research*, 37(2), 927–947. <https://doi.org/10.1287/isre.2022.0694>
- Hanseth, O., Grisot, M., & Aanestad, M. (2006). Reflexive standardization: Side effects and complexity in standard making. *MIS Quarterly*, 30, 563. <https://doi.org/10.2307/25148773>
- Heimburg, V., & Wiesche, M. (2023). Digital platform regulation: Opportunities for information systems research. *Internet Research*, 33(7), 72–85. <https://doi.org/10.1108/INTR-05-2022-0321>
- Helfat, C. E., & Raubitschek, R. S. (2018). Dynamic and integrative capabilities for profiting from innovation in digital platform-based ecosystems. *Research Policy*, 47(8), 1391–1399. <https://doi.org/10.1016/j.respol.2018.01.019>
- Henfridsson, O., & Bygstad, B. (2013). The generative mechanisms of digital infrastructure evolution. *MIS Quarterly*, 37(3), 907–931. <https://doi.org/10.25300/MISQ/2013/37.3.11>
- Iansiti, M., & Levien, R. (2004). Strategy as ecology. *Harvard Business Review*, 82(3), 68–78, 126.
- Ingram Bogusz, C., Teigland, R., & Vaast, E. (2019). Designed entrepreneurial legitimacy: The case of a Swedish crowdfunding platform. *European Journal of Information Systems*, 28(3), 318–335. <https://doi.org/10.1080/0960085X.2018.1534039>
- Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, 39(8), 2255–2276. <https://doi.org/10.1002/smj.2904>
- Jagtiani, J., & John, K. (2018). Fintech: The impact on consumers and regulatory responses. *Journal of Economics and Business*, 100, 1–6. <https://doi.org/10.1016/j.jeconbus.2018.11.002>
- 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>
- Katz, M. L., & Shapiro, C. (1994). Systems competition and network effects. *Journal of Economic Perspectives*, 8(2), 93–115. <https://doi.org/10.1257/jep.8.2.93>
- Khanagha, S., Ansari, S., Paroutis, S., & Oviedo, L. (2020). Mutualism and the dynamics of new platform creation: A study of Cisco and fog computing. *Strategic Management Journal*, 43(3), 476–506. <https://doi.org/10.1002/smj.3147>
- Kim, A., & Dennis, A. R. (2019). Says who? The effects of presentation format and source rating on fake news in

