Abstract. Digital platforms have radically transformed how we work, shop, and socialize. Despite their numerous benefits, they may also threaten social justice due to unforeseen or unintended consequences of specific design choices, preventing end-users from participating equitably in the digital economy. As platform owners compete by leveraging personal data, it remains unclear how digital platforms can be designed to empower end-users to control, legally own, and benefit from their data in a privacy-preserving way. Integrating design science research with heuristic theorizing, this study proposes a design theory for end-user-centric digital platforms. We derive design theory components from over nine years of data regarding the Dataswyft platform, including five meta-requirements and eight design principles. They reveal how digital platforms can be designed for social justice to address distributive and procedural social injustices by empowering end-users, both technically and legally, to protect and control their data through a containerized microservice platform infrastructure. This platform design includes multiple data protection layers, end-user-driven data collection, reconfiguration, and exchange functionalities, safeguarding mechanisms, and semi-centralized ecosystem governance structures. By evaluating an expository instantiation of the proposed design principles, we demonstrate the applicability and utility of our design theory, paving the way for data self-sovereignty and social sustainability.

Keywords: digital platforms, social justice, social sustainability, personal data control, data ownership, data privacy, end-user empowerment, design science

Suggested Citation:
1. Introduction

Digital platforms underlie nearly all modern industries, radically transforming the way we work (e.g., Salesforce), shop (e.g., Amazon), socialize (e.g., Meta), move (e.g., Uber), and travel (e.g., Airbnb). Until recently, public and academic interest primarily focused on the numerous ways digital platforms spur innovation, disrupt markets, and equalize access to services (Bharadwaj et al., 2013). However, high-profile incidents such as the 2018 Cambridge Analytica scandal and the 2021 Facebook Files highlight how digital platforms can also act as a “double-edged sword” (Cusumano et al., 2019), sometimes threatening social justice by infringing on fundamental human rights and values, such as privacy, safety, autonomy, fairness, equality, and democratic sovereignty (Cinnamon, 2017; Ransbotham et al., 2016). While information systems (IS) scholars increasingly acknowledge the “dark side” of digital platforms, exploration into addressing platform-related social injustices, especially for platform end-users, has only recently begun (e.g., Constantinides et al., 2018; Jacobides et al., 2024; Tarafdar et al., 2015; Zuboff, 2015).

Threats to social justice on digital platforms are typically tied to specific platform design choices (Edelman et al., 2017). Platform owners regularly make design choices as part of their value creation objectives and those choices often alleviate social injustices, from reducing non-consumption of marginalized consumers (Schaefer et al., 2018) to giving voice to minorities (Ransbotham et al., 2016). However, design choices may also have unforeseen or unintended consequences, and it is often unclear a priori whether they will impact end-users positively or negatively (Edelman et al., 2017). One such design choice relates to the way platform owners derive value by monetizing the personal data of their users (Sadowski, 2020). When using digital platforms, end-users produce digital trails of their behaviors, beliefs, and interests – from shopping habits and social relations to location and health data. Platform owners often generate substantial economic value by processing this data to personalize offerings, improve operations, and target advertising (Spiekermann et al., 2015). While end-users clearly benefit from enhanced platform services, prevailing platform design often hinders them from realizing equal value from their data. This disparity primarily stems from their inability to access the data they produce and their lack of expertise and technical tools to analyze their data to derive meaningful insights.

Based on Fraser’s (2008) theory of abnormal justice, platform design choices may therefore hinder parity among all platform participants by preventing “social arrangements that permit all to participate as peers in social life” (Fraser, 2008, p. 405). Resulting imbalances may lead to economic injustices of maldistribution, referring to the unequal distribution of resources, goods, and opportunities (Fraser 2008). Coupled with uncertainties about how platform owners collect, use, and protect end-user data (Al-Natour et al., 2020), data maldistribution may also inadvertently lead to privacy-related injustices of misrecognition and misrepresentation. Misrecognition refers to the failure to adequately recognize the contributions, identities, and experiences of all platform participants, especially those from marginalized groups, such as LGBTQ+ or ethnic minority users (Cui et al., 2020; Laouénan & Rathelot, 2022; Mejia & Parker, 2021). Misrepresentation, in turn, prevents all platform participants from having a voice in shaping the rules of how their data is used and how they are portrayed on digital platforms (Puntoni et al., 2021).

Preserving privacy and transferring control of personal data to end-users are often seen as pivotal steps in mitigating these obstacles to social justice (Cinnamon, 2017; Gal-Or et al., 2018). This shift requires platform owners to adopt design choices that promote “data self-sovereignty,” or end-users’ ability to exert “meaningful control, ownership, and other claims to data” (Hummel et al., 2021, p. 12) to ultimately improve social sustainability, including social equity and inclusion (Schoormann & Kutzner, 2021). Privacy regulations, like the European General Data Protection Regulation (GDPR), along with technological solutions, like personal data exchange platforms and management systems, have emerged to enhance end-user control and privacy. Yet, without adequate functionalities and safeguards to prevent end-user exploitation, these solutions may even exacerbate existing social injustices (Anciaux et al., 2019). Also, platform owners typically respond swiftly to privacy breaches and bias accusations, but often make reactive rather than proactive design changes, without necessarily addressing the root causes of these injustices, thus potentially amplifying platform failures (Jacobides et al., 2024; Sokol & Zhu, 2021).

In short, social injustices that emerge from a lack of end-user data control and privacy are “wicked problems.” Such problems are “poorly formulated, confusing, and permeated with conflicting values of many decision makers or other stakeholders” (Pries-Heje & Baskerville, 2008, p. 731). Their complexity requires a “wicked solution” that considers the diverse needs of all platform participants, as well as the solution’s potential technological, legal, and economic ramifications. Yet, extant IS literature does not offer prescriptive guidance on how digital platforms should be designed for social justice to address the wicked problems of data control and privacy. Thus, the research question of this study is: How can digital platforms be designed for social justice by empowering end-users to control and protect their personal data?

To answer this question, the present study integrates a design science research (DSR) approach (Gregor & Hevner, 2013; Hevner et al., 2004) with heuristic theorizing (Gregory & Muntermann, 2014). The purpose of this
study is to develop a design theory that “gives explicit prescriptions ... for constructing an artifact” (Gregor, 2006, p. 620) [i.e., a digital platform] that centers on social justice by empowering end-users to unlock the value of their data for their own (rather than primarily the platform owner’s) benefit. Drawing on over nine years of longitudinal data from the design, implementation, and evaluation of an end-user-centric digital platform, referred to as the Dataswyft API Platform (hereafter referred to as the Dataswyft platform), built on the open-sourced Hub-of-All-Things (HAT) Microserver, we derive a comprehensive set of design theory components (Gregor & Jones, 2007). These components include an outline of (a) the purpose of such a platform through the derivation of five meta-requirements (MRs), (b) the provision of eight design principles (DPs), and (c) the delineation of several testable propositions (TPs). We further demonstrate how each of the DPs can be implemented in practice by evaluating an expository instantiation of the proposed design theory (i.e., the Dataswyft platform) to attest sufficient proof of concept, proof of value, and initial proof of use (Nunamaker et al., 1990, 2011).

Our design theory represents the first attempt in IS literature to offer explicit guidance on how digital platforms can be designed to empower end-users to control and protect their personal data. Specifically, we extend IS research on end-user control (Gal-Or et al., 2018; Tsai et al., 2011) and data ownership (Al-Khoury, 2012) by showing how a containerized microservice platform architecture (DP1) facilitates legal data ownership (DP2) that provides the technical and legal basis for end-user control, and subsequently, data self-sovereignty (Hummel et al. 2021). By outlining how platform design can allow end-users to import, reconfigure (DP3), and exchange their data (DP4) with end-user-centric tools (DP5), we show how end-users can decide what data they share, with whom, and for what benefit. Advancing prior literature on personal data commercialization (Acquisti et al., 2016; Spiekermann & Korunovska, 2017), these DPs outline a novel way for end-users to transform their data into tradable assets, thereby mitigating economic injustices of maldistribution. Coupled with multiple data protection layers (DP6), semi-centralized governance (DP7), and continuous communication efforts (DP8), our study offers an alternative pathway for digital platforms to preserve end-user privacy and reduce injustices of misrecognition and misrepresentation. Instead of relying on regulation and privacy technologies alone (Al-Natour et al., 2020; Bélanger & James, 2020), our design theory allows end-users to choose which data to process and share, thus ensuring a more accurate representation (Puntoni et al., 2021), while allowing end-users to withhold more sensitive data, like race or LGBTQ+ status (Mejia & Parker, 2021). Collectively, our design theory showcases how digital platforms can be designed for social justice by providing a blueprint that enables platform owners to think through design choices that may foster economic fairness, equity, and inclusion, thereby contributing to the emerging field of social sustainability in IS research (e.g., Schoormann and Kutzner 2021).

This paper proceeds as follows: After a conceptual background, we detail our DSR approach. Next, the derived design theory components are presented, applied, and evaluated. We conclude with theoretical and managerial implications, and future research avenues.

2. Conceptual Background
2.1. Digital Platforms and Social Justice

Digital platforms refer to “a set of digital resources—including services and content—that enable value-creating interactions between external producers and consumers” (Constantinides et al., 2018, p. 381). Digital platforms share three characteristics: (1) they are mediated by technology, (2) they facilitate interaction between different groups of platform participants (e.g., producers, end-users, and third parties), and (3) they enable those groups to perform a defined task (Bonina et al., 2021). Beyond being an information technology (IT) artifact, a digital platform is a socio-technical entity, part of a “platform ecosystem” (Tiwana, 2015) with many economic, social, and institutional actors contributing to its functioning (Cecchagnoli et al., 2012). Despite their various benefits, digital platforms may also pose threats to social justice. These threats are often tied to specific platform design choices that may have unforeseen or unintended consequences (Edelman et al., 2017; Jacobides et al., 2024), which, in turn, may inadvertently prevent end-users from participating equitably in the digital economy. Following Fraser (2008), three obstacles to equal participation lead to social injustices: maldistribution, misrecognition, and misrepresentation.

The first obstacle, maldistribution, refers to end-users’ inability to benefit equally from their personal data while platform owners often gain disproportionately. Such “distributional failures” (Jacobides et al., 2024) may lead to economic injustices that typically stem from the way digital platforms are designed to extract value. Digital platforms usually extract value either by charging for service access (e.g., membership or per-use fees) or by monetizing user data for targeted advertising (Bonina et al. 2021). The latter design choice is common when end-users access a platform for free, creating a “data rent” scenario wherein end-users effectively pay with the data they produce when using those platforms, including content (e.g., likes) and metadata (e.g., location data) (Sadowski,
Both data types represent personal data or information related to an identified or identifiable natural person (Pangrazio & Selwyn, 2019). Rapid advances in data collection and analysis have rendered personal data a key resource for platform owners, while its value to end-users is less clear (Birch et al., 2021). Unlike platform owners, end-users often lack the access and tools to collect, store, and analyze their data to derive valuable insights, and the means to trade these insights for benefit. While new business models (Searls, 2012) and marketplaces (e.g., Swash or Ocean Protocol) envision end-users trading their data, and discussions on personal data valuation are ongoing (Acquisti et al., 2016; Spiekermann & Korunovska, 2017), it remains unclear how platforms can be designed for end-users to control and use their data as a tradable asset to overcome these economic injustices of maldistribution.

The second obstacle, misrecognition, often stems from platform design choices that may unintentionally reinforce social hierarchies that privilege some platform participants over others. Platforms can inherit societal biases if awareness of multiple user perspectives is not sufficiently considered during platform design, including design decisions about what types of end-user data to collect and when and with whom to share it. For instance, if there is insufficient recognition of the privacy needs of marginalized groups, such as ethnic minorities and LGBTQ+ individuals, misrecognition may emerge. For example, prior studies show that ethnic minority or LGBTQ+ end-users have different, more negative, experiences on ridesharing and rental platforms, from increased ride cancellations to lower earnings (Cui et al., 2020; Edelman et al., 2017; Laouènan & Rathelot, 2022). These injustices often arise from platform design choices that fail to foresee the potential discriminatory impact of sharing sensitive end-user data, such as race or LGBTQ+ status, with other platform participants. Thus, without explicit platform design that accounts for these privacy uncertainties, end-users may be unable to discern the privacy implications of the data they entrust to platforms (Al-Natour et al., 2020), while platform owners may inadvertently reinforce “institutionalized hierarchies … [resulting in] status inequality” (Fraser, 2008, p. 405).

