It is not (only) about privacy

How multi-party computation redefines control, trust, and risk in data sharing

Agahari, W.; Ofe, H.A.; de Reuver, G.A.

DOI
10.1007/s12525-022-00572-w

Publication date
2022

Document Version
Final published version

Published in
Electronic Markets

Electronic Markets
https://doi.org/10.1007/s12525-022-00572-w

RESEARCH PAPER

It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing

Wirawan Agahari[1] · **Hosea Ofe**[1] · **Mark de Reuver**[1]

Received: 18 February 2022 / Accepted: 11 July 2022

Abstract
Firms are often reluctant to share data because of mistrust, concerns over control, and other risks. Multi-party computation (MPC) is a new technique to compute meaningful insights without having to transfer data. This paper investigates if MPC affects known antecedents for data sharing decisions: control, trust, and risks. Through 23 qualitative interviews in the automotive industry, we find that MPC (1) enables new ways of technology-based control, (2) reduces the need for inter-organizational trust, and (3) prevents losing competitive advantage due to data leakage. However, MPC also creates the need to trust technology and introduces new risks of data misuse. These impacts arise if firms perceive benefits from sharing data, have high organizational readiness, and perceive data as non-sensitive. Our findings show that known antecedents of data sharing should be specified differently with MPC in place. Furthermore, we suggest reframing MPC as a data collaboration technology beyond enhancing privacy.

Keywords Privacy-enhancing technology · Multi-party computation · Data sharing · Control · Trust · Risk

JEL Classification L86

Introduction

Multi-Party Computation (MPC) is a key enabler for safe and secure data sharing (Balson & Dixon, 2020), which is important as data is estimated to create an economic value of more than 800 billion Euros in 2025 (European Commission, 2020). MPC is based on a cryptographic technique where multiple parties perform a joint computation without revealing the input provided by each party (Bestavros et al., 2017; Choi & Butler, 2019; Zhao et al., 2019). While the theoretical concept of MPC is not novel (Yao, 1982), recent advances in computational power and efficiency are bringing MPC increasingly close to large-scale and real-life applications. MPC is a rapidly emerging technology (Gartner, 2021), which is very timely given the growing tension between sharing and protecting data in the digital society (cf. Gast et al., 2019). On the one hand, data sharing between businesses could enable value creation by allowing firms to combine multiple data sources to discover new insights (Koutroumpis et al., 2020; Spiekermann, 2019; Virkar et al., 2019). On the other hand, concerns are mounting over, among others, the fear of losing data control (Zrenner et al., 2019), privacy risks (Eurich et al., 2010), and trust in big technology companies (Dahlberg & Nokkala, 2019), resulting in firms' reluctance to share data (Jernigan et al., 2016; Richter & Slowinski, 2019).

At the backdrop of these challenges, Information Systems (IS) scholars researching inter-organizational information sharing have emphasized control (Klein & Verhulst, 2017; Priego et al., 2019), risk (Johnson, 2009; White et al., 2007), and trust (Arnaut et al., 2018; Kembro et al., 2017) as key antecedents of data sharing by firms. However, since MPC is a fundamentally different way of sharing data, the relevance of these antecedents can be questioned (cf. Alvesson

Responsible Editor: Katharina Ebner

✉ Wirawan Agahari
w.agahari@tudelft.nl

Hosea Ofe
h.a.ofe@tudelft.nl

Mark de Reuver
g.a.dereuver@tudelft.nl

[1] Faculty of Technology, Policy, and Management, Delft University of Technology, Jaffalaan 5, 2628 BX Delft, the Netherlands

Published online: 30 July 2022

& Sandberg, 2011). On the one hand, MPC enables computational analysis without revealing input data (Bestavros et al., 2017; Choi & Butler, 2019; Zhao et al., 2019), eliminating the need for a trusted third party as an intermediary that facilitates data sharing (Bruun et al., 2020; Helminger & Rechberger, 2022). Hence, firms should be able to retain data control and possibly reduce the risk of data sharing in the process. On the other hand, MPC is not yet widely applied due to limitations of computational efficiency. As a result, MPC could create new sources of control, new forms of trust, and new types of risk that were not known in existing data sharing approaches. As MPC is emerging in the market (Gartner, 2021), it is important for scholars studying data sharing to understand if and under which conditions existing antecedents are no longer relevant or need to be specified in new ways (cf. Gkeredakis & Constantinides, 2019).

This paper aims to investigate the impact of MPC on perceived control, trust, and perceived risks in the context of data sharing by firms, in order to understand how MPC affects known antecedents of firms' data sharing decisions. To gain an in-depth understanding, we opt for a qualitative approach by conducting semi-structured interviews with experts and practitioners. Then, we establish a set of propositions on the impact of MPC on perceived control, trust, and perceived risk and conditions under which the impact of MPC is deemed relevant. We select a study setting with a high level of risks and need for control, and a low level of trust. We choose a data marketplace setting: a platform to facilitate data sharing and trading between businesses with no prior relationship (Abbas et al., 2021). Since participants in a data marketplace have no prior relationship, they face a lack of inter-organizational trust and control over data (M. Spiekermann, 2019). We specifically focus on data marketplaces in the automotive industry, where key actors like original equipment manufacturers (OEMs) are mindful of retaining control over sensitive data (Docherty et al., 2018; Kerber, 2018).

Based on the research objective and setting, the research question for this paper is: *What are the impacts of multi-party computation (MPC) on perceived control, trust, and perceived risks in data sharing by firms through data marketplaces?*

Our primary contribution is to the literature on business-to-business data sharing. This study is among the first to show that MPC challenges what we know about the key antecedents of data sharing decisions: perceived control, trust, and perceived risks. We develop an understanding of how known data sharing antecedents change or even become obsolete with MPC in place. In other words, we set a basis to extend existing theory on data sharing antecedents to the emerging context of MPC. Our secondary contribution is to the MPC literature by being among the first to explore the business impact of MPC beyond citizen privacy. In this way, we expand the understanding of the socio-economic aspects of MPC, which are overlooked in the MPC literature (Agahari et al., 2021; Agrawal et al., 2021; Bruun et al., 2020; Kanger & Pruulmann-Vengerfeldt, 2015).

Background

Multi-party computation (MPC)

MPC is a cryptographic technique where two or more parties perform a joint computation that results in a meaningful output without disclosing the input provided by either party (Bestavros et al., 2017; Choi & Butler, 2019; Zhao et al., 2019). MPC primarily relies on the secret-sharing protocol, which is efficient and allows the participation of more parties in the computation (Shamir, 1979). Based on this protocol, each party splits its input data into multiple encoded parts called secret shares, which are then computed and recombined to generate the final output. In this way, input data can be computed without revealing any information about it. A popular illustration of MPC is the millionaire's problem (Yao, 1986), a secure comparison function to determine which one of two millionaires is the richest without revealing the net worth to each other. Besides MPC, other technologies also share similar characteristics in enabling privacy-preserving computation (Agrawal et al., 2021), like homomorphic encryption (Gentry, 2009; Naehrig et al., 2011) and differential privacy (Dwork, 2006; Dwork & Roth, 2014). However, according to Apfelbeck (2018), these technologies differ because MPC requires multiple data owners to perform computation, while only one data owner is needed in homomorphic encryption. Moreover, unlike MPC, which uses encryption, differential privacy protects the data by adding random noise during the analysis. Nevertheless, those technologies can complement each other to implement robust security requirements in various use cases (e.g., Alter et al., 2018; Pettai & Laud, 2015; Zhong et al., 2020).

While the theoretical foundation of MPC has been around for some time (Yao, 1982), recent advances in computational power and efficiency are making it closer to implementing MPC in real-life applications. Now, MPC can be deployed in various contexts of use-cases: between companies within the same domain (e.g., assessing common customers between organizations for marketing purposes), across other units within the same company (e.g., cross-selling), and across supply chain tiers (e.g., streamlining manufacturer-supplier in supply chains). Examples include auction-based pricing (Bogetoft et al., 2009), tax fraud detection (Bogdanov et al., 2015), satellite collision prevention (Hemenway et al., 2016), and identifying the gender wage gap (Lapets et al., 2018). There are also some attempts to explore how MPC

can be implemented in data marketplaces. For instance, Garrido et al. (2021) conducted a systematic review to understand the landscape of MPC, homomorphic encryption, and differential privacy within the context of an IoT data market. Moreover, Roman and Vu (2019) combined MPC and smart contracts to propose a data marketplaces architecture. In addition, Koch et al. (2021) used MPC to offer privacy-preserving distributed analytics in personal data marketplaces.

Despite its potential, various barriers hinder MPC adoption by businesses. First, MPC still suffers from performance limitations and scalability issues (Choi & Butler, 2019). This low maturity could result in unclear economic risks and high adoption costs for businesses (Zöll et al., 2021). Second, MPC is deemed highly complex to understand by non-experts, making it difficult for prospective users to be aware of what MPC is capable of (Choi & Butler, 2019; Kanger & Pruulmann-Vengerfeldt, 2015). Third, regulations still tend to discourage data collaboration initiatives and are yet to clearly describe the position of MPC in light of data protection regulations (Choi & Butler, 2019; Zöll et al., 2021). Nevertheless, much of the discussion on MPC has been focusing on technical aspects, particularly improving its efficiency and scalability. Only a small amount of research focused on socio-economic perspectives beyond technical aspects of MPC. For instance, Kanger and Pruulmann-Vengerfeldt (2015) investigated the conditions for MPC adoption and found that MPC developers should focus on its usefulness and finding a target group that needs the technology. Meanwhile, Agahari et al. (2021) found that MPC could enable data marketplaces to employ a "privacy-as-a-service" business model. Moreover, Agrawal et al. (2021) interviewed MPC experts and practitioners to explore design and governance challenges in developing MPC. They argued that future development of MPC should consider issues like explainability, usability, and accountability, in order to promote its adoption. Similarly, Bruun et al. (2020) argued that while MPC offers "trustless trust" that eliminates the need for intermediaries, it raises accountability issues due to the inability to link the results and the original input data. Furthermore, from the legal perspective, Helminger and Rechberger (2022) found that companies using MPC could comply with the General Data Protection Regulation (GDPR) while benefiting from the privacy-preserving computation.