- social media. *MIS Quarterly*, 43(3), 1025–1039. <https://doi.org/10.25300/MISQ/2019/15188>
- Kim, S. S., Kim, S., & Kim, H. W. (2025). Hate speech detection on online news platforms: A deep-learning approach based on agenda-setting theory. *Journal of Management Information Systems*, 42(3), 673–705. <https://doi.org/10.1080/07421222.2025.2520173>
- Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the internet: Attacks, costs and responses. *Information Systems*, 36(3), 675–705. <https://doi.org/10.1016/j.is.2010.11.003>
- Kumar, N., Venugopal, D., Qiu, L., & Kumar, S. (2018). Detecting review manipulation on online platforms with hierarchical supervised learning. *Journal of Management Information Systems*, 35(1), 350–380. <https://doi.org/10.1080/07421222.2018.1440758>
- Kumar, V., Kumar, S., Chatterjee, S., Chaudhuri, R., & Gupta, S. (2026). Decoding deepfake perceptions: Trustworthiness, importance and behavioral intention. *Information Systems Frontiers*, 1–19. <https://doi.org/10.1007/s10796-026-10765-9>
- Kummer, M., & Schulte, P. (2019). When private information settles the bill: Money and privacy in Google's market for smartphone applications. *Management Science*, 65(8), 3470–3494. <https://doi.org/10.1287/mnsc.2018.3132>
- Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review*, 24(4), 691. <https://doi.org/10.2307/259349>
- Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, 61(1), 35–46. <https://doi.org/10.1016/j.bushor.2017.09.003>
- Lee, S., Shin, D., Kwon, K. H., Han, S. P., & Lee, S. K. (2024). Disinformation spillover: Uncovering the ripple effect of bot-assisted fake social engagement on public attention. *MIS Quarterly*, 48(3), 847–872. <https://doi.org/10.25300/MISQ/2023/17195>
- Liebowitz, S. J., & Margolis, S. E. (1994). Network externality: An uncommon tragedy. *Journal of Economic Perspectives*, 8(2), 133–150. <https://doi.org/10.1257/jep.8.2.133>
- McIntyre, D. P., & Srinivasan, A. (2017). Networks, platforms, and strategy: Emerging views and next steps. *Strategic Management Journal*, 38(1), 141–160. <https://doi.org/10.1002/smj.2596>
- McMahon, L. (2022). Instagram: Video selfies trial to verify age of teens. *BBC*.
- Miles, M., Huberman, A., & Saldaña, J. (2014). *An expanded sourcebook: Qualitative data analysis* (2nd ed.) (M. B. Miles & A. M. Huberman, (Eds.)). SAGE Publications.
- Moravec, P. L., Minas, R. K., & Dennis, A. R. (2019). Fake news on social media: People believe what they want to believe when it makes no sense at all. *MIS Quarterly*, 43(4), 1343–1360. <https://doi.org/10.25300/MISQ/2019/15505>
- Nash, V., Bright, J., Margetts, H., & Lehdonvirta, V. (2017). Public policy in the platform society. *Policy and Internet*, 9(4), 368–373. <https://doi.org/10.1002/poi3.165>
- Nguyen, A., Rai, A., & Maruping, L. (2024). Understanding the unintended effects of human-machine moderation in addressing harassment within online communities. *Journal of Management Information Systems*, 41(2), 341–366. <https://doi.org/10.1080/07421222.2024.2340831>
- Ofe, H. A., & Sandberg, J. (2023). The emergence of digital ecosystem governance: An investigation of responses to disrupted resource control in the Swedish public transport sector. *Information Systems Journal*, 33(2), 350–384.
- 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>
- Parker, G., Van Alstyne, M., & Jiang, X. (2017). Platform ecosystems: How developers invert the firm. *MIS Quarterly*, 41(1), 255–266. <https://doi.org/10.25300/MISQ/2017/41.1.13>
- Peng, C., Liu, S., & Lu, Y. (2019). The discursive strategy of legitimacy management: A comparative case study of Google and Apple's crisis communication statements. *Asia Pacific Journal of Management*, 38(2), 519–545. <https://doi.org/10.1007/s10490-019-09667-z>
- Polasik, M., Hutarska, A., Iftikhar, R., & Mikula, Š. (2020). The impact of Payment Services Directive 2 on the PayTech sector development in Europe. *Journal of Economic Behavior and Organization*, 178, 385–401. <https://doi.org/10.1016/j.jebo.2020.07.010>
- Rietveld, J., & Schilling, M. A. (2021). Platform competition: A systematic and interdisciplinary review of the literature. *Journal of Management*, 47(6), 1528–1563. <https://doi.org/10.1177/0149206320969791>
- Rinta-Kahila, T., Someh, I., Gillespie, N., Indulska, M., & Gregor, S. (2022). Algorithmic decision-making and system destructiveness: A case of automatic debt recovery. *European Journal of Information Systems*, 31(3), 313–338. <https://doi.org/10.1080/0960085X.2021.1960905>
- 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>
- Saldaña, J. (2013). *The coding manual for qualitative researchers* (Second ed.). SAGE Publications Ltd.
- Schaarschmidt, M., Homscheid, D., & Kilian, T. (2019). Application developer engagement in open software platforms: An empirical study of Apple iOS and Google Android developers. *International Journal of Innovation Management*, 23(4), 1950033. <https://doi.org/10.1142/S1363919619500336>
- Schrieck, M., Wiesche, M., & Krcmar, H. (2016, June). Design and governance of platform ecosystems-key concepts and issues for future research. In *24th European Conference on Information Systems (ECIS)*, Istanbul, Turkey.
- Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, 21(1), 1–16. <https://doi.org/10.1016/j.infoandorg.2010.11.001>
- Scott, W. R. (2001). *Institutions and organizations* (2nd ed.). Sage Publications.
- Selander, L., Henfridsson, O., & Svahn, F. (2013). Capability search and redeem across digital ecosystems. *Journal of Information Technology*, 28(3), 183–197. <https://doi.org/10.1057/jit.2013.14>
- Singal, A. K. (2021). Designing platform ecosystems for collaboration, innovation and growth. *Benchmarking: An International Journal*, 29(9), 2806–2821. <https://doi.org/10.1108/BIJ-12-2020-0619>
- Staykova, K. S., & Damsgaard, J. (2015). The race to dominate the mobile payments platform: Entry and expansion strategies. *Electronic Commerce Research and Applications*, 14(5), 319–330. <https://doi.org/10.1016/j.elerap.2015.03.004>
- Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management*