The third obstacle, misrepresentation, occurs when end-users lack adequate representation in shaping or challenging the rules and decisions about how their data is used on platforms. This lack of decision-making control potentially weakens their voice against privacy violations, data misuse, and their inaccurate portrayal on platforms (Puntoni et al., 2021). Resulting injustices often stem from the way platforms are designed to process and handle end-user data (Zuboff, 2015), particularly in how they profile, target, or match end-users with other platform users or content. For example, the non-transparent sharing of sensitive end-user data, such as medical history, sexual orientation, or political affiliation, or end-users’ inability to influence algorithmic classification decisions regarding the content they see on platforms may lead to misrepresentation because platform owners may inadvertently establish “decision rules that deny [end-users] equal voice” (Fraser, 2008, p. 406) in how end-users want their data to be used on digital platforms.

Threats to social justice posed by digital platforms thus extend beyond economic injustices of maldistribution to challenges of misrecognition and misrepresentation. Importantly, these injustices are neither innate nor permanent features of any digital platform; they typically arise because of unforeseen or unintended consequences of specific platform design choices, whose effects on end-users—both positive and negative—are often unclear prior to their implementation (Edelman et al. 2017). However, designing digital platforms that address these three data control and privacy obstacles is a wicked problem, but also critical in establishing the distributive and procedural justice necessary to achieve equal participation in digital platforms (Fraser, 2008).

2.2. Data Control and Privacy as a Wicked Problem

Extant IS research underscores the “wicked” nature of problems related to data privacy and end-user control (Lowry et al., 2017). Both are abstract concepts that are created and upheld by legal, cultural, and organizational structures that differ across jurisdictions and societies. Data privacy, in particular, is recognized as notably wicked because privacy concerns vary widely among end-users (Plangger & Montecchi, 2020). Privacy in relation to information refers to “an individual’s self-assessed state in which external agents have limited access to information about him or her” (Dinev et al., 2013, p. 299). In contrast to general privacy, information privacy does not concern the physical access to an end-user or their private space, but instead the access to individually identifiable information, that is, personal data (Smith et al., 2011). Heightened privacy concerns can deter end-users from sharing personal data, or using location-based or personalized services (Dinev & Hart, 2006). For other end-users, however, privacy is not a major concern, and end-users may not take simple measures to improve privacy, even when they are readily available.

Wicked problems such as data privacy and control can thus not be solved piecemeal (Pries-Heje & Baskerville, 2008). For example, IS research has explored a range of privacy-enhancing technologies (e.g., cryptography tools, privacy-preserving interfaces) and approaches (e.g., privacy-by-design) to preserve end-user privacy (Lowry et al., 2017). However, limited research explores the unintended outcomes when end-users neglect their privacy, while much work on privacy technologies is either conceptual or disconnected from end-users, and
often overlooks societal implications (Bélanger & Crossler, 2011; Prat et al., 2015). In addition, IS literature has proposed different personal data management systems (PDMS) to enhance end-user data control. Instead of being hosted on corporate servers or company-managed cloud services, PDMS lets laymen end-users control the collection, storage, and dissemination of their data (Anciaux et al., 2019). Yet, various privacy and security risks remain, as most PDMS use centralized cloud infrastructure, often hosted by third parties, with limited tools to help non-expert end-users gauge the impact of granting data access to (often unvetted) third parties. PDMS are also closed systems that limit end-user-driven data exchange, let alone commercialization (Anciaux et al., 2019).

Thus, while prior solutions focus on addressing a particular facet of data control or privacy, they inadvertently create new challenges. Prior research has yet to examine data privacy and control as intertwined issues of the same wicked problem. Innovative platform design is therefore needed that centers on end-user empowerment to provide an equally “wicked solution” that takes a holistic perspective to address the three obstacles threatening social justice on digital platforms.

2.3. End-User Empowerment as a Wicked Solution

Wicked problems such as data privacy and control “cannot be parted or solved piecemeal…They can only be formulated in terms of a [wicked] solution. Their solutions are value-laden and cannot be denoted true or false, only good or bad. Their solution space is unbounded” (Pries-Heje & Baskerville, 2008, p. 731). Although wicked problems cannot be approached with certainty, we argue that an end-user-centric platform design is needed for a wicked solution to data privacy and control. Yet, centering platform design on end-user empowerment introduces new challenges in designing the platform’s 1) infrastructure, 2) its core functionalities, and 3) its ecosystem.

Regarding the design of the platform infrastructure, a layered modular architecture is needed, encompassing everything from the hardware to the software, to the data housed within the platform. Prior research shows how such an architecture would increase the flexibility of the platform (Yoo et al., 2010). The platform infrastructure must also enable end-users to legally own their data, as ownership is suggested to increase end-users’ willingness to share personal data (Gal-Or et al., 2018; Xu et al., 2012). However, to bestow legal ownership of data to end-users would require property rights such as the rights to possess, use, sell, or exclude others from one’s data (European Commission, 2016). While IS scholars increasingly call to “[c]larify intellectual property rights to establish [personal data] ownership” (Constantinides et al., 2018, p. 396), establishing such rights is challenging. Data often lack boundaries, and have multiple associations, and few jurisdictions consider it as property (Al-Khoury, 2012; Purtova, 2015). This issue remains unresolved even with progressive regulations such as GDPR, which overlooks data ownership rights (Milka 2018). Yet, adopting property rights would not only grant end-users full legal control over their data, thus enabling data sovereignty, but it would also enable the separation of data supply from demand, allowing markets to emerge. To date, however, personal data is usually stored centrally in organizational databases, preventing legal ownership by end-users.

In terms of platform functionalities, Iivari and Iivari (2011) stress system personalization as fundamental for end-user centeredness, referring to customizable technologies that are adaptable by, or automatically adaptive to, end-users given their unique needs or situations (Frias-Martinez et al., 2005). However, designing end-user-centric functionalities goes beyond improved usability, demanding a focus on end-user data control. Specifically, platform design should allow end-users to customize data control (Gal-Or et al., 2018) to ensure they can not only legally own their data but are also able to exchange their data with third parties as they see fit (De Hert et al., 2018).

Finally, regarding platform ecosystems, suitable governance structures need to ensure end-user control and privacy. Centralized governance offers platform owners complete data control, while decentralized governance enables end-users to collectively control the platform, reflecting their perspectives and using local insights. Chen and colleagues (2021, p. 1306) recognize the tradeoffs and propose a middle ground – a semi-centralized governance that suggests “a moderate level of decentralization is more likely to achieve incentive compatibility, improve informational efficiency, and help ensure desirable governance outcomes.” However, it is unclear how adopting such semi-centralized governance can spur the development of end-user-centric ecosystems.

Thus, despite these valuable insights, extant IS literature lacks guidance on designing digital platforms for end-users to own and manage their data with privacy, coupled with governance structures for data exchange in platform ecosystems – all of which are needed to design digital platforms for social justice and realize a wicked solution to end-user control and privacy. In short, a comprehensive design theory for end-user-centric digital platforms is needed.
3. Methodology
3.1. The Research Setting
To derive a design theory for end-user-centric digital platforms, we collaborated with researchers, developers, and end-users of Dataswyft (formally the HAT project). Starting in June 2013 with a £1.2 million research grant, the HAT involved 16 researchers from six universities in the United Kingdom (UK), before transitioning to a commercial venture. This study’s fourth author, a senior member of Dataswyft and former lead on the HAT project, provided access to the project. The other authors observed the HAT project and Dataswyft without direct involvement from June 2014 to February 2023, gaining first-hand insights into its development. These insights allowed all authors to jointly reflect on and learn from the development process of the Dataswyft platform, and to distill more abstract prescriptive design theory (Gregory & Muntermann, 2014).

3.2. Design Science Research and Heuristic Theorizing
We draw on DSR, a problem-solving process that generates design theory as prescriptive knowledge regarding the design of artifacts (Hevner et al., 2004; Peffers et al., 2007). Following Iivari’s (2015) DSR Strategy 1, we aim to create a conceptual IT meta-artifact that offers a general solution concept for designing end-user-centric digital platforms. Hevner et al. (2004, p. 76) describe artifacts as “innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, and use of information systems can be effectively and efficiently accomplished.” A design theory comprises six key components: (1) meta-requirements (MRs), (2) constructs, (3) principles of form and function (DPs), (4) artifact mutability, (5) testable propositions (TPs), and (6) justificatory knowledge (Gregor & Jones, 2007). Optional components include principles of implementation and expository instantiation. These components reflect the anatomy of a design theory and address two classes of problems, namely, end-user privacy and data control, despite their high uncertainty and complexity (Iivari, 2015). We use these components to organize and specify emergent design knowledge.

To systematically derive these components, we employ heuristic theorizing, referring to “the process of proactively generating design theory for prescriptive purposes from problem-solving experiences and prior theory [i.e., justificatory knowledge, referring to theories and literature from relevant disciplines, such as IS, marketing, and computer science, that provide necessary explanations for the design theory]” (Gregory & Muntermann, 2014, p. 639). Using heuristics (i.e., rules of thumb guiding problem structuring and artifact design generation), the heuristic theorizing process shifts between (1) the heuristic search for a satisficing solution to the problem (i.e., end-user control and data privacy) and (2) the heuristic synthesis of prescriptive insights (i.e., abstraction of insights from Dataswyft’s development). Heuristic search describes the iterative alignment of problem structuring and the derivation of satisficing artifact design components. This process involves creating solution candidates, assessing their fit with artifact requirements, and continuously refining the design of the artifact to meet evolving artifact requirements (Gregory & Muntermann, 2014). Heuristic synthesis, in turn, entails the extraction of prescriptive design knowledge from the substantial amount of information generated during heuristic search. This extraction requires reflection and learning that involves “select[ing] relevant pieces of information, abstract[ing] and relat[ing] these pieces of information to individual design theory components, and integrat[ing] them into a whole” (ibid., p. 646).

To synthesize design knowledge throughout the heuristic synthesis process, we collected data over 8.5-years from June 2014 until February 2023, covering a total of over nine years of longitudinal data from March 2013 until February 2023. We utilized a mix of various primary, archival, and secondary data sources (detailed in Table 1). Following Gregor and Jones (2007), the platform’s purpose was synthesized in five MRs, alongside principles of form and function made up of eight DPs. These components form the “abstract ‘blueprint’… for the construction of an IS artifact” (ibid., p. 326). To ensure the DPs satisfy the MRs, TPs were proposed, and justificatory knowledge was used to triangulate empirical evidence from the Dataswyft case. The Dataswyft platform further served as an expository instantiation of our proposed design theory.

<table>
<thead>
<tr>
<th>Table 1. Overview Data Sources, Documents, Codes, and Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Sources</strong></td>
</tr>
<tr>
<td>Interviews with leading HAT/Dataswyft developers (2014-2022)</td>
</tr>
<tr>
<td>Interviews with HAT beta users (2016-2017)</td>
</tr>
<tr>
<td>Survey responses of Dataswyft testers (2023)</td>
</tr>
</tbody>
</table>
3.3. The Heuristic Search and Synthesis Process

In total, we undertook three heuristic search and synthesis iterations, each involving alterations among multiple problem-structuring and artifact design heuristics, resulting in the iterative emergence and modification of wicked subproblems and respective MRs and DPs (see Table 2).
<table>
<thead>
<tr>
<th>Table 2. Evolution and Relationship Between Design Principles and Meta-Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design Principles (DPs)</strong></td>
</tr>
<tr>
<td><strong>First Heuristic Search Iteration (2013 – 2015)</strong></td>
</tr>
<tr>
<td>DP1: Enable Fully Secure and Private Personal Data Vault</td>
</tr>
<tr>
<td>DP2: Enable Secure Import and Export of Personal Data</td>
</tr>
<tr>
<td>DP3: Facilitate Personal Data Transformation for Enhanced End-User Value</td>
</tr>
<tr>
<td><strong>Second Heuristic Search Iteration (2015 – 2017)</strong></td>
</tr>
<tr>
<td>DP1: Enable Private Personal Data Storage</td>
</tr>
<tr>
<td>DP2: Establish Multiple Layers of Personal Data Security</td>
</tr>
<tr>
<td>DP3: Enable End-User Driven Personal Data Collection and Contextualization</td>
</tr>
<tr>
<td>DP4: Enable End-User Driven Personal Data Commercialization</td>
</tr>
<tr>
<td>DP5: Develop Data Management and Visualization Tools</td>
</tr>
<tr>
<td>DP6: Develop Multi-Sided Market Structures</td>
</tr>
<tr>
<td><strong>Third Heuristic Search Iteration (2017 – 2022)</strong></td>
</tr>
<tr>
<td>DP1: Adopt a Microservice Container Approach</td>
</tr>
<tr>
<td>DP2: Prioritize Legal Ownership to Maximize End-User Privacy and Control</td>
</tr>
<tr>
<td>DP3: Expand Security to Protect Personal Data at Rest, In Transit, and In Use</td>
</tr>
<tr>
<td>DP4: Enable End-User Driven Data Collection and Contextualization</td>
</tr>
<tr>
<td>DP5: Enable End-User-Controlled Personal Data Exchange</td>
</tr>
<tr>
<td>DP6: Establish Semi-Centralized Ecosystem Governance and Security Structures</td>
</tr>
<tr>
<td>DP7: Develop End-User-Centric Visualization and Management Tools</td>
</tr>
<tr>
<td>DP8: Continuous Communications with Current and Potential Platform Parties</td>
</tr>
<tr>
<td><strong>Final Design Principles 4.0</strong></td>
</tr>
<tr>
<td>DP1: Adopt a Decentralized, Containerized Microservice Platform Infrastructure</td>
</tr>
<tr>
<td>DP2: Prioritize Legal End-User Database Ownership</td>
</tr>
<tr>
<td>DP3: Enable End-User-Driven Data Collection and Contextualization</td>
</tr>
<tr>
<td>DP4: Enable Responsible End-User Controlled Data Exchange</td>
</tr>
<tr>
<td>DP5: Develop End-User-Centric Data Visualization and Management Tools</td>
</tr>
<tr>
<td>DP6: Establish Multi-Layered Security for Data at Rest, In Transit, and In Use</td>
</tr>
<tr>
<td>DP7: Establish Semi-Centralized Ecosystem Governance Structures</td>
</tr>
<tr>
<td>DP8: Continuous Communications with Current and Potential Platform Parties</td>
</tr>
</tbody>
</table>