How MPC is used in data sharing: an illustration

To illustrate how MPC is used in data sharing, particularly in data marketplaces, we developed a hypothetical scenario in the automotive industry (see Fig. 1). This scenario was developed based on prior studies (Bestavros et al., 2017; Bogdanov et al., 2015; Bogetoft et al., 2009; Roseman Labs, 2022) and also used to help with the data collection process in this study (see "interview procedures and questions" section). In this use case, we consider an example where three car manufacturers want to monetize their car performance data. One possible option would be through data marketplaces to facilitate matchmaking and data exchange between data owners (i.e., car manufacturers) and data users (i.e., automotive suppliers). However, this option requires data owners to transfer data to data marketplace operators and data users, meaning that other parties can have access to complete datasets during the exchange. As a result, data owners might find it difficult to control what data users will do with the data. Ultimately, data owners might refrain from data sharing and trading.

MPC could tackle those concerns by employing advanced cryptographic techniques for sharing and trading through data marketplaces. First (step A in Fig. 1), automotive suppliers write a query of a meaningful output (i.e., computation results or data insights) that they want to acquire using data marketplaces, like aggregated car performance data from multiple car manufacturers. Subsequently (step B in Fig. 1), each car manufacturer locally encrypts and splits their car performance data into multiple parts using the secret-sharing protocol (Shamir, 1979) as described in the MPC section. Then, these parts are distributed to multiple servers managed by multiple partners and completely independent of each other (Archer et al., 2018). Together, these servers form the so-called privacy engine (Roseman Labs, 2022), which can compute the encrypted and partitioned data according to the requested function (step C in Fig. 1). Each server in the privacy engine calculates parts of data received from different data owners to form partial results that do not reveal anything about the input data (step D in Fig. 1). Finally, those partial results are recombined to form the aggregated car performance data as requested by the automotive supplier as a data user (step E in Fig. 1).

With this use case of MPC in data marketplaces, there will be no movement of datasets from data owners to the data marketplace operator and data users. Put differently, the original datasets owned by each car manufacturer will stay with them, and only the computation results will be revealed to data users. Moreover, to proceed, all data owners have to approve the computation that will be performed or opt-out if they do not want to participate (Agahari et al., 2021). Furthermore, the data marketplace operator will not be able to see the complete datasets during the computation. Thanks to the secret-sharing protocol, the data is encrypted and split into meaningless parts that will not reveal anything about the input data (Shamir, 1979).

To sum up, MPC is expected to change the way inter-organizational data sharing is performed due to its ability to eliminate the need for a trusted third party as an intermediary that performs data processing and analysis. Nevertheless, from a theoretical perspective, the underlying mechanisms behind these changes are yet to be explored due to

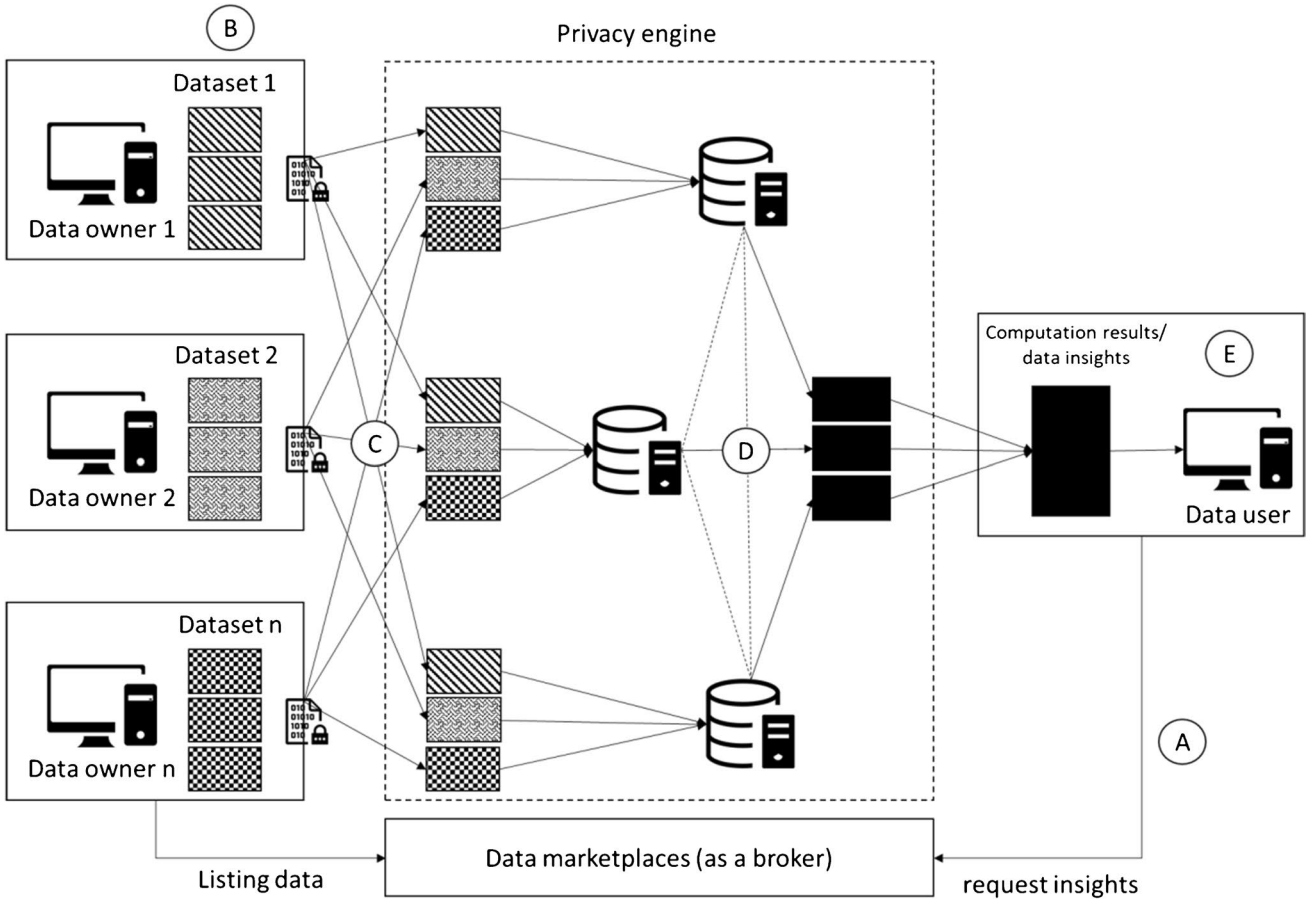

Fig. 1 An illustration of how MPC is used for data sharing in data marketplaces (adapted from Bestavros et al., 2017; Bogetoft et al., 2009; Bogdanov et al., 2015; Roseman Labs, 2022)

the emerging nature of MPC implementations in organizations. Therefore, in subsequent sections, we review existing literature on organizational willingness to share data, three main concepts of interest (control, trust, and perceived risks), and their interrelations. This knowledge will serve as a theoretical basis for what we currently know about inter-organizational data sharing in order to understand the impact of MPC.

Organizational willingness to share data

Literature on organizational willingness to share data draws from multiple theoretical perspectives. One stream of research invokes control and coordination benefits in explaining organizational (un)willingness to share data (Li et al., 2006; Stefansson, 2002). For example, drawing on coordination theory, Li et al. (2006) found that information sharing improves supply chain performance. Firms will participate in data sharing if the benefits are clear to them, such as improving efficiency and stimulating innovation (Fu et al., 2014; Sun et al., 2018). However, firms are reluctant to share data if the cost and investments needed are higher than the benefits they would receive (Penttinen et al., 2018; Saprikis & Vlachopoulou, 2012). Samaddar et al. (2006) explore the relationships between the design of a supply network and inter-organizational information sharing. They posit that strategic information is likely shared in networks with a centralized coordination structure (i.e., centralized authority, control, and decision) since control can be exercised over who uses the shared information. By contrast, operational data is shared to improve coordination and decisions as networks become decentralized to include multiple partners exercising control (Samaddar et al., 2006).

The second stream explains organizational willingness to share data drawing on social-relational concepts such as trust, commitment, reciprocity, and values (e.g., Chen et al., 2014; Kolekofski & Heminger, 2003; Zaheer & Trkman, 2017). For example, Bachmann (2001) points out that while social relations can be considered at the inter-personal level, they are also relevant at the inter-organizational level in building trust and relations between organizations. Studies in this stream draw on theories such as information sharing

(Constant et al., 1994) and social exchange theory (Cropanzano & Mitchell, 2005; Emerson, 1976). For instance, using social exchange theory, Hall and Widén-Wulff (2008) found that the degree of social integration of firms with other partners is more important in influencing firms' decision to exchange information than financial incentives. Also, organizations are more likely to share data if they trust and have a committed and reciprocal relationship (Zaheer & Trkman, 2017). Further, the willingness to exchange information is further strengthened as collaboration grows between organizations (Du et al., 2012).