- Review, 20(3), 571–610. <https://doi.org/10.5465/amr.1995.9508080331>
- Taeuscher, K., & Rothe, H. (2021). Optimal distinctiveness in platform markets: Leveraging complementors as legitimacy buffers. *Strategic Management Journal*, 42(2), 435–461. <https://doi.org/10.1002/smj.3229>
- Taeuscher, K., & Rothe, H. (2024). Entrepreneurial framing: How category dynamics shape the effectiveness of linguistic frames. *Strategic Management Journal*, 45(2), 362–395. <https://doi.org/10.1002/smj.3554>
- Tan, B., Pan, S., Lu, X., & Huang, L. (2015). The role of IS capabilities in the development of multi-sided platforms: The digital ecosystem strategy of Alibaba.com. *Journal of the Association for Information Systems*, 16(4), 248–280. <https://doi.org/10.17705/1jais.00393>
- Teixeira, A. (2009). Swimming with dolphins: A study on legitimacy processes in the Southern California tuna industry.
- Thomas, L. D. W., & Ritala, P. (2021). Ecosystem legitimacy emergence: A collective action view. *Journal of Management*, 48(3), 515–541. <https://doi.org/10.1177/0149206320986617>
- Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research commentary-digital infrastructures: The missing IS research agenda. *Information Systems Research*, 21(4), 748–759. <https://doi.org/10.1287/isre.1100.0318>
- Tiwana, A. (2014). *Platform ecosystems aligning architecture, governance, and strategy library of Congress cataloging-in-publication data*. Elsevier Inc.
- Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research*, 21(4), 675–687. <https://doi.org/10.1287/isre.1100.0323>
- Uzunca, B., Rigtering, J. P. C., & Ozcan, P. (2018). Sharing and shaping: A cross-country comparison of how sharing economy firms shape their institutional environment to gain legitimacy. *Academy of Management Discoveries*, 4(3), 248–272. <https://doi.org/10.5465/amd.2016.0153>
- Van Angeren, J., Alves, C., & Jansen, S. (2016). Can we ask you to collaborate? Analyzing app developer relationships in commercial platform ecosystems. *The Journal of Systems & Software*, 113, 430–445. <https://doi.org/10.1016/j.jss.2015.11.025>
- Van der Geest, C., & Van Angeren, J. (2023). Architectural generativity: Leveraging complementor contributions to the platform architecture. *California Management Review*, 65(2), 71–92. <https://doi.org/10.1177/00081256231159398>
- Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- Van Dijck, J., de Winkel, T., & Schäfer, M. T. (2023). Deplatformization and the governance of the platform ecosystem. *New Media and Society*, 25(12), 3438–3454. <https://doi.org/10.1177/14614448211045662>
- Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.
- Venkatraman, N., & Lee, C.-H. (2004). Preferential linkage and network evolution: A conceptual model and empirical test in the US video game sector. *Academy of Management Journal*, 47(6), 876–892.
- Wareham, J., Fox, P. B., & Cano Giner, J. L. (2014). Technology ecosystem governance. *Organization Science*, 25(4), 1195–1215. <https://doi.org/10.1287/orsc.2014.0895>
- 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>
- Wiener, M., Cram, W. A., & Benlian, A. (2023). Algorithmic control and gig workers: A legitimacy perspective of Uber drivers. *European Journal of Information Systems*, 32(3), 485–507. <https://doi.org/10.1080/0960085X.2021.1977729>
- Yin, R. (2018). *Case study research and applications: Design and methods*. SAGE Publications, Inc.
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>