Danatzis et al. (2024): Designing Digital Platforms for Social Justice – Author Accepted Manuscript
3.3.1. First Heuristic Search and Synthesis Iteration. The heuristic cycle began in May 2013 with framing the wicked problem. The use of problem-structuring heuristics revealed two interrelated wicked subproblems. First, HAT developers expressed concerns about personal data privacy and security (subproblem 1.1), citing risks from insufficient legal regulations and insecure data practices (COM-PR4). Second, they also stressed end-user exploitation (subproblem 1.2), with some describing access to platform services in return for end-user data as “robbery” (D5). Platform owners and third-party providers (but not end-users) were seen to benefit from end-user data. Hence, HAT developers decided “that it is time to rebalance this systemically, both through enabling technology and through the law” (COM-BP3) to design a platform that securely stores all end-user data to maximize privacy (MR1) and control (MR2). Drawing on artifact design heuristics, developers created working design components to address those subproblems and MRs, focusing initially on creating a fully secure personal data vault that would enhance privacy (DP1) and diminish end-user exploitation through maximum data security for importing and exporting data from the vault (DP2).

Yet, internal assessments revealed that such a vault would render the data unusable, leading HAT developers to return to problem-structuring heuristics. Drawing on problem reformulation, two new wicked subproblems emerged. One concerned end-user data ownership and control (subproblem 1.3) as “the data [that is] generated by individuals, doesn’t belong to us [end-users] but to those collecting it” (COM-WS2). HAT developers decided that “access and use of HAT data … [must be] controlled by the individuals … [including] tracking of all access to the HAT, its transaction entries into and out of the HAT, and any requests by any … [third]‐‐‐rd parties” (AAD1). The other dealt with the ambiguity of how end-users could benefit from their data (subproblem 1.4). HAT developers concluded that “personal data is like diamonds in the rough” (OE1). To enable end-users to harness the value of personal data (MR3), the platform must transform it to enhance its value for end-users (DP3). These artifact design components formed a satisficing working solution, resulting in a pre-alpha version of the HAT platform released to select developers in November 2014. Their feedback, guided by artifact design heuristics, refined the platform components, culminating in the release of the platform’s alpha version to a wider group of developers in November 2015, marking a first break out of the heuristic search cycle.

3.3.2. Second Heuristic Search and Synthesis Iteration. Following developer feedback, HAT developers re-entered the heuristic search cycle. Using artifact design heuristics alongside problem-structuring heuristics, they refined the platform’s storage (DP1) and security (DP2) architecture, but also identified two new problem areas. First, there was uncertainty about the platform’s functionalities and tools to transform imported data since they “still [don’t] pinned down the context” (D6) in which end-users utilize their data, as well as uncertainty about how those functionalities, tools, and user interfaces could best be “visualized, because” at the moment, [they were] hidden (D3) (subproblem 2.1). Second, it was unclear how the platform could be embedded in a wider personal data market, “providing [end-users] a safe place in which to trade [their personal data]” (COM-WS8) (subproblem 2.2).

To tackle subproblem 2.1 and ensure effective personal data collection, contextualization, and visualization (MR3), HAT developers created “Rumpel,” a personal data dashboard that lets end-users control “the access to and acquisition of ‘raw’ personal data” (AAD1) and its “transformation [by] creating a horizontal ‘row’ of time-sensitive contextual data relevant to [end-user] event[s]” (AAD1) (DP3). To tackle subproblem 2.2 and allow end-users to commercialize their data (MR4), developers created “MarketSquare,” a managerial tool linking end-users with platform issuers and third-party application providers, allowing them to directly exchange their data for monetary benefit (e.g., cash, discounts, rewards credits) (DP4). In pursuit of a multi-sided personal data market (MR5), developers also derived various regulatory, economic, and participatory market structures (DP6) in an “attempt to engineer [such a]… market” (AAD13). This involved outlining the roles and business models for all market participants and governance structures, leading to the creation of two entities: the ‘HAT Community Foundation’ (HCF) and the ‘HAT Data Exchange’ (HATDeX). A crowdfunding campaign raised over £50,000 to realize these design efforts. This paved the way for the HAT platform’s beta release in April 2016 and the first public launch in January 2017, marking the end of the second heuristic search cycle.

3.3.3. Third Heuristic Search and Synthesis Iteration. After feedback from application providers and end-users, the heuristic search cycle was re-entered. While artifact design heuristics were used to

---

1 All data source references are abbreviated. For example, “COM-PR” stands for “Press releases/news HAT/Dataswyft” while “D” stands for “Interviews with leading HAT/Dataswyft developers.” See Table 1 for an overview.
refine the platform’s functionalities (DP1–v3 – DP4–v3), a reassessment revealed the need to make the platform more commercially attractive. This meant giving end-users scalable control over the exchange of their data (subproblem 3.1) while demonstrating the platform’s industry value (subproblem 3.2), as developers emphasized the challenge in “translat[ing] the HAT’s…value proposition for practitioners” (OE4).

To address subproblem 3.1 and enable end-user-controlled data exchange (MR4–v3), artifact design heuristics were used to release improved exchange tools from January 2017 to September 2019 (DP5–v3, DP7–v3). The ongoing refinement of the platform’s regulatory, legal, and economic models specified the platform’s ecosystem (DP6–v3) “as a three-tiered … system” (COM-BD4) that integrates multiple parties at (1) the top/core level (end-users), (2) the service level (platform providers, application providers), and (3) the foundational level (HAT Foundation). The HAT platform was increasingly envisioned as an “infrastructure for personal data access, storage, and portability” (COMP-R11) with “personal data accounts” (PDAs) at its core. Using microservice containers, these PDAs represent a decentralized, “self-contained personal data storage solution” (COM-BD4), legally allowing end-users to license and share their data directly with third parties while retaining ownership and control of their data. To address subproblem 3.2 and foster an ecosystem centered on end-user data (MR5–v3), developers enhanced communication with relevant platform parties (DP8–v3) and launched an open innovation platform for business partnerships and a portal for startups. These efforts accelerated business interest and led to the development of new applications using PDAs. In February 2019, the first industry use case with OneZero-Me was realized, demonstrating the real-life utility of the platform and its data sharing practices.

In September 2019, Dataswyft secured £1.8 million in seed funding, leading to a separation of the HAT Microserver open-source code from the Dataswyft platform, which provisions and hosts the microservers for applications and provides the APIs to enable the access and use of the self-sovereign data within; and HATDeX to Dataswyft, focusing on global market acquisition. Dataswyft Ltd took over PDA rollouts, while HCF oversaw ecosystem regulation. New products were introduced (Dataswyft APIs, Jumpstart, and Dataswyft Plus) and cross-industry partnerships were initiated between September 2019 and February 2023. With a growing number of PDA owners (over 1,100 as of February 2023) and applications running (14 applications as of February 2023) or being developed on the Dataswyft platform, the platform ecosystem continues to grow, thus demonstrating its utility and potential to serve as a wicked solution, leading to the final break out of the heuristic search cycle.

4. A Design Theory for End-User-Centric Digital Platforms

4.1. Meta-Requirements and Constructs

Five MRs successively emerged through three heuristic theorizing iterations to address the wicked problems of 1) end-user data privacy and 2) control. The MRs outline the purpose and scope (the “causa finalis”; Gregor and Jones 2007) of end-user-centric digital platforms (as the class of artifacts): for end-users to legally own, control, and exchange their data in an ecosystem in a privacy-preserving way. They serve as “ends in mind … [to guide designers in finding] the means by which artifacts will achieve those ends” (Pries-Heje & Baskerville, 2008, p. 736), offering guidance for designing digital platforms for social justice and end-user empowerment. Each MRs is detailed in Table 3, while their evolution and relationship to DPs are detailed in Table 2. Constructs, on the other hand, refer to “representations of the entities of interest in the theory … [building] the most basic level in any [design] theory” (Gregor & Jones, 2007, p. 325). Describing “what” is being designed, the constructs of our design theory entail the different layers of digital platforms. Drawing on Tiwana et al. (2010), digital platforms typically consist of four layers: 1) the platform infrastructure, 2) the platform core, 3) the platform interfaces, and 4) the platform ecosystem. Each construct and their links to each other are detailed in Table 3. Next, we delineate eight DPs that outline “how” to design each of these four elementary constructs.

<table>
<thead>
<tr>
<th>Table 3. Meta Requirements and Constructs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meta Requirements (MRs)</strong></td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td><strong>MR1: Personal Data Privacy and Security</strong></td>
</tr>
<tr>
<td>MR1 addresses the challenges associated with ensuring data privacy and security in end-user-centric digital platforms (see subproblem 1.1). This is because end-user-centric systems are especially prone to risks of “releasing information from [prior] loosely-related personal data [that] has even more troubling implications for individual privacy” (Jiang &amp; Landay, 2002, p. 59). Although privacy breaches may not be intentional, such platforms cross personal boundaries which results in data collected from the lives of end-users where even “a few privacy violations could lead to user distrust and abandonment” (ibid., p. 60). The platform should therefore be engineered as “a platform for securely storing the totality of [end-user] data” (COM-WS8) to reduce privacy uncertainties (Al-Natour et al., 2020).</td>
</tr>
</tbody>
</table>

Danatzis et al. (2024): Designing Digital Platforms for Social Justice – Author Accepted Manuscript 10
MR2: Personal Data Control

MR2 centers on allowing end-users (not platform owners, application providers, or other third parties) to maximally control their personal data within the platform (see subproblems 1.2 and 1.3). Specifically, digital platform design should rebalance power and control asymmetries by allowing the “access and use of ... [personal data to] be controlled by the individuals through the [platform’s] architecture ... The tracking of all access to the platform, its transaction entries into and out of the platform, and any requests by any other [third parties that are not the individual ... [must be] audited and available to the individual” (AAD1). Such platform design would increase end-users’ willingness to share personal data and encourage data dissemination across platform participants (Gal-Or et al., 2018; Phelps et al., 2000; Xu et al., 2012).

MR3: Personal Data Collection, Contextualization, and Visualization

MR3 highlights that end-user-centric digital platforms must provide functionalities to allow end-users to collect, reconfigure, and visualize their data (see subproblems 1.4 and 2.1). The platform design should enable the transformation of isolated pieces of personal data into useful end-user resources (Currin & Ram, 2012). Thus, platform design should support end-user involvement in constructing dynamic ways of collecting, combing, and visualizing data, thereby increasing the value of personal data to end-users and third parties.

MR4: Personal Data Exchange

MR4 emphasizes the importance of allowing end-users to exchange their personal data for monetary and non-monetary benefits (see subproblem 1.4, 2.2, and 3.1). Specifically, end-user-centric digital platforms should enable end-users to buy services to use their data or exchange it for some benefit (DES5). This requires the creation of compelling applications that make use of ubiquitous access to personal end-user data and preferably real-time data exchange among end-users and third parties (Phelps et al., 2000). Platform design should thus provide revenue generation opportunities to support the platform’s profitability and adoption (Cusumano et al., 2019) while implementing safeguarding mechanisms to ensure that third parties are trustworthy and that end-users fully understand the impact of their exchange decisions (Aniaux et al., 2019).

MR5: Platform Ecosystem Centering on Personal Data

MR5 emphasizes the need to create a platform ecosystem that centers on end-user-controlled personal data and connects end-users, application providers, and other (non-)commercial third parties (see subproblem 2.2 and 3.2). Platform design should establish appropriate ecosystem governance structures that regulate 1) access to the platform, 2) the interactions on the platform, and 3) enforce regulatory compliance among platform participants (Chen et al., 2021; Hagiu, 2014). Platform architecture should further be modular and scalable to accommodate changes in the number of platform users (Yoo et al., 2010). Finally, to reach the critical mass of participants that is crucial for platform success, platform design should clearly delineate the roles, business models, technical requirements, and benefits to all platform participants (Cusumano et al., 2019).