Finally, the third stream of literature considers context-specific factors such as data standards, security, and the sensitivity of data (Azarm-Daigle et al., 2015; Harris et al., 2007; Shen et al., 2019). For example, in the healthcare domain, organizations are reluctant to share data due to various standards, regulations, and lack of integration across healthcare systems (Azarm-Daigle et al., 2015; Harris et al., 2007). Such risks are evident in this context due to issues like information security and integrity (e.g., Shen et al., 2019) and standardization (Harris et al., 2007).

Taken together, the three streams of literature provide an overview of concepts relevant to understanding inter-organizational data sharing. The first stream outlined the importance of control in data sharing. Control indirectly assumes that organizations (i.e., economic agents) involved in data sharing are self-interested. In this regard, control is essential in preventing collaborating firms in data sharing from pursuing their self-interest alone. However, while an emphasis on control is essential, this first stream neglects the importance of social dynamics among parties that could affect the willingness to share data. Meanwhile, the second stream emphasizes the role of social and relational aspects such as trust in a factor influencing organizational willingness to share data. However, the second stream does not inform us about how trust could be established between firms with no prior business relationships. Furthermore, the third stream focuses on risks stemming from data characteristics. It recognizes that even in the presence of control and trust, willingness to share data might be affected by perceived risk associated with a transaction. However, how the perceived risk of data sharing could be impacted by trust among partners or control to influence the willingness to share data is not discussed in the third stream. Therefore, although the three streams are distinct and focus on three different concepts of control, trust, and perceived risks, they cannot provide a comprehensive understanding of why firms share data with other firms when viewed separately. Instead, each concept complements our understanding of firms' willingness to share data. We elaborate on these concepts and their interrelationships in the following sections.

Perceived control over data

Generally, control refers to any attempt to ensure that the controlee (the target of control) behaves according to the objective of the controller (the source of control) (Tiwana et al., 2010; Wiener et al., 2016). Control is essential in the interaction between the controller and the controlee because their interests are likely to be divergent, for example, due to information asymmetry or self-interest among actors. Hence, the controller typically exercises control via various mechanisms, such as technical artifacts, rules, and incentives, to create convergent goals between the controller and the controlee (Goldbach et al., 2018; Tiwana, 2014).

Current literature differentiates control mechanisms into two distinct types: formal and informal control (Goldbach et al., 2018; Mukhopadhyay et al., 2016; Tiwana, 2014). Formal control can more broadly be considered the visible aspects of control and is further divided into input, process, and output control. In *input control*, the controller implements various selection and acceptance criteria that need to be fulfilled by the controlee before both parties interact. Meanwhile, *process control* focuses on aspects like rules, guidelines, and specific methods that the controlee needs to follow to ensure their behavior aligns with the controller. Furthermore, *output control* broadly includes specifications expected to be fulfilled by the controlee to maintain interaction with the controller.

Regarding informal control, two categories can be identified: self-control and relational/clan control (Goldbach et al., 2018; Mukhopadhyay et al., 2016; Tiwana, 2014). *Self-control* relies on the controlee's commitment to monitor their own behavior independently. Although it is implemented by the controlee, the controller can provide tools and guidelines to strengthen the capacity of the controlee and encourage self-control. Meanwhile, in *clan/relational control*, all controlees are engaged in shared norms and values that can be encouraged by the controller. Ultimately, this could lead to mutual beliefs and common goals among the controlees in producing desirable outcomes that are in line with the primary objective of the controller.

Control in the context of data sharing goes beyond existing conceptualization in the IS literature and, more recently, platform literature. The current view is based on the perspective of the project/platform owner as a controller and focuses on the object that needs to be controlled (i.e., input, process, output, and relations) (Tiwana et al., 2010; Wiener et al., 2016). Meanwhile, the context of data sharing views control from the data owners' perspectives and focuses on data as the object. Our study will adopt the latter view and explore ways to enhance owners' data control. Furthermore, we also investigate the impact of MPC in enhancing owners' control in data sharing.

Drawing from Otto et al. (2019), we refer to owners' data control as data owners' ability to determine data usage by data users. It plays a key role in the data-driven society as firms need to find a balance between protecting their data and sharing data to stimulate innovation (Gast et al., 2019; Otto et al., 2019; van den Broek & van Veenstra, 2018; Vimercati et al., 2021). Lack of owners' data control could result in firms' reluctance to share data, as they fear losing sensitive information that might benefit competitors (Arnaut et al., 2018; Richter & Slowinski, 2019). Hence, firms need to maintain control over who got access to which data and for what purpose (Koutroumpis et al., 2020; Mosterd et al., 2021; Reimsbach-Kounatze, 2021). In this way, firms can protect their valuable assets and maintain an advantage over competitors (Nokkala et al., 2019). Only after firms are able to control data usage and flow would they be more willing to share data with other firms (Dahlberg & Nokkala, 2019; Opriel et al., 2021).

Trust and perceived risks in data sharing

According to Mayer et al. (1995), trust is defined as the extent to which one party (i.e., the trustor) is willing to be vulnerable to the actions of another party (i.e., the trustee). Trust reduces tendencies for opportunistic behavior by firms (Morgan & Hunt, 1994). In data sharing, trust is central as a foundation to sustain interaction between firms (Chen et al., 2014; Richter & Slowinski, 2019; Spiekermann, 2019). Data owners need to trust that data users are committed to the agreement for data usage. Otherwise, data owners will refrain from sharing data (Kembro et al., 2017; Müller et al., 2020).

Prior research has identified various mechanisms that can be used to establish trust in data sharing between firms. One mechanism is *technical solutions*, as proposed by Ratnasingam et al. (2002). Examples include digital signatures, encryption, and authorization, which can be implemented as protective measures to ensure reliable data sharing transactions between firms. Another mechanism is *screening and review* (Richter & Slowinski, 2019; Son et al., 2006; Subramanian, 2017). Such mechanisms can help inform firms about the reputation of prospective data users before deciding to participate in data sharing. Finally, Noorian et al. (2014) proposed a *data use agreement* that clearly states the purpose of data usage, including the penalty that will be enforced in the event of a violation.

Trust is often associated with perceived risk, especially while interacting in an online environment (Nicolaou & McKnight, 2006; Pavlou & Gefen, 2004). Following Pavlou and Gefen (2004), we define perceived risk as a firm's subjective belief of suffering a loss from the occurrence of an uncertain event. Unlike physical goods or other services, data characteristics might pose a higher risk in the context of data sharing for several reasons. First, competitors may use the data in ways that harm data owners' business interests. Through reverse engineering or de-anonymization, data users may identify critical business processes, harming the competitive advantage of data owners (M. Spiekermann, 2019). Second, the possibility to re-sell and re-share data at no cost once exchanged may create risks as unauthorized third parties can use the data in unforeseen ways (Koutroumpis et al., 2020). Third, the possibility of combining the data and the ability to apply algorithms to the data may result in the de-anonymization of personal data and create privacy harm (Li et al., 2020).

Interrelations between perceived control, trust, and perceived risks

The extant literature suggests that control, trust, and perceived risks are vital aspects that affect firms' willingness to share data. Nevertheless, despite being three separate concepts, they are inherently related in a way that trust and risks are seen as consequences of (lack of) control. For instance, firms struggle to maintain control over what and how data might be used by data users once it is shared (Asare et al., 2016). This lack of control could create risks for data owners if they engage in data sharing, like becoming vulnerable to losing competitive advantage or harming the privacy of their end-users. In this regard, trust among organizations could reduce the tendency for opportunistic behavior by firms using the data in the presence of relatively limited control (Emsley & Kidon, 2007; Kagal et al., 2001). Similarly, having control mechanisms in place is also essential in reducing risks involved in transactions and building trust among third parties (Bons et al., 1998, 2012). This can be in the form of formal documents outlining obligations, prohibitions, and commitments among parties (Bons et al., 1998, 2000). At the same time, the trustworthiness of any procedures to control risk is also contingent on the procedures themselves not being vulnerable to risks. For instance, procedures to control risk like inspecting, exchanging, and confirming documents among parties could be susceptible to fraud (Bons et al., 1998). Insufficient trust among parties might arise due to the absence of prior trading relationships (Bons et al., 2012). In this regard, Lee (1998) emphasized that control procedures to establish trust should be accessible to the public or maintained by independent agencies.

In summary, reinforcing various control mechanisms is important in data sharing since it could reduce risks and establish trust between data owners and data users. This interrelation between the three concepts suggests that they cannot be separated in analyzing the impact of MPC in the context of data sharing. In the next section, we confront MPC with these theoretical concepts to understand the

Table 1 Initial propositions

Theoretical concept	Initial proposition
Perceived control over data	P1. Perceived control over data is more relevant while sharing through data marketplaces that use MPC
Trust	P2. Trust is less relevant while sharing through data marketplaces that use MPC
Perceived risks	P3. Perceived risks are less relevant while sharing through data marketplaces that use MPC

expected mechanisms under which MPC could impact inter-organizational data sharing by firms.

Confronting MPC with theoretical concepts

We can now connect insights from the theoretical concepts (i.e., perceived control, trust, perceived risks) with the MPC literature in the context of data marketplaces. This results in initial propositions as a basis to understand the impact of MPC on those concepts while sharing through data marketplaces. First, we expect that MPC could serve as a means for firms to exercise control in data marketplaces by allowing distributed data sharing without storing it centrally. By enabling joint computation between multiple parties and only sharing the results (data insights), sharing individual datasets becomes unnecessary. Moreover, MPC could eliminate the need for intermediaries that performs data analysis and processing. As a result, data marketplaces would only act as a broker that performs matchmaking between data owners and data users (Agahari et al., 2021). The computation will be performed automatically and result in aggregated insights (instead of datasets) that restrict the way data users utilize the data. This approach represents a change in how data is stored and processed, allowing firms to regain control while sharing data through data marketplaces (Agahari et al., 2021). In short, with MPC in place, we expect that perceived control might still be relevant to understanding firms' data sharing decisions in data marketplaces. As such, the first initial proposition of this study is:

P1. Perceived control over data is more relevant while sharing through data marketplaces that use MPC.