Appendices

Appendix A. Definitions of core concepts

Core concept	Definition	Examples from case study
Platform sponsor	Owners that have architectural control over the platform and can set the conditions under which third parties can join the platform (Eisenmann et al., 2009)	PayNow
Governance processes	Microlevel internal organisational processes through which platform sponsors reason, reflect, and adapt governance	Spotting externalities, questioning internal assumptions, restricting membership
Negative network externalities	Harm arising from actions in a network (Afuah, 2013; Katz & Shapiro, 1994)	Fraudulent sellers, privacy breaches, consumer fraud
Moral legitimacy	Compliance with ethical values and principles (Scott, 2001)	Fulfilling duty of care, fairness towards consumers
Regulatory legitimacy	Compliance with laws, regulations, and formal rules within an industry or market (Aldrich & Ruef, 2006; Suchman, 1995)	Adherence to financial and privacy regulations
Legitimacy challenge	Situation in which the accumulation of pressures leads to a point where the organisation must act to preserve or repair legitimacy (cf. Suchman, 1995)	Overload of consumer complaints

Appendix B. Literature overview on types of negative network externalities

Type of negative network externality	Example references	Focus of the literature
Network congestion	Asvanund et al. (2004); Liebowitz and Margolis (1994)	Same-side users compete for shared, finite network capacity (e.g., road infrastructure, telecommunication lines)
Choice overload	Boudreau (2010)	Growth in number of sellers or complementors constrains users to evaluate and choose among offerings
Fraud, review manipulation	Gu et al. (2025); Kumar et al. (2018)	Malicious actors manipulate marketplace signals, reducing trust, transaction quality and platform value
Misinformation, deceptive content	Kumar et al. (2026); Kim and Dennis (2019); Moravec et al. (2019), Lee et al. (2024)	False, misleading, manipulated content affects beliefs, attention and trust
Privacy violations	Kummer and Schulte (2019)	Platform complementors collect personal information in ways that harm users
Security threats and cyberattacks	Kim et al. (2011)	Malicious behaviours such as phishing, malware, fraud, and cyberattacks impose costs on platform participants
Toxic behaviour / harassment	Nguyen et al. (2024); Kim et al. (2025)	Harmful interactions (e.g., hate speech) affect platform participants
Low-quality complements	Afuah (2013); McIntyre and Srinivasan (2017)	Participants or complementors exploit platform resources, reputation, or openness in ways that reduce value for others

Appendix C. Overview of documents analysed

Documents	Event 1	Event 2	Event 3	Event 4	Event 5
D1: Notes made on investigation documentation		x			
D2: Due diligence process		x			x
D3: Due diligence introduction presentation		x			
D4: Terms and conditions for users / suppliers	x	x			x
D5: Data processing agreement				x	
D6: Standard contract template	x				
D7: Privacy statement				x	
D8: Privacy assessment (Data Privacy Impact Assessment)				x	
D9: Internal data leakage procedure					
D10: Data processing activities register			x	x	
D11: Data leakage register			x		
D12: Transaction policy					
D13: API documentation					
D14: Responsible disclosure agreement					

Appendix D. Overview of interviewees and duration of interviews

Interviewee code	Duration(h/m/s)	Date	Function/role
IN1	1:03:24	02-04-2020	Compliance manager/ legal officer
IN2	0:42:29	03-03-2020	Manager IT / Case informant
	0:55:12	08-04-2020	
IN3	0:29:45	07-04-2020	IT specialist
IN4	0:42:46	06-04-2020	Operations manager
IN5	0:57:23	10-04-2020	Finance manager
IN6	0:46:01	14-04-2020	Due diligence manager partner
IN7	0:42:19	14-04-2020	Sales / partner manager
IN8	0:24:07	15-04-2020	Due diligence assistant / customer service
IN9	0:26:51	23-04-2020	Due diligence assistant / customer service
IN10	0:33:03	06-05-2020	Chief technology officer
IN11	0:31:21	07-05-2020	Chief executive officer

Note: All interviews took place via video calls.