Constructs

Construct 1: Platform Infrastructure

The platform infrastructure is the foundation of any digital platform and refers to the underlying socio-technical system that provides the necessary digital infrastructure, such as computing and network resources, to enable the platform’s functionality (Constantinides et al., 2018). Controlled by the platform owner and largely hidden from the end-user and third parties, it encompasses the back end of the platform, including servers and storage. Its design —often irreversible— significantly impacts the performance and scalability of the platform, as well as its ability to ensure data security, privacy, and control, and must accommodate for future changes unforeseen when the platform is created (Tiwana et al., 2010).

Construct 2: Platform Core

The platform core sits on the platform infrastructure and consists of tightly coupled components (Constantinides et al., 2018). These components provide the platform’s “core functionality shared by the modules that interoperate with it and the interfaces through which they interoperate” (Tiwana et al., 2010, p. 676). The platform core consists of several core modules in the form of applications, each extending the platform’s functionality. These modules can be understood as “add-on software subsystems” (Tiwana et al., 2010, p. 675) or “executable pieces of software that are offered as applications, services or systems to end-users” (Ghazawneh & Henfridsson, 2013, p. 175) that may also be developed by third parties (Bonina et al., 2021).

Construct 3: Platform Interfaces

The platform interfaces describe the boundaries of modules, referring to the “[s]pecifications and design rules that describe how the platform and modules interact and exchange information” (Tiwana et al., 2010, p. 675). Interfaces can be internal and external and act as boundary resources between the platform owner, end-users, and other third party providers (Bonina et al., 2021). The design of interfaces are crucial as “[c]ontrol over interfaces [ultimately] amounts to control over the platform and its evolution” (Tiwana et al., 2010, p. 680).
Construct 4: Platform Ecosystem

The platform ecosystem refers to the platform’s periphery and the “collective of organizations having a common interest in the prosperity of a digital platform for leveraging their application development” (Ghazawneh & Henfridsson, 2015, p. 200). Ecosystem design decisions include setting rules for end-users and third parties to follow to ensure interoperability (Tiwana et al., 2010) and platform governance structures to determine the degree of control each party exerts in the platform ecosystem (Chen et al., 2021).

4.2. Principles of Form and Function (Design Principles)

Eight principles of form and function iteratively emerged from the development of the Dataswyft platform. All final DPs and their TPs are detailed next, which form the core of our proposed design theory (Gregor & Jones, 2007). For a graphical overview see Figure 1, and for a summary of their evolution and respective links to MRs, see Table 2.

**4.2.1. Design Principle 1: Adopt a Decentralized, Containerized Microservice Platform Infrastructure.** Design principle 1 (DP1) postulates that end-use-centric digital platforms should adopt a decentralized, container-based microservice architecture for the infrastructure of end-user-centric digital platforms to enable flexible and scalable management of servers, storage, and services while facilitating end-user data privacy and control. Addressing personal data privacy and security (MR1) and control (MR2), DP1 proposes that end-user-centric digital platforms require a platform architecture that enables a high degree of flexibility and end-user control (Tiwana, 2015; Yoo et al., 2010). Being one of the key insights of the heuristic theorizing process, the Dataswyft developers concluded that end-user data should not be “stored in an account-based system, where each user is a (series of) records in a database hosted by a service provider, but [instead in one where end-user data is] ideally stored in a (virtual) private server that is accessible only to the user” (COM-BD7). Adopting a microservice architecture was judged as the best approach to meet this requirement. This architecture pattern entails microservices – applications composed of sets of small, decoupled services (Newman, 2015), each having its own database that allows them to be deployed independently. Unlike traditional monolithic architecture in which end-user data is stored...
in a centralized firm database, a microservice architecture allows for the decentralized storage of end-user data, enabling greater data privacy and control for end-users.

When it comes to deploying microservices, Dataswyft developers favored containerization over traditional hypervisor-based virtual machines, as the latter would be too costly for mass deployment due to their limited application scope (COM-BD7). Recent literature supports their decision, highlighting containerization as a high-performing and scalable deployment alternative, particularly suitable for decentralized data storage and edge computing (Fan et al., 2020). Docker containers wrap “a complete system that contains everything it needs to run: code, runtime, system tools and system libraries” (COM-BD7), enabling several containers to run microservices in isolated processes on the host operating system, sharing the same kernel for more efficient use of system resources, greater portability, and scalability. Unlike virtual machines, containers also offer end-users more granular control over data access and use (Docker Website, 2023).

While some security risks still exist with such an architecture, recent research shows that implementing continuous deployment systems can effectively mitigate them (Brady et al., 2020). Hacking individual containers is also less appealing, as they only reveal data of single end-users, thus discouraging mass attacks. Hence, combining a container-based microservice architecture with additional data protection layers (DP6) can balance costs, flexibility, security, privacy, and end-user control. Thus, we posit adopting this approach for end-user-centric digital platforms to maximize end-user data control (TP1.1) and ensure efficiency (TP1.2), and scalability (TP1.3).

4.2.2. Design Principle 2: Prioritize Legal End-User Database Ownership. Design principle 2 (DP2) posits to prioritize legal end-user ownership of databases to maximize end-user privacy and control over personal data by granting end-users property rights over stored data. Addressing personal data privacy (MR1) and control (MR2), DP2 emphasizes that platform design should maximize end-user control and privacy through the provision of legal rights over the use of their data. While different privacy-enhancing technologies, such as database anonymization or data set encryption have been proposed (Terrovitis et al., 2008), Dataswyft’s experiences reveal that facilitating legal ownership of databases offers the most effective means of providing end-users with data rights (see also Al-Khoury 2012). Adopting a container-based microservice platform infrastructure (see DP1) can fulfill this requirement. By enabling end-users to push and pull data into their containerized private databases, this approach enables end-users to become data controllers under the law (Regulation (EU) 2016/679). This is important because many jurisdictions recognize data controllers as the gatekeepers of personal data (Reding, 2012), providing end-users full custodial rights over their personal data, both technically and legally. In the digital context, custodial rights refer to the right of a party (in this case, the end-user) to grant permission to access, use, and exchange personal data, i.e., the right to give rights (COM-BP5). This way, end-user control over personal data stored within their containerized private databases can effectively be established, maximizing end-user privacy. Thus, we posit that facilitating legal database ownership for end-users maximizes their data control and privacy and is more effective than third-party privacy-enhancing technologies (TP2.1). Further, providing end-users with custodial rights over personal data is necessary to ensure data privacy and control (TP2.2.).

4.2.3. Design Principle 3: Enable End-User-Driven Data Collection and Contextualization. Design Principle 3 (DP3) postulates that end-user-centric digital platforms should enable end-users to import and reconfigure their personal data from multiple data sources to derive superior insights and maximize their value for both end-users and firms. DP3 is a core functionality of end-user-centric digital platforms that addresses data collection, contextualization, and visualization (MR3). It posits how platform design should allow end-users, rather than the platform owner or any third party, to import and contextualize their data within the platform, reconfiguring or recombining it to generate more meaningful insights. Specifically, data import should be automated using platform-ready services that input end-user data from Internet-connected devices (e.g., sensor data) or applications (e.g., online calendars), as well as third-party data, such as public transportation or weather information. To facilitate contextualization, end-user-centric digital platforms should implement a schema and provide tools that allow end-users to bundle and reconfigure their collected data within applications according to different entities of interest to them or third parties, such as things, persons, locations, or events. Such a horizontal data approach would allow personal data to be “contextualized” as it would enable end-users to link and reorganize vertical data points to fit their understanding and use of data in their personal lives. This aligns with literature on context-aware (edge-)computing (Perera et al. 2014; Zhu et al. 2014) and end-user-centered systems personalization (Frias-Martinez et al. 2005). Thus, we posit that contextualized, horizontal data will be more valuable for end-users (TP3.1) and profitable for firms (TP3.2) than non-contextual, vertical data; particularly when data contextualization is driven by the end-user as opposed to the platform owner or a third-party provider (TP3.3).
4.2.4. **Design Principle 4: Enable Responsible End-User-Controlled Data Exchange.** Design principle 4 (DP4) posits that end-user-centric digital platforms should enable end-users to responsibly exchange personal data with third parties with full control over which data is shared, with whom, for how long, and for what monetary or non-monetary benefit, while implementing safeguards to prevent exploitation and minimize user error. Addressing the exchange of personal data (MR4), privacy (MR1) and control (MR2), DP4 articulates another core functionality of end-user-centric digital platforms. It emphasizes how platform design should ensure that end-users decide which data to share, with whom, for which duration, and for what (non-)monetary benefit in return. This can be realized in two ways: End-users can either (1) give permission to others to access certain subsets of their data or (2) install applications that exchange data from their private database with third-party providers. To achieve this, the platform database must offer a “common semantic structure” (COM-BD7), be open-sourced, and accommodate a regulatory system that grants end-users access (i.e., gives explicit permission) to each defined subset of their data.

In addition, platform design should enable end-users to either (a) sell or (b) license (bundles of) their data. Selling data grants third parties permission to process it on their servers, leaving end-users with limited data control. Licensing data, on the other hand, ensures that it is processed according to licensing rules with legal recourse, maximizing end-user data control. However, in both cases, appropriate safeguard mechanisms should be implemented to ensure end-users fully understand the impact of their decisions to promote responsible exchanges, prevent end-user exploitation, and minimize user error (Anciaux et al., 2019). DP4 therefore ensures the platform is not just a private and secure vault where end-users “lock-up” their data, but rather a platform that allows for the development of services that commercialize end-user data. This, in turn, facilitates value creation both for end-users and firms (rather than only the latter), spurring the development of a platform ecosystem centered on end-user empowerment (Ceccagnoli et al., 2012; Kahl & Grover, 2008; Tiwana, 2015). Hence, we posit that responsible personal data exchange that is primarily controlled by the end-user as opposed to the platform owner or third-party providers will generate greater (non-)monetary value for both end-users (TP4.1) and firms (TP4.2), particularly when platform functionalities incentivize licensing over selling data (TP4.3).

4.2.5. **Design Principle 5: Develop End-User-Centric Data Visualization and Management Tools.** Design principle 5 (DP5) posits that end-user-centric digital platforms should develop intuitive and user-friendly graphical interfaces and user-driven data management tools that allow end-users to easily visualize, monitor, and control the collection, analysis, reconfiguration, and exchange of their personal data with third parties. Addressing personal data control (MR2), collection, contextualization, and visualization (MR3), exchange (MR4), and platform ecosystem (MR5) requirements, DP5 refers to the interfaces of end-user-centric digital platforms. It highlights that the platform’s core functionalities (DP3 and DP4) rely on effective user interfaces and end-user-centered management tools. Evidence from the Dataswyft project suggests that at least two interfaces should be provided: First, an internal interface like a personal dashboard tool, that allows end-users to visualize and control the collection and contextualization of their data. Such a tool would represent a space for end-users to collect, store, and (re-)organize their data for subsequent data exchange. Second, an external interface such as a digital marketplace tool that connects all platform ecosystem participants (Ghazawneh & Henfridsson, 2013) would allow end-users to claim their data and accept offers from other end-users or third parties. Hence, we propose that at least one inward- (toward the end-user) and one outward- (connecting all platform participants) visualization and management tool should be embedded in the platform to enhance the user experience (TP5.1) and ensure responsible end-user-driven data exchange (TP5.2).

4.2.6. **Design Principle 6: Establish Multi-Layered Security for Data at Rest, In Transit, and In Use.** Design Principle 6 (DP6) suggests that end-user-centric digital platforms should establish multiple layers of end-user data protection to ensure authorized access, recovery, and security of personal data when it is stored (at rest), transferred (in transit), and processed (in use). Addressing personal data privacy and security (MR1), DP6 refers to the design of the platform infrastructure, the core, and interfaces. It addresses prevalent security challenges in digital platforms such as confidentiality, integrity, availability, performance, accountability, and maintenance risks (Ackermann, 2013) across the three main states of data: (a) data at rest (i.e., when personal data are inactive and stored within the server’s storage), (b) data in transit (i.e., when personal data are downloaded, uploaded, or transferred between data storages), and (c) data in use (i.e., when personal data are processed by the end-user or other third-party services) (Ramachandran & Chang, 2016). This aligns with Dataswyft developers’ conclusions that digital platforms should be designed to ensure “security of the data including (1)
integrity that ensures information is not altered during transit and storage; (2) access: authentication that addresses the verification of a user’s identity and eligibility to data access; (3) and confidentiality that requires data use is confined to authorized purposes by authorized people” (AAD1).