Second, we also expect that MPC could impact trust in data sharing through data marketplaces. With MPC, data owners and data users can still perform computation together and generate insights while keeping the data secure. In this regard, there is no need to establish trust between both parties (Hastings et al., 2019). Trust in intermediaries is also eliminated since MPC essentially removes the need for a trusted third party that performs data processing and analysis. This line of argument suggests that trust in data sharing might be less relevant with MPC in place. Therefore, our second initial proposition of this study is:

P2. Trust is less relevant while sharing through data marketplaces that use MPC.

Third, MPC is expected to impact perceived risks in data sharing through data marketplaces. As described earlier in this section, data users are only allowed to receive computation results without revealing the input data. In this way, data owners have more control over how the data is processed and utilized by data users. Hence, data owners might not feel risky anymore to engage in data sharing because their data stays with them during the computation. This line of argument suggests that perceived risks in data sharing might be less relevant with MPC in place. Therefore, we propose that:

P3. Perceived risks are less relevant while sharing through data marketplaces that use MPC.

Table 1 summarizes the initial propositions based on the theoretical concepts.

These propositions are important as a basis for the data collection and analysis processes, particularly during the development of interview protocol and the coding of interview transcripts. Furthermore, based on the findings, our initial propositions might need to be refined. Therefore, in the next section, we describe our research approach in investigating whether our initial propositions are applicable in studying MPC or need to be specified further.

Research approach

We employ a qualitative research approach in this paper, which is suitable for the exploratory nature of our research objective (Verschuren & Doorewaard, 2010). While much research has been done on control, trust, and perceived risk as antecedents of business-to-business data sharing, the impact of MPC has not yet been studied empirically. This is because MPC is a relatively new technology and has not been applied in the context of automotive data marketplaces, leading to a limited understanding of the phenomenon. Hence, the qualitative approach allows us to investigate the "why" and "how" concerning the possible link between MPC and implications for perceived control, trust, and perceived risks, as well as conditions for these implications to materialize (Recker, 2013). We opted for semi-structured

interviews with experts and practitioners as our data collection strategy. This technique is beneficial to be used in our study as it offers both rigidity (i.e., guided by pre-defined general questions) and flexibility (i.e., allows improvisation based on interactions with interviewees) (Kallio et al., 2016).

As for the research context, we focus on the emerging area of data marketplaces, particularly in the automotive industry. It is suitable for our study as it represents settings with a high fear of losing control over data, low trust between actors, and high risks of data sharing (Koutroumpis et al., 2020; Spiekermann, 2019). Although data marketplaces are perceived as the key enabler for the data economy (European Commission, 2020) and do exist in the automotive sector (e.g., Caruso,[1] Otonomo,[2] and Automat[3]), their adoption is still limited. Generally, firms are unwilling to share data through data marketplaces due to the fear of losing control over sensitive data that might benefit competitors (Koutroumpis et al., 2020). This is especially true for automotive firms like original equipment manufacturers (OEMs), car insurance companies, and mobility service providers, who are known to be very conventional and secretive when dealing with their car data (Docherty et al., 2018; Kerber, 2018). Nevertheless, the growing trend of digitalization drives firms to open up (access to) their data for developing novel products and services (Günther et al., 2017; Hartmann et al., 2016). Examples in the automotive sector include connected cars, usage-based insurance, and shared mobility (Athanasopoulou et al., 2019; Kaiser et al., 2021). the importance of control over data, trust, and perceived risks of data sharing in this domain make it highly relevant to investigate the impact of MPC on those aspects.

Sample selection

We followed a judgment sampling approach in recruiting our interviewees (Sekaran & Bougie, 2016). We selected interviewees with expertise in the data-related role in the automotive and mobility industries. We started by leveraging our networks to select potential interviewees in these industries. As a complement, we looked into relevant scientific articles to identify relevant scholars who work in the area of, e.g., data marketplaces, data platforms, automotive data sharing, and connected cars. Moreover, we consulted grey literature such as reports and white papers to gather additional business actors. After each interview, we employed a snowball sampling approach by asking them to recommend the next potential interviewees. After the interviews did not provide new information, we stopped looking for new candidates.

Table 2 presents an overview of our interviewees, organized based on the order of the interview. Twenty-three interviews with automotive experts and practitioners were conducted online from June to October 2020, with sixteen of them coming from businesses. From this number, three interviewees worked in relatively new companies in the automotive and mobility sector, while the rest worked in established companies. All of our interviewees are men and hold positions at a senior management level with an average of nine years of experience.

Interview procedures and questions

To ensure that interviewees had the same understanding of data marketplaces and MPC, we developed a short presentation explaining (1) the definition of data marketplaces and their use cases; (2) how MPC works and its use cases; and (3) how MPC can be implemented in data marketplaces. This presentation was validated with MPC experts (Agahari et al., 2021) to ensure we provided correct information to our interviewees on how MPC works. We gave the presentation at the beginning of each session of one interview, in which we offered interviewees an opportunity to clarify and discuss each concept to reach a common understanding. Any feedback that we received was used to refine the presentation, which was shown in the subsequent interview. This way, we can improve interviewees' understanding of MPC definition and use cases.

Nevertheless, this approach could lead to a potential bias due to interviewees' reliance on our explanation of MPC in answering interview questions. However, the explanation is based on the literature (see the background section), validated in an expert study (blinded for review), and kept constant in each interview. In this regard, we minimize the potential bias resulting from our approach. Furthermore, as always the case in understanding new phenomena, explaining MPC use cases are inevitable since it is still in an early stage of development and adoption by businesses, with few known implementations of MPC in data marketplaces.

To guide the interview, a protocol based on the theoretical concepts (see the "background" section) was developed by the first author, which the third author then reviewed. The questions for each concept comprise one question about the current situation of data sharing without MPC and one question about the impact of MPC (see Table 3). In the first part, after introducing the concept of data marketplaces, we asked questions about the current data sharing situation (without MPC). We did this to get interviewees in the mood to talk about data sharing and invite them to be as close to the current situation as possible. Then, we moved to the second part of the interview, starting with introducing interviewees to

[1] https://www.caruso-dataplace.com/

[2] https://otonomo.io/

[3] https://automat-project.eu/

Table 2 Overview of interviewees

ID	Organization	Type	Profile	Experience (in years)
A01	Research institution	Expert	Project manager and doctoral researcher (B2B digital platforms)	7
A02	Not-for-profit research and consulting institution	Expert	Researcher and project manager (data spaces in the mobility sectors)	5
A03	Platform integrating shared mobility services	Newcomers	Head of partnerships & business development	3
A04	Research institution	Expert	Scientific director (IoT and business model innovation)	10+
A05	Insurance company	Established players	Fraud investigation specialist	10+
A06	Technology advisory and consultancy service	Established players	CEO	10+
A07	Mobility software and data analytics service provider	Newcomers	Business development consultant (transport and mobility)	10+
A08	Innovation lab for data marketplaces technologies	Expert	Initiator and digital connectivity lead	9
A09	Research institution	Expert	Senior scientist (transport and urban mobility)	10+
A10	Payment provider	Established players	Head of connected car & IoT	7
A11	Automotive R&D company	Established players	Product line manager (data intelligence)	10+
A12	Mobility service provider	Established players	Senior product manager (dynamic services)	10+
A13	Car OEM	Established players	Function owner for privacy management	4
A14	Advisory and consulting	Established players	Associate director & advisory (mobility & automotive)	7
A15	Automotive supplier	Established players	Senior manager (IoT business model innovation)	8
A16	Corporate mobility consulting service	Newcomers	CIO	5
A17	Automotive R&D center	Expert	Senior researcher (connected car)	8
A18	Fleet management software provider	Established players	Product manager (connected car)	7
A19	Platform integrating connected car services	Newcomers	Co-founder and head of data transformation	10+
A20	Car OEM	Established players	Business development manager (connected car)	10+
A21	Car OEM	Established players	Project manager (connected car)	3
A22	Car OEM	Established players	Product owner (car app store)	4
A23	Automotive bodyshop association	Expert	Public affairs & communication	4

Table 3 Interview protocol

Theoretical concept	Guiding questions	
	Part 1: data sharing without MPC	Part 2: data sharing with MPC
Organizational willingness to share data	What are the reasons behind your company's decision to share/not share data in data marketplaces?	With MPC in place, would it change your opinion on sharing those data in data marketplaces? Why?
Control in data sharing	What kind of control over data would you want while sharing in data marketplaces, and why?	With MPC in place, do you expect to have more or less control over those data while sharing in data marketplaces? Why?
Perceived risks	What risks might emerge if your company starts to share data in data marketplaces? How do these risks play a role in your company's decision to share those data?	With MPC in place, do you expect to encounter more or fewer risks of sharing those data in data marketplaces? Why?
Inter-organizational trust	What about trust towards other business actors that would get access to the data? How does it play a role in your company's decision to participate in data sharing?	With MPC in place, do you expect to have more or less trust towards other business actors while sharing those data in data marketplaces? Why?