Appendix E. Overview of evidence and codes for the events

	Evidence	Materialising externalities	Spotting potential externalities	Perceiving legitimacy challenges	Questioning internal assumptions	Trading-off legitimacy and growth	Securing the platform
Event 1: Return address policy	D4, D6 IN1, IN3, IN11	Misleading consumers	- Foreign-based webshops cause problems - Consumers are not paying	- Willingness to improve practices - Bad payment behaviour by consumers - Financial benefits from dubious webshops - Financial repercussions from non-paying consumers	Importance of fairness / duty of care	Need for early cash-flows as a startup	- Compliance policy - Supplier configuration - Country of origin
Event 2: Dubious webshops that mislead consumers	D1, D2, D3, D4 IN1, IN2, IN5 IN7, IN8, IN9	- Misleading consumers, trade practices - Non-compliant webshops	- Webshop doesn't want to resolve issues - Similar complaints keep coming in - Gut feeling says it's not right - Consumer complaints, reviews - Consumers are not paying	- Criticism from consumers - Receptivity to feedback - Financial benefits from dubious webshops - Bad payment behaviour by consumers - Increasing workload - Financial repercussions from non-paying consumers	- Responsibility as a transaction platform - Importance of fairness / duty of care	- Growing importance of reputation - Need for early cash-flows as a startup	- Due diligence policy - Conditions for webshops: Due diligence
Event 3: Consumer fraud risk	D10, D11 IN5, IN7, IN8, IN9, IN11	Fraud consumers	- Nature of product evokes fraud - Customer complaints - Consumers are not paying	- Ignoring potential issues (e.g., consumer fraud) - Bad payment behaviour by consumers - Financial repercussions from non-paying consumers	Responsibility as a transaction platform	Growing importance of reputation	Controls over consumers: Payment limit; Credit check
Event 4: Privacy evaluation of providers	D5, D7, D8, D10 IN1, IN2, IN3, IN10, IN11	N/A	Similar complaints keep coming in	- Criticism from consumers - Willingness to improve practices	- Importance of privacy - Responsibility as a transaction platform	Lack of processes and awareness, being a startup	- Formal policies: agreement / contract; privacy policy - Controls over consumers: Credit check
Event 5: Prohibiting smart shops	D2, D4 IN4, IN6, IN8, IN9	- Illegal products - Non-compliant webshops	- Suspicious marketing and advertisements - Particular kind of consumers is attracted	- Criticism from stakeholders - Bad payment behaviour by consumers	- Responsibility as a transaction platform - Importance of fairness / duty of care	N/A	Conditions for webshops: Product mix; Due diligence



Appendix F. Descriptive overview of main externalities, legitimacy challenges and governance responses

	Spotting negative network externalities	Regulatory legitimacy	Moral legitimacy	Trading off legitimacy versus growth	Securing the platform
Event 1: Return address policy	Foreign return addresses are a hassle (or worse) for consumers	N/A	Duty of care becomes more important	- Non-paying consumers create financial harm - Income from dubious webshops becomes less important as platform grows	Stricter conditions for webshops
Event 2: Dubious webshops that mislead consumers	Consumers get unwanted subscriptions due to misleading practices, leading to complaints	Platform sponsor was not aware of looming regulatory intervention	Internal debates and public discussion ultimately made duty of care more important, thus assuming more responsibility	Image and reputation became more important due to wanting to attract better webshops	Stricter due diligence
Event 3: Consumer fraud risk	- Most negative network externalities are internalised, as PayNow (self-)insures defaults. - The consumer fraud could potentially reduce trust in webshops on the platform	Not applicable	- Accepting orders without checking could lead to reputation harm - Credit check could signal ethical behaviour and thus be a unique selling factor	Payment defaults are costly	Stricter credit checks
Event 4: Privacy evaluation of providers	Privacy violations could harm consumer interests, although these did not materialise	GDPR played a minor role in motivating the changes	- Growing societal awareness - Internal values of company shifted - Maintaining trust and privacy	N/A	Not sharing data with complementors that do not respect privacy
Event 5: Prohibiting smart shops	PayNow may become associated with illegal activities, reducing the value for legit webshops	High difficulty of attaining legal compliance (changing regulation, changing products of webshops)	- Discussion about morality of selling products for undesirable/illegal activities - Undesired association with dubious consumers and activities	Lack of legal jurisprudence	Stricter due diligence

Appendix G. Timeline of events

- Early 2010s: Launch of the platform
- 2013: Privacy officer is appointed, first privacy policies implemented
- 2016: Conditions for webshops are made stricter, regarding the product mix and due diligence process
- 2017: Terms and conditions for webshops are amended, requiring webshops to have local return addresses
- 2018: PayNow ends the outsourcing of insurance for payment defaults
- 2018: Ousting of dubious webshops
- 2018: Generic credit checks of consumers are replaced by more sophisticated risk assessments (price, tradability of goods)