Specifically, when end-users’ personal data are at rest, data should be protected on two levels: (a) at the storage system and (b) at its underlying system architecture (Zissis and Lekkas 2012). When personal data is in transit, communication (and thus, data input/output) among end-user databases or other services using an end-user’s data should be limited to designated encrypted APIs to prevent potential security issues from other data input/output channels. Generally, end-users should review and approve all data input/output and the platform’s infrastructure should be protected from unauthorized access using industry-standard protection techniques. To ensure the security of an end-user’s personal data in use, data should be protected at the level of (a) managerial usage and (b) third-party usage. Managerial usage, referring to the ability and rights to process data stored within the storage system, should solely be made available to the end-user as the owner of that storage. Third-party usage, in turn, is closely linked to the governance and design of the platform’s ecosystem (see DP7). However, the security of personal data should not only be enforced technologically, but also through the establishment and enforcement of privacy, security, confidentiality, compliance (PSCC) principles, and corresponding policies, codes of practices, and legal contracts for personal data exchange. These multiple layers of protection for personal data in rest, transit, and use are fundamental to platform success, exceeding the level of end-user data security protection of existing PDMS and other solutions due to its decentralized nature and reduced surface area of attack (Anciaux et al., 2019).

Hence, we propose that digital platforms need to protect the personal data of their end-users at rest, transit, and use to safeguard end-user control and privacy (TP6.1). We also propose that effective PSCC principles should complement technological measures to ensure appropriate third-party access, usage, and exchange of data throughout the platform’s ecosystem (TP6.2).

4.2.7. Design Principle 7: Establish Semi-Centralized Ecosystem Governance Structures. Design Principle 7 (DP7) suggests that the design of end-user-centric digital platforms should establish semi-centralized ecosystem governance overseen by an independent organizational entity that enforces regulatory compliance to safeguard end-user control and privacy and ensure trusted data flow among platform participants. Addressing the importance of platform ecosystems (MR5), DP7 emphasizes that platform design should adopt semi-centralized ecosystem governance that “is characterized by giving community members freedom and rights to participate in platform governance while having some key organizations or individuals sponsor and shape platform governance” (Chen et al., 2021, p. 1311). Overcoming shortcomings of overly (de)-centralized platform governance, semi-centralized governance allows trusted key parties to overlook governance processes to avoid deadlocks, overcome impasses, ensure checks and balances, and allow effective rule enforcement (Chen et al., 2021; Fan & Zietsma, 2017). Evidence from the Dataswyft project further suggests that ecosystems of end-user-centric digital platforms should comprise three tiers: (1) the core level, (2) the service level, and (3) the institutional level (COM-BD4). The core level includes the platform’s end-users, while the service level encompasses platform issuers (i.e., organizations that host and deploy platforms to end-users) and application providers (i.e., firms that develop, sell, and run applications on the platform). Finally, the institutional level includes the regulatory system realized by a community-based, non-profit foundation governing the ecosystem (COM-BD4) and reinforcing self-regulation by its members. In addition, PSCC principles should be established; this could include a requirement that all third parties undergo a certification process before receiving (temporary) access to end-user data, ensuring uniform security standards across the ecosystem.

Hence, we propose the adoption of a semi-centralized ecosystem governance structure controlled by an independent organizational entity as a more effective way to ensure end-user data control and privacy compared to (de-)centralized platform governance (TP7.1). This entity should be regulated by its members to enhance platform adaptability (TP7.2) and monitor and enforce privacy and security rules across all platform participants to foster end-user trust (TP7.3).

4.2.8. Design Principle 8: Continuous Communications with Current and Potential Platform Parties. Design Principle 8 (DP8) suggests that end-user-centric digital platforms should engage in continuous communication efforts with current and potential platform parties to promote the value of end-user-centric data exchange, highlighting the benefits for end-users to understand the value of their data and its potential uses, and the benefits for firms to incentivize their participation. DP8 highlights the need of ongoing communication in platform ecosystems (MR5) as an essential aspect of design efforts to attract “a ‘critical mass’ of consumers and producers on a platform” (Boudreau, 2012, p. 1411). Hence, we propose that to reach a critical mass of platform
participants, ongoing communication must be prioritized from the outset of the platform design efforts, with considerable intensification upon platform release (TP8.1).

4.3. Artifact Mutability
The three rounds of heuristic theorizing illustrate the ongoing evolution of our conceptual IT meta-artifact (and its MRs, DPs, and TPs) (Ilivari, 2015), from an initial focus on the delineation of the platform’s infrastructure and core functionalities (first iteration) to the development of its interfaces and exchange systems (second iteration) to the advancement of its ecosystem (third iteration), with each iteration building on the previous one to create more effective design theory (see Table 2). Nevertheless, our design theory components allow for further refinement. While we expect the MRs and DPs related to the platform’s infrastructure (DP1 and DP2) and its core functionalities (DP3 and DP4) to remain relatively stable, changes are more likely to occur in the ecosystem and its interfaces (DP5-DP8) as developers, end-users, and third parties identify new (wicked) challenges and opportunities for improvement. Such ongoing adaptation ultimately fosters the growth of the platform ecosystem, which is key to platform success (Boudreau, 2012).

5. Demonstration and Evaluation
Evaluation of DSR contributions entails two sub-activities: demonstration and evaluation (Peffers et al., 2007). Demonstration indicates the ability of the IT meta-artifact (as exemplified in our DPs) to address the identified research issues while evaluation seeks to validate its effectiveness. However, handling the demonstration and evaluation phase as independent and concluding stages is misleading, especially since a “concept-to-finish” solution is impossible to achieve for complex, wicked problems within a single study (Pries-Heje & Baskerville, 2008). Instead, and in keeping with Ilivari’s (2015) DSR Strategy 1, we follow Nunamaker et al.’s (1990, 2011) multi-methodological model that emphasizes how “major design science contributions to knowledge are made as concepts are defined, moved to the proof-of-concept [demonstration], proof-of-value, and finally proof-of-use stages [both evaluation] through a long-term, sustained stream of research studies” (Twyman et al., 2014, p. 109). This study falls between the categories of proof of value and proof of use, as we provide sufficient proof of concept and proof of value, and initial proof of use for our proposed design theory which we detail next in the following two sections.

5.1. Demonstration of the DPs: Expository Instantiation and Principles of Implementation
To demonstrate our DPs’ utility, we apply them to the Dataswyft platform and outline respective principles of implementation (Gregor & Jones, 2007). In line with Ilivari’s (2015) DSR Strategy 1, the Dataswyft platform serves as an expository instantiation of our IT meta-artifact and thus as a real system implementation of our design theory to provide the basis for its subsequent evaluation. While several working versions of the platform were developed, we solely report the application of the DPs on its most recent version, which are summarized in Table 4 (see Figure 2 for illustrations of core functionalities). We demonstrate proof of concept by evaluating the instantiation against our previously derived MRs. According to Nunamaker et al. (2011, p. 25-26), proof of concept “requires building and testing a prototype system under laboratory conditions to determine if the proposed technology actually works.” The Dataswyft platform can be characterized as sufficiently developed. Importantly, Gregory and Muntermann (2014, p. 646) note that at this stage it “is important to ensure that the artifact design “works” in the eyes of those who experience the problem at hand in practice” – in this case, the Dataswyft developers. As detailed in Table 5, sufficient proof of concept can be attested for each of the MRs.

<table>
<thead>
<tr>
<th>Table 4. Deriving Principles of Implementation by Applying the Proposed Design Principles to the Dataswyft Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPs</td>
</tr>
<tr>
<td>DP1: Adopt a Decentralized, Containerized Microservice Platform Infrastructure</td>
</tr>
<tr>
<td>DP2: Prioritize Legal End-User Database Ownership</td>
</tr>
<tr>
<td>DP3: Enable End-User-Driven Data Collection and Contextualization</td>
</tr>
<tr>
<td>DP4: Enable Responsible End-User-Controlled Personal Data Exchange</td>
</tr>
<tr>
<td>DP5: Develop End-User-Centric Data Visualization and Management Tools</td>
</tr>
<tr>
<td>DP6: Establish Multi-Layered Data Security for Data at Rest, In Transit, and In Use</td>
</tr>
</tbody>
</table>
| DP7: Establish Semi-Centralized Ecosystem Governance Structures | Ecosystem Governance Structures: Semi-centralized ecosystem oversight is realized through the “HAT Community Foundation” (HCF). The HCF is a non-profit public initiative that ensures that all ecosystem participants adhere to PSCSS principles such as adherence to global privacy standards and the scope, consent, collection, use, retention, exchange, access, and security of personal data. Datasywyft Ltd facilitates the provisioning of PDAs and enables the use of PDAs within them by establishing the necessary contracts and permissions between PDA owners and application owners who wish to operate within the platform ecosystem. **Ecosystem Security Structures:** For data at rest, a wide range of AWS built-in security solutions are used. For data in transit, all application providers are required to undergo a review process based on Datasywyft’s PCSS principles. For data in use, application
providers must adhere to Dataswyft’s code of practice and are obliged to disclose how they want to use end-user data and to demand access to specified data bundles.

| DP8: Continuous Communication with Current and Potential Platform Parties | Targeted and continuous communication efforts are conducted toward all potential platform stakeholders, including end-users, firms, developers, media, academia, and other public institutions using a wide range of online and offline channels, such as various social media channels, websites, videos, blogs, the Dataswyft community and developer forum, chat rooms, emails, press releases, journal, and conference papers, as well as designated Dataswyft events. |
Figure 2. Illustrations of Core Functionalities and Interfaces (Design Principles 3-5)
Table 5. Proof-of-Concept and Proof-of-Value Evaluations (Early Adopters) of the Dataswyft Platform

<table>
<thead>
<tr>
<th>MRs</th>
<th>Proof-of-Concept Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MR1: Personal Data Privacy and Security</strong></td>
<td>The use of docker containers reduces the risk of large-scale security breaches, as each PDA container runs isolated from one another. Communication between individual PDAs or other third parties is restricted to user-controlled APIs. The Dataswyft platform further implements multiple layers of data protection. All methods were subject to several rounds of internal auditing and were judged to be reliable. Furthermore, neither developers nor beta testers or active users reported any privacy or security breaches since the release of the beta version.</td>
</tr>
<tr>
<td><strong>MR2: Personal Data Control</strong></td>
<td>The Dataswyft’s microservice container approach of PDAs prevents end-user data from being mixed with other data from other users or third parties with code-level execution and control. The Dataswyft’s PDA containerization is therefore the technical operationalization to meet the legal requirement to grant end-users property rights and full custodial rights over their personal data. Within the Dataswyft ecosystem, these rights are safeguarded through contractual agreements between application owners and the PDA owners set up by Dataswyft and the application rating, review, and risk assessment process, under the oversight of the foundation. In this way, custodial rights guarantee that each PDA is controlled by the end-user.</td>
</tr>
<tr>
<td><strong>MR3: Personal Data Collection, Contextualization, and Visualization</strong></td>
<td>Different data plugs allow for the collection of personal data within the PDA storage system that can then be transformed through the PDA’s schema. While no issues were documented with the schema, some technical issues have been documented with the setup of some data plugs. Similarly, during beta-testing, the developers experienced minor technical issues as well as problems with Rumpel. Accordingly, efforts were made to fix the bugs and increase the usability and reliability of the platform and all its functionalities.</td>
</tr>
<tr>
<td><strong>MR4: Personal Data Exchange</strong></td>
<td>Dataswyft developers designed and implemented the data debit system to facilitate the exchange of personal data between end-users and third-party application providers. Since the beta version was released, developers have not reported any major issues with the data request system. Similarly, beta and active user evaluations of the system have also been predominantly positive.</td>
</tr>
<tr>
<td><strong>MR5: Platform Ecosystem Centering on Personal Data</strong></td>
<td>The HAT project transitioned from a research project to an end-user-centric digital platform with an ecosystem including over 11,000 users (as of February 2023) and various application providers across different industries. With the Dataswyft PDA’s being lightweight and built on containers, it is portable across devices, thereby allowing more parties to join the ecosystem, without minimal lock-in or proprietary risks. However, while the platform ecosystem is growing, the Dataswyft developers recognize the need to further attract more third-party industry partners and other commercial and non-commercial partners who wish to build applications and offer services on the Dataswyft platform.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MRs</th>
<th>Proof-of-Value Evaluation (Early Adopters: Beta Version 2017-2018)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MR1: Personal Data Privacy and Security</strong></td>
<td>Early adopter evaluations were predominantly positive and early adopters were mostly comfortable with storing data on their PDA. Although there were some concerns about the PDA being hacked, most early adopters felt that the platform’s design of using isolated microservice containers would deter hackers because it would not be worth the effort to hack an individual account as opposed to centralized databases. The ongoing requirement to give explicit permission for all data input/output to and from their PDAs was also seen to increase perceptions of altered end-user privacy.</td>
</tr>
<tr>
<td><strong>MR2: Personal Data Control</strong></td>
<td>Early adopters of the Dataswyft platform recognized the importance of control over personal data and believed that the management of data would be a ubiquitous skill in the future. Early adopters felt that using the Dataswyft platform gave them greater control and power over their personal data by enabling them to better appreciate what type of data is collected, when it is collected, and by whom it is collected for which purpose.</td>
</tr>
<tr>
<td><strong>MR3: Personal Data Collection, Contextualization, and Visualization</strong></td>
<td>The idea to transform their personal data through platform functionalities was received positively by early adopters. The dashboard’s mashup function was popular, although some early adopters did not understand its function and demanded further explanation or specific usage showcases. Overall, early end-users appreciated the idea of reconfiguring, bundling, and transforming data, but expressed difficulty using the interface. They recognized that the Dataswyft platform was still in development.</td>
</tr>
</tbody>
</table>
at this stage, and it was their perception of the future value of the Dataswyft platform that kept them engaged.