MPC and its possible use case in data marketplaces. We then asked questions about the impact of MPC on each concept. We did this to allow interviewees to critically reflect on how MPC changed the current data sharing situation. By dividing the interview into two parts (without and with MPC), we can better understand the baseline conditions of data sharing

Table 4 Examples of coding schemes

Quote	Assigned codes
"… they will have much more control. And as you have more control over the data, you do not have to have the same level of trust in the other party. The more control you have of the data, the more you control how it can be used. The less you have to trust in the partner not cheating on you." [A06]	• MPC could increase control over data, only share insights not input data • MPC could increase trust between data owners and data users
"… what is the data going to be used for? I can give you an example. When we ask for sample data from an OEM, they put in the contract that they want to be informed about what things we want to develop from the data. They want to have pretty good insight into what we are doing with the data. And, of course, it is very restricted. You can only use it for those purposes. [In that case,] no misuse is happening." [A12]	• Control: strict terms & conditions/data sharing agreements • Data sharing is based on the use case • Risk: data misuse risk • Trust: what are the intended party does with the data
"At the moment, I think when you want to develop a service, you must discuss with them and present your idea. If they see a chance that there might be a risk, then they will discuss it with you. And maybe [they will] prohibited it and say you are not allowed to do this and that with the data. We have GDPR in Europe, so, in general, I think you must say what you will do with the data before you collect it in terms and conditions. So, I think that is what they want to check." [A17]	• control: authorization • control: strict terms & conditions/data sharing agreements • control: who is using the data and for what purpose
"I think the concept is very promising since it does not require you to share the original data or, let's say, the sensitive data outside. It basically provides you a means or a way how to share this data without actually sharing it, which is great. But then, as I mentioned again, the second issue, next to the part about the broker's involvement, is the ambiguous definition." [A21]	• MPC could increase control over data, only share insights not input data • MPC enables sharing data while preserving the confidentiality • MPC: need to understand the viability of MPC

without MPC and compare them with the expected impact of MPC in data sharing.

Each interview was conducted via video call by the first author and lasted for one hour on average. All interviews were recorded, transcribed, and sent back to interviewees for approval. We anonymized transcripts to prevent revealing confidential information. After each interview, we wrote down key insights and interesting remarks as input for analysis.

Analysis of data

Each interview was coded and analyzed individually using ATLAS.ti 9.0 software. The first author did the coding process based on open, axial, and selective coding (Bryant & Charmaz, 2007). In the open coding phase, an initial code list based on the theoretical concepts, the impact of MPC, and boundary conditions were used to guide the analysis. These codes were assigned to each statement in the transcript based on its relevance. However, additional and unexpected insights that go beyond the theoretical concepts were also included as additional codes. This process of keeping an open mind is important to prevent missing out on insights that might explain our findings (Miles & Huberman, 1994). Examples of coding schemes are provided in Table 4.

In the axial coding phase, codes from all transcripts were combined, resulting in a long list of similar and overlapping codes. Then, similarities and relations between codes were analyzed and merged into high-level concepts. For instance, codes such as *agreements*, *contracts*, and *consent* were grouped into one broader category of *contract-based control*. See Table 5 for examples of merged codes. In this phase, categories and sub-categories were also reconsidered and adapted when needed. For example, the category "boundary conditions" was not considered in the first coding round. It is only added during the axial coding because it explains conditions under which MPC impacts control, inter-organizational trust, and perceived risks in data sharing. Table 7 in the Appendix provides a grounded table of categories and sub-categories.

Finally, in the selective coding phase, all codes were re-examined to establish an understanding of how they are related to the main topic of the impact of MPC on control, inter-organizational trust, and perceived risks in data sharing. This was done through regular discussion between the first and the third author. The first author reviewed memos and notes written down during each interview to develop argument lines. Then, the first author identified and structured the connections between codes and high-level concepts, which resulted in a preliminary summary outlining the impact of MPC and its boundary conditions. As a next step, the third author critically reviewed categories and sub-categories to check for their interrelations as well as arguments and consistencies. Based on this review, the first and third authors discussed further and made

Table 5 Examples of code merging in the axial coding phase

Original codes	New code after merging
Authorization	Contract-based control
Contract	
Data sharing agreements	
Trust towards the partner	Trust in actors
OEMs consider sharing data with trusted parties	
Not too much data sharing between OEMs	
Knowledge spill over	Competitiveness risk
Risk of having a direct competition with others on selling data	
The benefit of using MPC is unclear	Perceived benefits
Need to understand if MPC changes the business model and data sharing landscape	
MPC puts back some burden of providing data to OEMs	Organizational readiness
With MPC data buyers still needs to do data cleaning	
Managerial maturity	
OEMs only willing to share generic, non-sensitive data	Perceived data sensitivity
MPC would not change willingness to share strategically relevant data	
Data sharing depends on data type	

Table 6 Refined propositions based on the findings

Theoretical concept	Specified concept	Refined proposition
Perceived control over data	Technology-based control	P1a. Technology-based control is more relevant while sharing through data marketplaces that use MPC
Trust	Trust in actors	P2a. Trust in actors is less relevant while sharing through data marketplaces that use MPC
	Trust in technology	P2b. Trust in technology is more relevant while sharing through data marketplaces that use MPC
Perceived risks	Competitiveness risk	P3a. Competitiveness risk is less relevant while sharing through data marketplaces that use MPC
	Data misuse risk	P3b. Data misuse risk is more relevant while sharing through data marketplaces that use MPC

changes to codes. This discussion resulted in five propositions pertaining to this research, which are summarized in Table 6.

Findings

This section presents our findings based on three coding rounds. In discussing perceived control, trust, perceived risks, and boundary conditions, we first elaborate on interviewees' views concerning the current data sharing situation without MPC (as-is conditions). This serves as a baseline for the current situation, which is essential because we want to know the changes that resulted from implementing MPC. Then, we outline the implications of MPC on those factors (to-be conditions). We use an identifier from Table 2 (e.g. (A01)) to refer to the interviewees throughout this section.

Perceived control over data

Most interviewees generally agreed on the importance of having control while sharing via data marketplaces. As data owners, firms demand information about who the data users are, what kind of data they need, and the purpose of data usage (A14). This is important so that firms can avoid mistakenly giving away (access to) sensitive data that are not supposed to be shared (A21). Firms also "still want to own the data" (A09) and maintain control "in a way that data cannot be manipulated" (A03). Hence, during data sharing via data marketplaces, firms would like to know "where [the data] is going,... so we know where our data is at every point of time" (A21). In this regard, ensuring the compliance of data sharing rules and agreement is necessary (A08). Once data users violate this agreement, firms should be able to refrain from data sharing (A07, A22) to maintain control over the flow of their data (A07). Nevertheless, interviewees

are well aware that such requirements of control over data are challenging to realize in practice because "if you give somebody a dataset, you can hardly regulate it and cannot find out what people ultimately do with it" (A04).

Our interviewees outlined various control sources that should be present within the context of data sharing. Based on their elaboration, we clustered those control sources by comparing their similarities and differences. Our clustering resulted in three self-developed categories representing different control sources in data sharing. First, *contract-based control* refers to an arrangement to govern provider-buyers relationships concerning data access and usage. One example includes data-sharing agreements and contracts to define the purpose of using the data (A14), which is vital as some data is highly confidential and cannot be utilized beyond the agreed use case. Another mechanism is authorization, meaning that only parties with agreement and permission can get (access to) the data (A03). This mechanism could also be adjusted to allow different data users to access different data types. In this way, data owners can ensure that "the data reaches only [data users] that is intended to have the data" (A06) and "others who have a different security level are not allowed to look at that data" (A09).

Second, *structural-based control* refers to how the networked relationships between data owners and data users are structured. One way to implement this control mechanism is by keeping the data on the premises of data owners (A07) and "only provide [data users with] a way to process this data [while] not giving them access to the entire data" (A20). Firms could also opt for a bilateral partnership without intermediaries. Some interviewees prefer to pursue this approach because "it gets tricky whenever you have someone who is managing, storing, and brokering your data for you" (A21). Alternatively, companies could also implement this control mechanism by sharing data with existing partners in a closed ecosystem. This setup is more restricted and typically only filled by a network of firms that have already worked together for a long time (A19). Because firms do not want to destroy long-standing business relationships, firms are more likely to be more compliant (A14).

Third, *technology-based control* refers to any technological solutions to enforce control for data owners in data sharing. Interviewees frequently mentioned technical approaches like anonymization, encryption, and aggregation as ways to prevent data misuse, comply with privacy laws, and ensure that the data cannot be traced back to individual people (A09, A12). As long as these control measures are present, interviewees argued that companies would have no issue sharing and monetizing their data through data marketplaces (A12, A20). Nevertheless, some interviewees questioned whether "the technology is the right way to solve [the problem of control]" (A04) because "from the technical aspect, the technology is known... and not the issue [in data sharing]" (A21). Instead, some interviewees suggest that measures like contracts and rules are the most appropriate solution (A04).

Interestingly, interviewees pointed out a trade-off between data usability and data misuse risk concerning control in data sharing. On the one hand, a stricter control might result in unusable data. On the other hand, less control might lead to data misuse, and the data may end up somewhere unwanted. As one interviewee put it:

> You want to introduce these anonymization measures. But, . . . you can be very restrictive. The use case of the data that can be used is decreasing, so the data becomes less valuable for the market. That's an important balance to keep. . . . [Y]ou need to also take into account that it doesn't hurt the other part of the equation so that the data is still usable and still both for kind of offline and real-time use cases. (A12)

Zooming in to MPC, our interviewees expressed positive impressions towards this technology as a *technology-based mechanism* to enhance control over data. MPC makes it possible for data owners to "restrict what [data users] can do with the data" (A08) because it enables them to only share the computation results without having to release the input data (A01). The way MPC facilitates "a way how to share this data without actually sharing it" (A21) allows data owners to "preserve some information that they do not want to become public." (A02).