<table>
<thead>
<tr>
<th>MR4: Personal Data Exchange</th>
<th>Beta users’ evaluations of the data debit system were predominantly positive. However, while the concept of data exchange was mostly positively received, most early adopters did not indicate that they stored or traded personal data at that stage. Nonetheless, early adopters could see the promise of the possibility to do so in the future but were limited by the user interfaces of the beta version and the availability of options for exchanging personal data given the lack of third-party applications and services on the platform at that time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MR5: Platform Ecosystem Centering on Personal Data</td>
<td>At the time of the beta version release in 2017, a vibrant platform ecosystem had not yet come to fruition. However, a platform ecosystem with early use cases was beginning to emerge, including several researchers, application providers, and end-users who recognized the potential value of the Dataswyft platform and continued to apply their knowledge and skills for the benefit of others, even though the demand for this type of platform was largely unknown at the time.</td>
</tr>
</tbody>
</table>

5.2. Evaluation of the DPs: Practitioner and End-User Evaluations

To evaluate the effectiveness of our DPs, we next assess the proof of value and proof of use of our proposed design theory. Proof of value involves “taking the revised prototype … to the field and measuring whether the users are more productive [and retrieve greater value] with the system than without it” (Nunamaker et al., 2011, p. 26). This involves both (1) the direct evaluation of the DPs through relevant practitioners external to Dataswyft and (2) their indirect evaluation through user evaluation of the Dataswyft platform as an instantiation of the DPs (Iivari, 2015).

5.2.1. Direct Practitioner Evaluation of DPs. To evaluate the effectiveness of our DPs, we conducted a minimum reusability evaluation following Iivari et al.’s (2021) procedures. We interviewed 14 practitioners ($M_{\text{age}} = 41.9$ years, $M_{\text{industry experience}} = 14.7$ years, 14% female) from the US, the UK, and Germany who would use our DPs to develop, implement, or operate such a digital platform. Key informants included software engineers, cybersecurity consultants, chief technology officers, data privacy lawyers, web interface developers, and product managers. The interviews consisted of three parts: 1) clarifying the interviewees’ role and experience; 2) presenting our DPs with explanations, and 3) evaluating the DPs in terms of their accessibility, importance, novelty, actability, and effectiveness (Iivari et al., 2021). Interviews lasted between 32 and 66 minutes (average: 52.4 minutes), and all but two were audio-recorded, transcribed verbatim, and analyzed primarily involving pattern-matching of evidence with evaluation outcomes (Yin, 2009). Next, we summarize the insights gained (see Table 6 for more detailed evaluations and illustrative quotes).

Collectively, practitioners highly value the set of DPs for their importance, novelty, and effectiveness. If implemented effectively, they judge the DPs to offer a novel, much-needed technical solution to rebalance data control and resolve privacy concerns that would improve end-users’ empowerment and benefit society. One practitioner noted: “[I]t would change so much, I mean, advertising would have to be rethought… And if some of that power was brought back to [the end-user] … that would be way better for the Internet as a whole … people aren’t seen as dollar value [instead] you need to offer value to these people, rather than just looking to like mindlessly scrape money from them” (I9). Accessibility was rated as medium, with practitioners finding the DPs straightforward, although noting abstract language. They also rated actability as medium, stressing implementation challenges, as one practitioner noted: “So, … they’ll all have… the challenges, but I think it, you know, like I said, I think it’s a good start to be able to break down, what are the different components that need to be taken into consideration” (I3).

Individually, practitioners provided a fine-grained evaluation of each DP, stressing their high importance (e.g., DP1, DP4, DP5, DP7, DP8), novelty (e.g., DP2, DP3, DP4), and effectiveness (e.g., DP2, DP4, DP5). However, concerns were raised about the accessibility of some DPs due to abstract language and broad descriptions (e.g., DP1, DP2, DP8). In terms of actability, practitioners repeatedly raised concerns over DP4, emphasizing the need to ensure “responsible” end-user data exchange decisions to prevent exploitation, as one practitioner noted: “absolutely [there could be user error because if you go one too far now that client has access to [all their data]. So, there’s no guardrails regarding the sharing permissions and accessibility at that level” (I2). Similarly, concerns were expressed about the actability of DP5, noting that it may require a lot of “hand holding… to make this interface user friendly, as much as possible, and user driven” (I3) while stressing the difficulty in articulating the benefits for both end-users and firms to participate in such a platform for DP8. As one practitioner noted: “[W]hy would the larger companies necessarily adopt something like this? … [and] how will you sell it to the average person?” (I10). In response to these issues, we revised the descriptions of all DPs.

Danatzis et al. (2024): Designing Digital Platforms for Social Justice – Author Accepted Manuscript 21
## Table 6. Minimum Reusability Evaluation of Design Principles

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Exemplary Quotes</th>
<th>Summary Evaluation</th>
</tr>
</thead>
</table>
| **Accessibility** | “I think it's fairly straightforward to understand... overall, I mean, for me, personally, this, this makes, this makes sense, especially as you kind of built up, you know, again, from the first design principle to the to the last one.” (I3)  
“And then, you know, comparing, you have these two platform layers, I guess, for someone to understand how data is, is owned and stored now helps to understand what you're trying to portray, here.” (I3)  
“I think from like, for me, it's clear because I've done a few of these steps already in another kind of like space.” (I9)  
“I understand it perfectly. And it makes total sense to me.” (I10)                                                                 | Medium: Practitioners find the DPs to be understandable, with some noting that the DPs build upon each other in a logical manner.  
Additionally, they highlight how understanding DP1 and DP2, in particular, helps to understand the overall concept of the platform.  
However, some practitioners mention that their previous experience with similar principles makes it easier for them to understand the DPs. |
| **Importance**   | “I think some people have tried not exactly the same idea, but they have tried, like similar they have done like, actual like payment for data for user data ... This is a on a bigger scale, obviously. And so, I think is a great idea.” (I1)  
“But I definitely see the advantages, or, you know, what, what, what the point is, for each, for each of each one of these, I wouldn't say they're all equally as important. But it really depends, if you're talking to, you know, someone on the legal side of things versus someone on the technical side of things, or you're talking to someone who's an end-user.” (I3) | High: Practitioners stress the importance of the set of DPs, emphasizing their collective importance as building blocks of an alternative digital platform design centered on social justice and the benefits of having a personal hub for end-users to own, manage, and exchange their data. |
| **Novelty**      | “I've never really, like spent a lot of time exploring that, or having someone you know, like, you explain what the breakdown with the so this is probably the most in depth I've gone as far as you know, moving over from how data is handled to a potential solution to, you know, privacy and data ownership.” (I3)  
“This is ...much more in depth proposition than I've ever encountered before. ... I’ve read about privacy by design, hard privacy versus soft privacy approaches ... with this is much more developed.” (I8)  
“I just haven’t heard those discussions. And I guess they come to us for compliance with the existing regulations and problems when they haven't complied with those regulations. But these discussions out there that are, you know, a lot more innovative.” (I3)  
“It definitely novel, I only like really put my head in when I was ... looking at some an angle of this for email, calendar and files. And but yeah, I think so that's, it's incredibly novel.” (I9)  
“I'm still convinced that data protection laws is not necessarily addressing the issue ... I think if we want to be successful, and I'm talking about the burden, but it's the responsibility, I think it's the user who should be responsible. It's not like Facebook, or Airbnb, or TikTok, which is responsible for my data. And which has to take like security measures, do not do this, or that, blah, blah, blah. But it's more like user centric. So, I like that the perspective is the perspective of the end-user.” (I11) | High: Practitioners regard the DPs as highly novel and comprehensive, providing a more developed and in-depth analysis on how an alternative end-user-centric digital platform design could look like that is centered on social justice, surpassing previous ideas and concepts that may have only touched on one or a few of those aspects. |
| **Actability**   | “So, a few of these will definitely. I mean, they'll all have, you know, the challenges, but but I think it, you know, like I said, I think it's a good start to be able to break | Medium: Practitioners generally express support for actability of the DPs, however, they also |
“And, and I think that the new generation, it's a little bit different. Now. They, they were born in a way where data are used every day, they notice social networks, it's, it's a second life for them. And I think that's why also, maybe time has come for this user centric perspective. You know, I think maybe it was too much to ask of people of the old generations, and I belong to that old generation, you know, where, in a way we needed protection, because we didn't really play the game with the same cards, as the platforms, or the engineers behind them, and so on, you know, and now I feel like users understand more and more what's happening. And I think that's why also, it's, it's a shift and a perspective, which also really corresponds to the time in which we are.” (I11)

Effectiveness

“...But they certainly don't trust big tech companies for that reason. So...Yeah, I think helping end-users gain a level of control and like agency is really important.” (I8)

“Like, I don't know how much malicious activity is going on. So, I don't know how much of the information is being taken and being sold or being used in ways that it shouldn't. And I would like to protect more against that. So, if you can, if I could say, right, this is where I'm using my data, it's anonymous is protected. And these companies only get access to my identity and what use I have when I say in an easy to use way that will be much much better for the Internet overall.’” (I9)

“[I]’s a solution that I think we’re going to need sooner than we think just as like data breaches, companies are getting more aggressive. AI search is now becoming the norm, almost, it's going to be like, our information is going to be sucked more and more for usage by massive companies and having that imbalance, as you say, and I think having an example of that would maybe be really useful to show that imbalance and show...how this would help reset that imbalance. That'd be really cool to see.” (I9)

“I think [such end-user-centric platform design] it’s exactly the direction in which we want, we want and we, we should go... [because] I think the main problem is that people don't understand what is happening with that data online. You know, and in the digital world. For instance, I'm always I'm always shocked when I see people like sharing pictures of their babies and so on, you know, I mean, I feel like it's very intimate, but it's, it's my personal opinion, but as a as a lawyer, and as a user of the social networks, I feel like what you put there is going to remain for the, the eternity ... I don't, I don't think that people really understand what can happen with the data. And what is already also happening with the data.” (I11)

5.2.2. Indirect User Evaluation of DPs. To gauge additional proof of value of our DPs, we conducted several rounds of indirect user evaluation of the Dataswyft platform. To provide a holistic picture of the platform’s benefits over time, in the following we will report proof of value both for early adopters of the beta version of the Dataswyft platform in 2017 and for its current users in 2023.
To gauge initial proof of value for early adopters of the platform’s beta version in 2017, transcripts of twelve interviews with active users and nine in-depth interviews with initial beta-version users were analyzed. The findings are summarized in Table 5. Overall, almost all beta users emphasized that using the Dataswyft platform gives them greater perceived control in two respects: First, it gives users “greater appreciation of the type of data that is collected, which may in turn help to inform them how to limit/control what services [the users] agree to use on the Internet” (BT 3). Second, users perceived that visualizing, contextualizing, and exchanging personal data through the platform, puts them in “a powerful position … [as their] HAT allows [them] to … have something about [their] data that companies don’t have and that makes [them] feel [they] have control” (BT 2). Furthermore, most of the beta users “don’t see … concerns to privacy” (BT 3) and “feel very comfortable putting private data on [their] HAT … [as they overall] feel it is secure” (BT 2). Notably, early adopters were often tied to the HAT/Dataswyft organization through organizational partnerships or university affiliations and were more familiar with personal data issues than a typical end-user. Nevertheless, their insights helped refine the platform’s functionalities during the second-to-third heuristic search iteration.

To gauge further proof of value, 13 senior executive part-time students (M<sub>age</sub> = 42.6 years, M<sub>d</sub> = 16 years, 38% female) from the US participated in user testing and observation of the Dataswyft platform and website. These students were selected as they work in industries where Dataswyft could operate such as IT, financial services, healthcare, and insurance. The user testing consisted of participants using the Dataswyft platform or website over several days and included an online survey with open-ended questions about the platform’s (potential) benefits in terms of privacy, empowerment, data ownership, control, and data commercialization, as well as four subsequent focus group discussions for more in-depth insights (all recorded and transcribed verbatim). Survey data were analyzed inductively using Gioia et al.’s (2012) first- and second-order thematic analysis. Findings are summarized next (see Table 7 for more details and quotes).

Overall, most respondents report a greater sense of control and agency that the Dataswyft platform would provide, mainly due to legal data ownership and the ability to exchange their data for (non)monetary benefit, as one user noted: “The key benefit is that I can do what I wish to with it [my data]. If I choose to commercialize it, great. If I choose to destroy it and leave no virtual trace, that’s also great. The agency and liberty that comes with ownership matters to me” (E11), and another user stresses how they “[c]an make choices for [themselves] and what happens to the data. Can package it and sell it, can curate it” (E3). Most end-users further report an improved sense of privacy, as Dataswyft “provide[s] privacy and empower[s] you to decide how you want to interact with the world, rather than the world deciding how it interacts with you” (E8). Many respondents also stress increased “protection from misuse, abuse, and corruption” (E7), and a greater awareness of data privacy issues as Dataswyft is “forcing them to learn about and grapple with key data privacy considerations that they can too easily ignore under the current system” (E4). Other respondents stress potential direct financial gains from commercializing their data, while others stress indirect benefits, such as more personalized marketing, “increase[d] trust and confidence and ways for utilization” (E10), leading to more empowered marketplace interactions. However, some also voice concerns over an increased perceived burden of user responsibility as they “feel that [end-users] have to learn more about each and every organization’s motives and use of [their] data… [and are] not sure [whether end-users] have the bandwidth to care” (E8).

Additionally, we gathered insights from end-user who interacted with an application built on the Dataswyft platform but not through the platform’s direct interface. Specifically, we analyzed the health application SejutaKG which launched a nationwide weight loss campaign in Malaysia in June 2022 that allows its users to track and exchange their verified weight loss data for benefits (e.g., vouchers, prizes, insurance, banking offers). Specifically, we interviewed two SejutaKG end-users (both male, average age = 38.5 years) who recently won a trip to Turkey for weight loss achieved through the application over several months. The interviews were conducted in Malay, audio-recorded, transcribed, and translated into English for analysis, and were complemented by the analysis of three questionnaires and chat conversations of four SejutaKG end-users. Additionally, we conducted two interviews with the CEO and founder of SejutaKG (average time: 52 minutes) to gather further insights into the potential benefits of using the Dataswyft platform both for application end-users and the application provider. Overall, app users placed less attention on privacy considerations, emphasizing instead the direct benefits of exchanging their weight loss data for prizes (EA1: “I wanted to prove to myself that I could do it and win a trip to Turkey”), a greater sense of control offered by the SejutaKG app through monitoring and convenience (EA2: “Tracking your weight regularly makes you feel more in control of your health”), and improved physical and emotional well-being through lifestyle changes (SA1: “It’s [g]reat. [I] sleep better. [I have] more stamina in cycling. Reduced snoring”).

The application provider, in turn, reported three main benefits for using Dataswyft: First, it empowers app providers to resolve siloed health data, thus enabling end-user data exchange and proactive data privacy. This benefits end-users, even if they did not prioritize or request it: “To be honest, this kind of set everybody else through
their privacy to the wind, in exchange for the prizes … that’s the thing. We’re doing it behind [their] backs…How to say it’s a benefit that they’re not asking us for, which [we are] doing [regardless]” (SF1). Second, using Dataswyft allows the app provider to ensure regulatory compliance with privacy legislation and to balance both profit and mission-driven values: “[I]f I were to call myself … a nonprofit, which is mission purpose driven, then we should double down on that, go all the way. … And if there is money to be made, it’s done in a responsible way, as enriching as possible to the [app] user” (SF1). Finally, from an partner perspective, using Dataswyft is seen to facilitate the emergence of an ecosystem around the application by improving access to end-user data, increasing the value of end-user data, and reducing customer acquisition costs for merchants: “A lot of merchants that we deal with do not have the resources or the capability to … build these kinds of databases… they … prefer to rely on us… [so] then they can go ahead to provide semi customized services” (SF1). In total, these user evaluations attest the numerous benefits of the Dataswyft platform for end-users, application users, and application providers, thus attesting sufficient proof of value of our DPs.

5.2.3 Initial Proof of Use Evaluation. The final evaluation phase “involves broad fielding and continued use by many users” (Nunamaker et al., 2011, p. 26). As of February 2023, the Dataswyft platform had over 11,000 active end-users, with various application providers across different industries offering services on the platform for users in the UK, US, Canada, and Malaysia. As of February 2023, 14 applications ran on the platform, with numerous others in development, providing personalized loans, insurance discounts, health scores for COVID-19 tracing, and identity and fraud verification. Overall, the Dataswyft platform has sufficiently reached the proof-of-value and initial proof-of-use stages, with real-life evidence demonstrating its value to practitioners, end-users, and application providers. With the ongoing development and the launch of new applications, we expect deeper value realization for all platform participants in the future.

<table>
<thead>
<tr>
<th>Table 7. User Evaluations with Illustrative Quotes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>End-User Benefits: Illustrative Quotes</strong></td>
</tr>
<tr>
<td>“The main benefit of commercializing one’s personal data is financial: individuals can make money from the use of their private personal data…” (E4)</td>
</tr>
<tr>
<td>“… the opportunity to monetize the information for personal gain. This allows the risk and the reward to be aligned at the individual level.” (E7)</td>
</tr>
<tr>
<td>“The owner can benefit from the advertisement and other opportunities available from the organization interested in the data.” (E6)</td>
</tr>
<tr>
<td>“You may be more respected by companies if they have to actually ask you and exchange something of value. Also, companies may have to make better efforts to show you that they are trustworthy.” (E8)</td>
</tr>
<tr>
<td>“It provide[s] protection and privacy of the personal data.” (E6)</td>
</tr>
<tr>
<td>“It would provide privacy and empower you to decide how you want to interact with the world, rather than the world deciding how it interacts with you.” (E8)</td>
</tr>
<tr>
<td>“Control over the quality of the information and protection from misuse, abuse, and corruption.” (E7)</td>
</tr>
<tr>
<td>“…impacts an end-user by forcing them to learn about and grapple with key data privacy considerations that they can too easily ignore.” (E4)</td>
</tr>
<tr>
<td>“Can keep a very clean profile of what to expect from the organization, and more comfortable with what is ultimately shared.” (E12)</td>
</tr>
<tr>
<td>“I can do what I want with it. That’s a value in and of itself.” (E11)</td>
</tr>
<tr>
<td>“The key benefit is that I can do what I wish to with it. If I choose to commercialize it great. If I choose to destroy it and leave no virtual trace, that's also great. The agency and liberty that comes with ownership matters to me.” (E11)</td>
</tr>
<tr>
<td>“That someone trust me enough to know that I own my own data without dictating to me what to do with it.” (E5)</td>
</tr>
</tbody>
</table>

Danatzis et al. (2024): Designing Digital Platforms for Social Justice – Author Accepted Manuscript 25
"The user will feel more in control of the relationship and what happens." (E12)  
Enhanced transparency and trust

"End-user empowerment [through the Dataswyft platform] creates more stress around what data might be shared. I feel that I have to learn more about each and every organization's motives and use of my data ... I ideally would control my data, but I am not sure I have the bandwidth to care." (E8)  
Increased stress and bandwidth concerns  Perceived burden of responsibility

**Application User Benefits:** Illustrative Quotes

<table>
<thead>
<tr>
<th>1st Order Concept</th>
<th>2nd Order Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Additionally, I wanted to prove to myself that I could do it [lose weight by using the SejutaKG app] and win a trip to Turkey.&quot; (EA1)</td>
<td>Increased motivation through incentives  Direct exchange benefit</td>
</tr>
<tr>
<td>&quot;It’s easy to lose control and forget to monitor food intake. By keeping an eye on [the SejutaKG app], we can track progress and stay motivated.&quot; (EA1)</td>
<td>Greater self-control through monitoring  Greater control through enhanced agency perceptions</td>
</tr>
<tr>
<td>&quot;I like that it's [the SejutaKG app] a convenient way to get a healthy breakfast. It's great for people who want to lose weight and live a healthier lifestyle.&quot; (EA2)</td>
<td>Greater self-control through convenience</td>
</tr>
<tr>
<td>&quot;With its system, it [the SejutaKG app] reduces the work required and helps me to eat healthier, more liquid-based meals.&quot; (EA2)</td>
<td>Improved physical and emotional well-being  Improved well-being through healthy lifestyle changes</td>
</tr>
<tr>
<td>&quot;I feel happy and healthy. After using SejutaKG frequently, you know the price before and after using it.&quot; (EA2)</td>
<td>Healthy habit building</td>
</tr>
<tr>
<td>&quot;Yes, I have followed SejutaKG’s dietary guidelines and have successfully reduced my weight.&quot; (EA1)</td>
<td></td>
</tr>
</tbody>
</table>

**Application Provider Benefits: Illustrative Quotes**

<table>
<thead>
<tr>
<th>1st Order Concept</th>
<th>2nd Order Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;... the asymmetry of information or the silo ... causing in what you call it, market failure. Right.... I think health is probably the biggest market failure of our time ... that's precisely why there's just so many people making profit from health care that we have sub optimal health outcomes.&quot; (SF1)</td>
<td>Reduce information asymmetries in the health industry  End-user benefit: Empower end-users</td>
</tr>
<tr>
<td>&quot;[T]here are … cancer campaigns to increase awareness..., those are the ones very keenly observing our progress, because they are also dealing with exactly the same situation, we are having the health data being siloed and unable to be integrated at the user level.&quot; (SF1)</td>
<td>Resolve siloed end-user health data to benefit end-user health</td>
</tr>
<tr>
<td>&quot;So, from the [app] user perspective, it has to be as simple…Here's my data. Where's my offer? That's, that's, that's one thing that we find works here.&quot; (SF1)</td>
<td>Enable end-user data exchange  End-user benefit: Enable end-user control and privacy</td>
</tr>
<tr>
<td>&quot;I think I can count on one hand, no more than two people who have said no, due to privacy issues ... That's, that's the thing. We're doing it [privacy] behind. Not behind users' backs but doing it out of sight of them are doing it. How to say it's a benefit that they're not asking us for which is doing it.&quot; (SF1)</td>
<td>Provide data privacy to end-users proactively</td>
</tr>
<tr>
<td>&quot;But if I were to call myself ... a non-profit, which is mission purpose driven, then we should double down on that, go all the way. And say even the data which everyone is thinking we are going to profit from is done in a decentralized way. And if there is money to be made, it's done in a responsible way.&quot; (SF1)</td>
<td>Balancing profit and mission-driven firm values  Application provider benefit: Ensure ethical monetization</td>
</tr>
<tr>
<td>&quot;And now you have to layer on top the challenge, which is to do it with GDPR.&quot; (SF1)</td>
<td>Ensure privacy compliance  Application provider benefit: Ensure regulatory compliance</td>
</tr>
</tbody>
</table>
Danatzis et al. (2024): Designing Digital Platforms for Social Justice – Author Accepted Manuscript

6. Discussion
6.1. Theoretical Contributions

This research contributes to the digital platform literature by delineating how digital platforms can be designed for social justice, particularly by empowering end-users to address social injustices related to 1) data control and 2) privacy. Grounded in a DSR approach that uses heuristic theorizing to systematically derive a design theory for end-user-centric digital platforms, our theory’s core comprises five MRs and eight DPs, thus extending extant literature on end-user centricity in platform or system design (De Hert et al., 2018; Iivari & Iivari, 2011; Yoo et al., 2010; Zhu et al., 2021). Notably, two of the DPs, DP1 and DP2, are of particular importance. DP1 proposes adopting a container-based, microservice platform architecture, while DP2 prioritizes legal end-user ownership of databases. These two DPs deal with the design of the underlying platform infrastructure, establishing the foundation of our design theory. Together, they outline how the adoption of such a platform architecture allows for the decentralized access, storage, and processing of end-user data, effectively conferring legal data ownership to end-users through the provision of full custodial rights over their data. Conferring such ownership rights to end-users, in turn, lays the technical and legal basis for meaningful end-user control and privacy, described by surveillance scholars “as a necessary first step towards addressing [today’s]…asymmetrical data accumulation and … unjust data practices” (Cinnamon, 2017, p. 622; see also Zuboff, 2015).