> You control what [can be] done with the data . . . [I]n this case, you do not just offer access, but you only give away the insights you want to give . . . [W]hen I think about it again, there is a relevant improvement in what you call a control. And especially in terms of what is done with the data, that you have more control over that. (A01)
>
> We need [MPC technology] to make sure that you get your answers, but I am sure you will not be able to do anything else with it. Then you are getting your answers. . . . I can check with MPC what can be done and what cannot. . . . [I]t might also be a good possibility to not share my original data but share a data set with you, which looks like [it] but cannot be traced back to your actual data. (A08)

Overall, findings suggest the relevance of control while sharing through data marketplaces, even though it requires a balance between usability and data misuse risk. Moreover, control in data sharing should be specified into three control sources: contract-based, structural-based, and technology-based control. Furthermore, technology-based control becomes more relevant with MPC since it enables control using a technical solution that facilitates sharing of

computation results without revealing the input data. Based on these findings, we propose that:

P1a. Technology-based control is more relevant while sharing through data marketplaces that use MPC.

Trust in data sharing

Interviewees expressed that firms generally have little trust in this emerging approach for data sharing through data marketplaces (A08). In this regard, interviewees stressed the importance of establishing *trust in actors*, which is trust between actors involved in the value network of data marketplaces: data owners, data users, data marketplaces operators, and end-users/consumers. In sharing data through data marketplaces, it is important for firms that act as data owners to establish trust with data users. This is because it is difficult for data owners to track the usage by data users once the data is shared (A06). Hence, firms would be more willing to share data with other firms that already have had a good relationship for a long time and have always been loyal to each other (A15). Moreover, given the involvement of third parties as intermediaries, data owners also need to establish trust with data marketplaces operators (A08, A11). One way to do that is by having a neutral third party as an operator. In this way, firms can ensure "everybody has an equal interest, and they are not acting in the interest of one company" (A16). Furthermore, since end-users or consumers (in our case, car owners or drivers) own the data generated in the car, they should have the final say on whether they are willing to give away their data or not (A18). Interviewees indicate that end-users have little to no degree of trust towards data owners (in our case, OEMs), saying that they either "[do] not want to share because they do not trust the OEMs" (A19) or "trusting OEMs that they do not do anything with my data … or gives me some disadvantage in any kind that you can consider" (A15).

Interestingly, other interviewees offered a different angle on trust by arguing that a lack of trust does not always hinder firms' willingness to engage in data sharing (A04). This is because trust is often viewed as a secondary aim and should be discussed within the benefits and use-cases of data sharing (A04). One interviewee even claimed that firms "do trust each other, but they are in a competition, and the competition matters" (A01). Therefore, decisions to share data through data marketplaces are more driven by strategic consideration instead of trust issues to gain economic benefits (A19).

> [I]f you are talking about business, I think in general there is little trust. So, I would never do anything with this type of data if I have the concerns I am talking about now based on trust. (A07)
>
> [N]o one trusts anyone because right now [because] it is all about negotiation positions [that] you try to strengthen or weaken in the digital age. . . . [E]veryone tries to keep the data for themselves in the first place. … in this case, [trust] actually does not play a role. (A15)

Regarding MPC, it is seen as a game-changer in the dynamics of trust in data marketplaces. MPC could facilitate collaboration between data owners and data users without fully trusting each other. In other words, MPC could potentially reduce the relevance of trust in actors in the context of data sharing through data marketplaces. This is possible since the input data is kept secure, and only the computation insights are provided. As a result, data owners could, in theory, allow data users to utilize the computation results while ensuring that they could not misuse the dataset beyond the data usage purpose. MPC could also become a novel approach to "ensure that the other partner cannot cheat the system" (A06), suggesting that trust in data marketplaces becomes less important.

> As you have more control over the data, you do not have to have the same level of trust in the other party. The more control you have of the data, the more you control how it can be used [and] the less you have to trust in the partner not cheating on you. (A06)
>
> [D]oing [data sharing in data marketplaces] based on an MPC algorithm where the OEMs keep control of their data and not giving away their data to other parties gives them trust to actually collaborate because they do not have that much more to lose anymore. (A15)

Strikingly, some interviewees argued that MPC is not just about reducing the relevance of inter-organizational trust but increasing the importance of *trust in technology*. The newness of MPC creates many questions on how it works, who the operator is, and its position in the whole data sharing process in data marketplaces. The lack of clarity makes people cautious and even skeptical about the impact of MPC on trust in data sharing through data marketplaces.

> I think this is highly connected to the trustworthiness of the MPC provider/operator. I think the whole thing works or does not work. But the question about who is the MPC is the trustworthy institution. And if that is the case, then that would add a lot to trust for the overall process. I think you need an intermediary to help there. I think you are not in a position to increase the trust among the actors by introducing a marketplace, but if you have a trustworthy process, then it could work. (A01)
>
> If the data marketplace or this MPC provider is not involved in the negotiation, I do not think the trust

> will not be provoked there. I believe they need to be involved because, again, I think big players will always fear or would always have trust issues with a party that they do not negotiate the terms of condition with. (A21)

Findings suggest that, while trust towards actors involved in data sharing is relevant, it is often a secondary aim that is embedded in the benefits and use cases of data sharing. Moreover, MPC reduces the need for trust in data sharing actors in collaborative data sharing, making it less relevant. Furthermore, MPC raises trust issues in its protocol due to a lack of accountability mechanism, resulting in the relevance of trust in technology. Therefore, we propose that:

> *P2a. Trust in actors is less relevant while sharing through data marketplaces that use MPC.*
> *P2b. Trust in technology is more relevant while sharing through data marketplaces that use MPC.*

Perceived risks in data sharing

Interviewees confirmed that it is very risky for firms to participate in data sharing, especially in the emerging context of data marketplaces. *Competitiveness risk* is one of the biggest risks, in way that firms could lose an advantage over competitors if they participate in data sharing via data marketplaces. In the automotive industry, OEMs are typically reluctant to share because "they want to create a monopoly in the market" (A16). Opening up (access to) data by OEMs through data marketplaces could result in knowledge spillovers, allowing competitors to compare and develop better cars. This creates a situation where data "becomes a commodity" (A21), which is disadvantageous for OEMs because "their unique selling points are being taken away" (A06). As one interviewee put it:

> [T]hey are . . . not so willing to share data . . . [because of] a competitive position. If company X knows how many times the trunk will open and close and how strong you should make it, then . . . you got extra insights in product development. . . . [I]n the end, it has an impact on your competitive position because you are, for example, more efficient in producing a car because you can make it lighter or cheaper. (A14)

Interviewees also expressed concerns regarding *data misuse risk*. If firms decided to participate in data sharing through data marketplaces, data users would use the data for other purposes that were not originally intended. Once the data is shared, it is difficult for data owners to check the purpose of data usage by data users (A08). This condition creates a risk in which data users could "use [the data] in any way that is harmful" (A01), such as security breaches in connected cars by hackers (A23).

> I can give you my data, but I cannot check if I say, "you can use this data for a certain sort of goal, which I would not like you to use for your commercial advantage or something." . . . Will they exploit [the data] to other means than I want to? (A08)
> We do not know how the third party would handle our data. . . . We [as an OEM] would like to share [data] with an automotive supplier through a data broker . . . but we do not know how the data marketplace would handle our information or data. (A21)

Moreover, most interviewees agree on the importance of *reputation risk* for data owners (in this case, OEMs), as they must maintain their brand and image to their end-users. In this regard, OEMs consider data sharing as a high-risk activity that could result in big protests if something terrible happens, like a privacy violation (A01) or a possibility that "others might find problems in [their] data" (A17). OEMs would like to save themselves from those troubles and prevent "negative or bad publicity when it comes to the usage of data" (A20). OEMs are also unwilling to pay huge fines since it is "damaging not only from the amount of profit that we receive per year but also from our reputation as a car company" (A13).

> For OEMs, especially premium OEMs, the brand is very important. So they cannot damage the brand of the car. You do not want to have a news headline that OEMs sold thousands of user data, and now you can track where you went with your car or something. That cannot happen. (A12)

Furthermore, *end-users privacy risk* is highly relevant in data sharing via data marketplaces. Interviewees pointed out that the emergence of connected cars makes it possible for OEMs to collect data about how their car users behave every day (A19). This is not taken lightly by car users, resulting in a cautious approach by OEMs in data sharing to prevent breaching car users' privacy. The strict implementation of the General Data Protection Regulation (GDPR) also makes OEMs more aware of the importance of protecting customers' interests in safeguarding their personal data. Hence, OEMs are trying to "protect the benefits of our customers" (A18) before taking part in data sharing; otherwise, they are at risk of getting a fine for violating GDPR.

> [OEMs] care about privacy; they care about data ownership. They question certain legal issues, whether they can share or not share data, which makes this data sharing so hard because it takes a lot of time and costs a lot. (A08)

Additionally, interviewees mentioned that data interoperability between different OEMs might create data quality risk since the data are defined in different formats. As a result, OEMs need to make much effort in aggregating and harmonizing the data before it is usable for other parties (A12). OEMs are also afraid that poor data quality might lead to misinterpretation and misunderstanding of the data (A12, A17). One interviewee stated that:

> If the data is wrong in the first place (garbage in), then a guy gets garbage out. But, if you do not know that, then the whole chain spent a lot of money without any use. (A09)

As for the impact of MPC in addressing those risks, we found that MPC could reduce the relevance of competitiveness risk for data owners. MPC could restrict data usage by data users and only allow them to get answers from the computation. This mechanism could reduce the risk of knowledge spillover to competitors, preventing them from gaining a competitive advantage. Nevertheless, the reduced risk also comes with an increased burden for both data owners and consumers, as they have to prepare better data that suit MPC requirements and clean the data themselves after acquiring it.

> I think it will change, but there is an increasing responsibility on the side of the data owners because they know what the requesting party wants to do with it. . . . [T]he overall risk is reduced, but the potential responsibility on the data owner side is increased . . . (A01)
> [W]hat they do not like is to provide the data to the competitors and allowing the competitors [to show] the advantage in using their [competitors' data] and not the other. If the data are not publicly available but only in an aggregated format, this usage of data from the competitor is not possible. So the risk does not exist. (A02)

However, the use of MPC could also increase the possibility of data misuse risk for data users. With MPC, data users need to ask queries (i.e., what kind of answers/insights do I want to know?), meaning that they need to reveal the process of analyzing the data (in the form of questions) through MPC-enabled data marketplaces. Such questions could allow data owners to reverse engineering and understand "the know-how" of data users, potentially leaking valuable information that data owners could misuse.

> Now, it is the other way around, I think. Because by specifying the aggregations, if I tell my supplier how to calculate and aggregate the values and how to assess the data, then I give away my own know-how. So now, the automotive suppliers need to at least tell the data marketplace and data owners on how the data must be aggregated. And this is sometimes already good know-how and the intellectual property of the data processors, the data analytics, and so on. So maybe now the OEMs who give away the data feel more confident, but now data users need to release a lot of their know-how because they need to specify how the data must be aggregated. (A11)

Findings suggest that, in sharing through data marketplaces, perceived risks should be specified into competitiveness risk, data misuse risk, end-users privacy risk, and reputation risk. As for the impact of MPC, it could make the competitiveness risk less relevant in data sharing by preventing knowledge spillover through the restriction of data usage. However, MPC could also increase the relevance of data misuse risk by potentially revealing firms' know-how and allowing reverse engineering through queries asked by data users. Based on these findings, we propose that:

> *P3a. Competitiveness risk is less relevant while sharing through data marketplaces that use MPC.*
> *P3b. Data misuse risk is more relevant while sharing through data marketplaces that use MPC.*

Boundary conditions for the impact of MPC on perceived control, trust, and perceived risks in data sharing

Interviewees pointed out that several conditions should be considered for the impact of MPC on perceived control, trust, and perceived risks to materialize. First, firms need to be sure of the *perceived benefits* in return for sharing data using MPC in data marketplaces. This is important as all business activities are about maximizing their profit by "creating value [and solving] customer problems" (A04). Examples of benefits mentioned by interviewees are personalization, service improvement, and direct monetization through data selling (A21). In the context of MPC, the main question is whether "some statistics [are] always enough, and how far can [firms] go [with MPC]" (A04). While MPC could be valuable for firms by generating insights from aggregated statistics, it might vary depending on domains and prospective users (A07). Therefore, firms would constantly assess if using MPC for data sharing is beneficial and valuable for their business.

> [I]f data privacy technology [like MPC] helps them to assure that they can monetize data better under the law, or with less risks in terms of data privacy concerns, then [firms] would be happy to employ that. (A15)

> If [MPC] is really . . . cost-efficient, cost-saving, and quality increasing, then [firms] will go for it. But otherwise, they will leave it alone. (A19)

Second, embedding MPC to data marketplaces might increase complexity for firms as they need to have sufficient *organizational readiness,* including data pre-processing skills such as cleaning and harmonization. This is due to the possible change in the role of data marketplaces operators towards pure matchmaking. In this regard, the computation is done directly between firms (i.e., data owners and data users). Hence, without proper data pre-processing skills, firms might find it challenging to materialize the impact of MPC. Furthermore, firms might not even be willing to share data through MPC if it is too costly and burdensome for them.

> [I]t looks to me that this technology shifts some value from the data marketplace provider and puts back some burden on the OEMs. If it is now more costly or complex for OEMs to provide data, then the technology adoption could be more difficult. . . . [T]he focus [of MPC] is so much on data anonymization, [while] the buyer still needs to do certain pre-processing to clean the data. . . . The fact that it seems to put more burden on the OEMs could worsen the willingness to share data if it is too costly. (A12)

Third, the impact of MPC would depend on *perceived data sensitivity*. Most interviewees agreed that firms would only be willing to share generic and non-sensitive data through data marketplaces. In the automotive sector, OEMs will refrain from sharing data that are "relevant for the development of vehicles" (A11) or "if it comes close to competitive edges" (A14) since competitors might be able in the future to "decompose the way that the vehicle's system works and copy what an OEM has built if you give away the data" (A17). Hence, OEMs are trying to protect their data as much as possible and not share it with others. Embedding MPC into data marketplaces is unlikely to change this situation. As data owners, OEMs might still feel hesitant to give away sensitive data, even though MPC could allow sharing only computation results without revealing input data. They would consider MPC useful if the shared data are non-core, non-sensitive, and non-strategic.

> I think for data types for which the company does not see as core values for their own strategic interest in their own service development, it would make the idea of offering and transacting these data [using MPC in data marketplaces] would help with that. (A01)

Taken together, the impact of MPC in data sharing would be apparent for firms when three boundary conditions are present. First, the benefits of using MPC and its relevant use cases must be clear (i.e., perceived benefits). Second, firms must have a data-driven mindset and possess data pre-processing skills like data cleaning and harmonization (i.e., organizational readiness). Finally, due to the early adoption phase of MPC, firms will only share data that are considered non-sensitive and generic (i.e., perceived data sensitivity).

Discussion

We found that MPC changes the relevance of control, trust, and risk in sharing through data marketplaces, particularly in the automotive industry. These factors should be specified in new ways to understand firms' data-sharing decisions through MPC-based data marketplaces, namely *technology-based control*, *trust in technology*, and *data misuse risk*. Moreover, we found that trust in other actors involved and competitiveness risk, which was relevant in the current data sharing situations, are less relevant with MPC in place. Furthermore, we found three boundary conditions in which the impacts of MPC on these factors are relevant: (1) firms' perception of the benefits of using MPC; (2) firms' organizational readiness in terms of data skills and data awareness; and (3) firms' perception about the sensitivity of their data. Table 6 summarizes the propositions derived from the results, which were updated from the initial propositions in Table 1.

Regarding owners' data control, we identified contract-based control, structural based-control, and technology-based control as relevant control mechanisms in the context of data sharing. This finding extends existing knowledge of control theory in the IS literature, which typically emphasizes the object of control (input, process, output, and relations) (Tiwana, 2014; Wiener et al., 2016). We also find that MPC is seen as a technology-based mechanism that enables data owners to have more control over how their data is used (see P1a in Table 6). This finding is consistent with Garrido et al. (2021), who found that the MPC can enhance control over input data and the computation process while maintaining data utility. As a result, MPC guarantees that the data users will only receive the computation results and not the input data. This is important as firms mainly own sensitive and confidential data, making it necessary to ensure no leakage that might result in competitive disadvantage

or breach of end-users privacy. Furthermore, we provide support to the work of S. Spiekermann (2005), who argued that privacy-enhancing technologies (PETs) could enhance control in the context of ubiquitous computing. We demonstrated that MPC, as one class of PETs, could also create a similar effect in a different setting, particularly in sharing data in automotive data marketplaces.

We also found that collaborative data sharing with MPC requires less trust between the actors involved since MPC enhances control over data during the computation. This finding means that, at least in theory, firms do not need to worry that their counterpart will get access to the input data since only the computation results will be revealed to requesting party. This finding also challenges the current understanding of trust, commitment, and reciprocal relationships with other firms as preconditions for data sharing (Zaheer & Trkman, 2017). However, an interesting observation is that while MPC could reduce the need for trust in actors involved in data sharing, it could raise trust issues concerning the underlying algorithms that execute the protocol. In this regard, we argue that MPC could change the way we conceptualize trust in data sharing. Traditionally, scholars see the trust between actors (i.e., inter-organizational trust) as a key aspect influencing data sharing decisions (Müller et al., 2020). Now, in line with Lumineau et al. (2020), trust in a system based on digital technologies is increasingly relevant, especially for emerging technologies that run on the background like MPC and blockchain. In the context of MPC, trust in technology becomes relevant because it takes over the process of enforcing control for data owners. Hence, the new conceptualization of trust should be considered when studying MPC and its implications for data sharing and collaboration (see P2b in Table 6).

A surprising finding is that while MPC reduces risks perceived by data owners, specific data sharing risks remain. For instance, the risks of revealing sensitive information might shift to data users. With MPC, data users become vulnerable because their queries could reveal insights they want to obtain, allowing data owners to guess the strategic interests of data users. This implies that MPC features are like a double-edged sword that eliminates the risk for data owners while creating risks for data users. We argued that this new risk might be due to the context in which MPC is implemented. The currently known MPC use-cases mainly aim to address societal problems, such as financial fraud detection (Sangers et al., 2019) and healthcare predictions (van Egmond et al., 2021). In those use-cases, all parties agree on data usage purposes to perform computational analysis and generate insights using MPC. Hence, the risk of revealing sensitive information by data users is eliminated. However, our research context of data marketplaces differs because it involves buyer–seller relationships with unknown participants, unclear data usage purposes, and business motives. In this regard, while MPC lowers the risks for data owners, it creates new risks for data users in revealing sensitive information while sharing through data marketplaces. In other words, the risk of revealing sensitive information is more significant in this use case compared to existing MPC use cases. Therefore, we argue that the shift in data sharing risks should also be taken into account when investigating the implications of MPC in data sharing and collaboration (see P3b in Table 6).