All other DPs serve to flesh out this potential of the platform architecture in addressing social injustices. Specifically, DP3-DP5 outline the design of core functionalities and interfaces that enable end-users to import, reconfigure (DP3), and responsibly exchange their data (DP4) using end-user-centric tools (DP5), while DP6-DP8 outline key ecosystem design decisions, including the establishment of multiple layers of data protection (DP6), semi-centralized governance mechanisms (DP7), and continuous communication with platform parties (DP8). Collectively, these DPs and the resulting design theory have profound social justice implications:

On the one hand, our design theory addresses economic injustices of maldistribution by empowering end-users to decide what data they share, with whom, and for what (non-)economic benefit, thus advancing research on end-user control (Gal-Or et al., 2018; Tsai et al., 2011) and personal data commercialization (Acquisti et al., 2016; Spiekermann & Korunovska, 2017). Whereas extant PDMS solutions (Anciaux et al., 2019) often act as data vaults where end-users can “lock-up” their data, our design theory outlines how end-users can not only control their data, but also use their data as a tradable asset. Besides allowing end-users to exchange their data for monetary benefit, our theory offers underserved, often marginalized, end-users an alternative route to exchange aggregate data insights for access to otherwise unreachable products, such as microloans, as exemplified by Dataswyft’s OneZero-Me app, thereby furthering financial inclusion. Importantly, our DPs also entail safeguarding mechanisms and ecosystem governance structures to counter end-user exploitation (Chen et al., 2021), addressing many of the security and privacy risks inherent in prior personal data exchange platforms (Anciaux et al., 2019).

On the other hand, our design theory offers platform firms an alternative way to protecting end-user privacy and mitigating procedural social injustices related to misrecognition and misrepresentation. Rather than relying on (self-)regulation and privacy-enhancing technologies alone, privacy preservation is at the heart of our design theory
via the adoption of a containerized microservice platform architecture. This design choice ensures that end-user data are stored and processed in isolation from other platform users and third parties, thus advancing recent IS research on information privacy on digital platforms (Al-Natour et al., 2020; Bélanger & James, 2020; Cusumano et al., 2019; Gal-Or et al., 2018). Combined with platform functionalities that allow end-users to decide what data to collect, process, and disclose, our design theory reduces the risk of end-user misrecognition. Reducing the risk of misrepresentation, in turn, our design theory enables end-users to collect, contextualize, and analyze their data to gain more meaningful insights into their behavior and journey when using platform services. These previously inaccessible insights can give end-users more control and promote personal growth and self-improvement, as demonstrated by Dataswyft’s SejutaKG app, which empowers app users to develop healthier habits and lifestyle changes. Furthermore, by enabling end-users to choose which insights to share with other platform parties, end-users could influence their profiling, targeting, or matching with other platform users or content. As such, our design theory may foster a more accurate representation of end-user needs, while offering an alternative avenue for end-users to correct potential algorithmic misclassifications (Cinnamon, 2017; Puntoni et al., 2021).

Overall, our design theory offers a novel approach to how digital platforms can be designed for social justice, addressing both key distributive and procedural injustices that might sometimes hinder end-users from participating equitably in the digital economy. Importantly, platforms are not inherently malevolent, and these injustices are neither innate nor permanent features of any platform. Rather, platform owners regularly make design choices as part of their value creation goals and these choices may have unforeseen or unintended consequences—both positive and negative—for end-users. As such, our design theory offers digital platforms with a blueprint for centering their design efforts proactively on advancing social justice. Besides advancing research on resolving inequities in the digital space (Hsieh et al., 2008; Jacobides et al., 2024; Ransbotham et al., 2016), our design theory addresses all critical points necessary to facilitate end-user data self-sovereignty: meaningful control, privacy, and legal data ownership (Hummel et al., 2021).

More broadly, our design theory contributes to the emerging social sustainability discourse in IS research, a crucial but often underemphasized sustainability dimension as compared to its economic and environmental dimensions (e.g., Mckenzie 2004; Seidel et al. 2017). We respond to calls to advance the limited research on how key IS artifacts, such as digital platforms, can be redesigned to leverage social sustainability (Schoormann & Kutzner, 2021). Our design theory offers eight fundamental DPs that can be applied to foster economic fairness, equitable data access, and inclusive participation for end-users. Complementing recent work outlining DPs for environmental sustainability (Seidel et al., 2018), our DPs span various social sustainability facets, primarily providing prescriptive knowledge for designing digital platforms that advance social justice, while also enhancing social equity and inclusion (Schoormann & Kutzner, 2021).

In sum, following Gregor and Hevner’s (2013) DSR knowledge contribution framework, our design theory can be classified as an invention because it represents a “clear departure from the accepted ways of thinking and doing” (ibid., p. 345) about how and by whom end-user data is managed, controlled, and exchanged on digital platforms. In essence, this invention offers a wicked solution to data control and privacy, and associated social injustices of maldistribution, misrecognition, and misrepresentation by centering platform design on end-user empowerment, shifting the focus of design efforts from the capabilities and goals of firms to those of end-users. As the collection of end-user data proliferates in society, there is an urgent need for a design theory that offers the prescriptive knowledge necessary to guide platform owners to think through platform design choices that foster social justice. This paper delivers on this need.

### 6.2. Managerial Implications

By demonstrating the applicability of our design theory through a real system implementation, we provide clear guidance to practitioners on how to translate our abstract DPs into a real-life end-user-centric digital platform that could advance social justice in practice. Our principles of implementation therefore offer actionable guidance for the implementation of each DP, providing a blueprint for the design of such digital platforms. The evaluation of the Dataswyft platform as an expository instantiation of these principles further increases our theory’s applicability by grounding our DPs and principles of implementation in the authentic environment of relevant platform stakeholders. Additionally, the direct evaluation of our DPs by practitioners external to Dataswyft further demonstrates their practical reusability. This evaluation ensures that our DPs are accessible, important, novel,actable, and effective in resolving real-life tensions that practitioners may experience when employing such prescriptive knowledge in practice. That said, building digital platforms that rely upon our design theory also poses various challenges.

First, our findings suggest that platform providers must pay attention to all four layers of platform design, including infrastructure that enables the platform to cross sectors, core functionalities for effective data collection, processing, and sharing, interfaces for meaningful user experiences, and ecosystems for structured interactions.
among platform parties. Importantly, all four layers must align to ensure seamless data flows. Their design requires the involvement of various platform stakeholders, including back-end software engineers, solution and security architects, and privacy lawyers at the infrastructure level, software developers, data scientists, and user experience (UX) designers at the platform core level, API developers and user interface designers at the interface level, and partnership, product, and marketing managers at the ecosystem level.

Second, by evaluating the proof of concept, proof of value, and initial proof of use of the Dataswyft platform, this study showcases the utility of our design theory in practice. However, practitioners involved in platform design must be mindful that the real-life impact of our DPs may vary among platform stakeholders. For example, our findings show how platform end-users benefit from a greater sense of control and privacy over their data, as well as financial gains and personalized marketing. App users, in turn, mostly value data control benefits that materialize through direct exchange rewards, convenience, and improved well-being through lifestyle changes, while app providers benefit by balancing profit and mission goals through improved data exchange, regulatory compliance, and increased access to end-user data. The design of such a wicked solution therefore requires continuous oversight to ensure that the desired outcomes are delivered satisfactorily to all platform parties (Ng, 2014) and that their behaviors are aligned to avoid generating new, unintended platform or ecosystem failures (Jacobides et al., 2024).

Finally, our findings suggest that the successful rollout of such a digital platform requires separating supply-side data-producing firms from demand-side data-usage firms, and a focus on user engagement and adoption. To accelerate adoption and scalability, platform owners should assess industry pain points, such as privacy, compliance, or data sharing issues. This assessment includes evaluating the benefits and tradeoffs of design choices and the regular updating of guardrails—whether through added data protection layers or platform functionalities—to ensure robust end-user control and privacy, especially as additional unforeseen wicked subproblems may arise.

6.3. Limitations and Future Research

This research provides proof of concept, proof of value, and initial proof of use of the proposed design theory. However, DSR is iterative and future researchers should test our TPs and explore alternative solutions to data control and privacy to integrate, challenge, or reconcile them with DPs discovered in this study. While this study offers evidence that the proposed DPs function and provide value to platform end-users, app users, and app providers, the ongoing development of the Dataswyft platform and the wicked problems it addresses require further evaluative research to substantiate the theory’s proof of value and use. As our design theory aims to transform how personal data is handled, scaling up may also pose several challenges, particularly in addressing end-users’ privacy concerns to gain trust and ensure long-term viability (Cusumano et al., 2019). Additionally, fostering the proactive role and readiness of end-users in collecting, transforming, and exchanging personal data needs further exploration (Danatzis et al., 2022). Overall, our study provides a solid foundation from which others can build to design platforms for social justice, yet our DSR approach highly encourages continued exploration and refinement.

6.4. Concluding Remarks for DSR Scholars

This longitudinal study used a DSR approach to develop a design theory for digital platforms that advance social justice, based on over nine years of data. The study’s key lesson for DSR scholars is that wicked problems equally require wicked solutions. By outlining the need of several years of iteration and modification of the theory’s MRs and DPs to tackle the wicked problems of data control and privacy, our study stresses the importance of continuously bouncing back preliminary solution candidates with relevant stakeholders. This iterative process enables the identification of emerging wicked subproblems that need to be addressed to develop a viable design solution.

Crucially, without the iterative extraction and articulation of MRs, a wicked solution is unlikely to emerge. Although often neglected in DSR studies, MRs are foundational for generating and refining DPs. They guide designers in creating initial working design components, set evaluation standards for their utility, and direct subsequent heuristic search efforts for new or updated DPs that might satisfy these MRs. At a minimum, we therefore recommend that DSR scholars 1) explicate their MRs, 2) outline how they evolve over multiple heuristic theorizing iterations vis-à-vis the emergence of new wicked subproblems, 3) map each MR to the identified subproblems they address, 4) detail how each DP aligns with specific MRs, and 5) demonstrate the utility of their resulting design theory against each derived MR. Such “minimum meta-requirements articulation procedures” (minMAP) would complement the minimum reusability evaluation procedures of DPs recently proposed by Iivari et al. (2021). If implemented effectively, these minMAP could serve as a valuable guide for authors, reviewers, and editors of DSR papers, thereby increasing the applicability, rigor, and relevance of DSR contributions.
Acknowledgements

The authors thank the anonymous reviewers, the Associate Editor, and the Special Issue Editorial Team for their invaluable feedback and guidance. We are also grateful to the management of Dataswyft for providing data access and continued support. Further, we would like to thank the CEO of SejutaKG for providing access to their app users. Finally, C. Wernicke’s and D. Reynold’s contributions to data collection, data analysis, and feedback before 2017 are acknowledged.

Note: The transparency material for this paper is available at https://doi.org/10.17605/OSF.IO/Y7BNF, licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License
References


Docker Website. (June 23, 2023). Use containers to build, share and run your applications. https://www.docker.com/resources/what-container


European Commission. (2016). Legal study on ownership and access to data. https://doi.org/10.2759/299944


https://doi.org/10.1287/isre.1120.0416


Author Biographies

Ilias Danatzis is an associate professor (senior lecturer) of marketing analytics at King’s College London, UK. His research interests revolve around services and digital marketing, with an emphasis on (dys-)functional service encounters, digital platforms, organizational frontlines, innovation, and service ecosystems. His award-winning research has been published in leading academic outlets such as the Journal of Service Research (Best Service Article Award 2023), Journal of Business Research, and Industrial Marketing Management.

Jennifer D. Chandler is professor of management at California State University, Fullerton. Dr. Chandler is an international scholar on ecosystems, platforms and data, institutional theory, service, and technology management. Dr. Chandler holds a BA (UCLA), MBA (University of Hawaii Manoa), and PhD (UC Irvine). Her award-winning research is published in Journal of Service Research (Best Paper Award 2015), Journal of Service Theory and Practice (Best Paper Award 2015), Journal of Service Management, Journal of Business Research, Journal of Business Ethics, Creativity and Innovation Management and Decision Sciences Journal of Innovative Education to name a few.

Melissa A. Akaka is professor of marketing and associate dean for research at the Daniels College of Business at the University of Denver. She is director of the Master of Science in marketing program and a co-director of the Consumer Insights and Business Innovation Center. Dr Akaka’s research investigates how consumption experiences, journeys, and collectives create value for both firms and consumers and explores the social drivers and consequences of innovation. Her scholarly work has been published in a variety of academic journals, including the Journal of Consumer Research, the Journal of the Academy of Marketing Science, and the Journal of Service Research. Her work has been recognized for being “highly cited” (in the top 1%) by Thompson and Reuters.

Irene C. L. Ng is the CEO of Dataswyft Ltd and professor at WMG, University of Warwick. Her specialism is in value-based contracts, market design and the economic engineering of digital markets and ecosystems. She has published in numerous international journals across multiple disciplines and is the author of The Pricing & Revenue Management of Services: A Strategic Approach, lead editor of the book Complex Engineering Service Systems: Concepts and Research and Creating New Markets in the Digital Economy: Value and Worth published by Cambridge University Press.