We find that the impact of MPC on perceived control, trust, and perceived risks in data sharing depends on three conditions. The first condition is perceived benefits, which refers to how firms understand and appreciate the benefits of using MPC. In this regard, firms must be sufficiently informed on how MPC use-cases are relevant and in line with their business activities (Kanger & Pruulmann-Vengerfeldt, 2015). The importance of perceived benefits as preconditions for data sharing is consistent with existing literature (Fu et al., 2014; Sun et al., 2018). Nevertheless, our findings show that in the early stage of MPC development and adoption, the benefits of MPC in enabling data sharing while keeping the input data private seem to be not highly compelling for firms. The second condition is organizational readiness. Firms must be willing to shift towards data-driven mindsets and develop data analytics skills (Svensson & Taghavianfar, 2020). Otherwise, firms will face challenges in realizing the business value of MPC in data sharing. This is important as MPC is a complex technology and might only create value for firms that are knowledgeable and aware of its potential (Zöll et al., 2021). The final condition is perceived data sensitivity. Firms must deal with highly sensitive data before considering using MPC in data sharing. However, as we found, firms will only share generic and non-sensitive data even with MPC in place, implying that data sensitivity is a necessary but insufficient condition to use MPC.

An explanation for firms' low perception of benefits and reluctance to share highly sensitive data might be due to the nature of the automotive industry, which was chosen as our research context. This industry is known to be (1) conventional when dealing with sensitive data, (2) have low trust between actors, and (3) strongly afraid of losing a competitive edge (Svahn et al., 2017). Therefore, despite a trend toward data-driven organizations, actors in the automotive

industry still perceive data sharing as high-risk business activity. Moreover, MPC is still a relatively new technology with a lack of proven use cases in the automotive industry. As a result, actors in the automotive industry are not yet convinced of the business value of MPC. Furthermore, the added setting of data marketplaces also increases risk since it involves selling (access to) car data to other parties without knowing the purpose of data usage.

Overall, our findings imply that scholars interested in researching business-to-business data sharing should specify the concepts of control, trust, and perceived risks in a new way while considering the impact of MPC. In particular, scholars should focus on technology-based control, trust in technology, and data misuse risk, while considering perceived benefits, organizational readiness, and perceived data sensitivity as boundary conditions. This is important because MPC is a distinct phenomenon compared to existing data sharing approaches, and therefore, the current understanding of data sharing antecedents is not simply transferrable. For instance, contrary to typical research on data sharing that only focuses on data owners, we found that data users' perspectives should be considered when studying MPC. This is due to the risk of reverse engineering based on queries asked by data users. Failing to recognize and incorporate those differences would lead to a problem in understanding why and how MPC changes the way companies share data.

Conclusions

This paper shows that using MPC in business-to-business data sharing via data marketplaces can provide higher control over data through technology-based control, lower the need for trust in other actors involved, and reduce competitiveness risks. However, new types of trust and risk are emerging in the form of trust in technology and data misuse risk. To realize these impacts, firms need to understand the benefits of MPC, have sufficient organizational readiness in terms of data-related capabilities, and be aware of the sensitivity of their business data.

This paper contributes to the literature on business-to-business data sharing by being among the first that specifies the concepts of perceived control, trust, and perceived risk into a set of propositions, which holds in the initial phase of MPC before its widespread adoption. We also identify three boundary conditions to consider when studying data sharing with MPC. These contributions are crucial because, so far, we lack knowledge on the meaning of MPC for firms' data sharing decisions, especially in the early stage of MPC adoption (Agahari et al., 2021). Furthermore, MPC differs from existing data sharing approaches that primarily rely on a trusted intermediary (Bruun et al., 2020; Helminger & Rechberger, 2022). Hence, we cannot simply transfer existing knowledge to this new phenomenon (cf. Alvesson & Sandberg, 2011; Gkeredakis & Constantinides, 2019). In this way, we set a basis to extend existing theory on antecedents of business-to-business data sharing to the MPC domain. In other words, scholars could draw upon our findings to deepen our understanding of the impact of MPC in data sharing.

Additionally, this paper contributes to the MPC literature by discovering control, trust, and risk reduction in data sharing as the business value of MPC. We found that, with data-driven mindsets and capabilities, firms can create value from MPC by sharing data to generate new insights while maintaining control. In this regard, MPC can be framed differently as a tool for governing collaboration in data sharing (Lundy-Bryan, 2021) that goes beyond privacy protection (Agrawal et al., 2021). This new framing of MPC is important because firms are still not seeing privacy as a compelling value proposition despite repeated calls from scholars to implement privacy-friendly business models (e.g., Agahari et al., 2021; Bonazzi et al., 2010; Conger et al., 2013; Zöll et al., 2021). Furthermore, we expand the understanding of the socio-economic aspects of MPC beyond citizen privacy, which is overlooked in the MPC literature (Agahari et al., 2021; Agrawal et al., 2021; Bruun et al., 2020; Kanger & Pruulmann-Vengerfeldt, 2015).

Managerial implications

Our research is relevant to MPC developers and service providers to rethink the value proposition of MPC for businesses. As our findings show, MPC as a privacy tool does not seem appealing to companies because privacy is often viewed as a secondary aim. Instead, MPC should be promoted as a collaboration tool to improve companies' perception of control over data and trust and reduce risks in data sharing (Lundy-Bryan, 2021). This is important because these three factors are a basis for inter-organizational data sharing and collaboration. In this way, we offer an alternative way of framing the benefits of MPC that go beyond privacy.

Our research could also benefit intermediary platforms that facilitate data sharing. As pointed out by Abbas et al. (2021), MPC could affect the value proposition of those platforms by (1) enabling sharing and computation of data insights without disclosing the input data; and (2)

affording control over data without a trusted third party. Our study provides empirical evidence that MPC could address control, trust, and risk issues in data sharing, which are challenges that data sharing platforms struggle to deal with (M. Spiekermann, 2019). MPC could even create other values for data sharing platforms by changing how these platforms perform matchmaking based on data collaboration potential. For instance, instead of matching data users with data owners that want to sell their data, data sharing platforms could perform matchmaking between multiple parties that have the potential to collaborate in addressing collective problems such as financial fraud, traffic congestion, and energy transition. Then, platform owners could offer an end-to-end solution by implementing MPC-based privacy-enhancing analytics as a way to address those collective problems. Alternatively, data marketplaces could also completely move from the matchmaking function and fully focus on offering privacy-enhancing data analytics platforms to potential customers. Therefore, those platforms could transform their business models by implementing MPC to offer unique services for their customers and gain a competitive advantage (Agahari et al., 2021).

Limitations and future research

This research has four limitations. First, real-life and large-scale implementations of MPC are currently limited and even more lacking in the context of data marketplaces. As a result, we rely on a thought experiment on a possible scenario of MPC-enabled automotive data marketplaces rather than actual real-life implementation. In this regard, the generalizability of our findings is limited and might only be relevant in the early stage of MPC adoption. Future research could perform a follow-up study by exploring the impact of MPC on control, trust, and risks in data sharing based on a working prototype or its real-life implementation, as the perception regarding MPC might differ when it is widely adopted by businesses. Second, we used a short presentation to explain what MPC is and how it can be used for data sharing in data marketplaces. This would lead to a potential bias in the interviews since interviewees might base their understanding of MPC mostly on our explanations, which should be considered when interpreting our findings. Future research could address this limitation by involving more participants with different levels of knowledge concerning MPC to reduce bias from researchers' influence.

Third, as described in the introduction, we refer to data marketplaces as platforms for buying and selling datasets between firms, which was also explained in the short presentation. However, we observed that interviewees sometimes based their answers on (1) data-sharing platforms that purely focus on facilitating data exchange between partners; or (2) general view of data sharing without considering intermediaries like data marketplaces. This limitation is expected since interviewees are not very familiar with data marketplaces due to the diversity of data marketplaces' business models (Bergman et al., 2022; Fruhwirth et al., 2020; van de Ven et al., 2021). Therefore, we kept an eye on this issue during the interviews and clarified the concepts to the interviewees when this issue arose. In this regard, scholars could also investigate the differences in the control-, trust-, and risk-related implications of MPC within the context of data-sharing platforms that purely focus on data exchange between partners. Since this type of platform is different compared to data marketplaces for trading data (which is the focus of our study), there might be some nuanced effects for both types of platforms, which should be interesting for future research. Fourth, the findings in our study were derived in a setting with high data sharing hurdles (i.e., data marketplaces in the automotive domain). Given that the magnitude of data sharing hurdles is important in assessing the impact of MPC, different findings might emerge in settings with a lower magnitude of hurdles. Hence, we suggest scholars investigate the impact of MPC in contexts with a varying magnitude of data sharing hurdles, like sharing non-sensitive data between two known business partners for their competitive advantage.

In this study, we used an exploratory approach through semi-structured interviews as our data collection strategy. Future research could consider quantitative approaches such as surveys and experiments to test the propositions as well as the impact of MPC on those factors compared to currently known data sharing solutions such as a trusted third party. The three conditions of benefits, readiness, and data sensitivity are also relevant as implications for future research. One way is to think of them as moderating effects, which strengthen or weaken the relationship between MPC and the antecedents of data sharing decisions. For instance, in experiments, researchers should keep benefits and readiness at constant and high levels, while sensitivity should be maintained at constant and low levels. Alternatively, researchers could treat these three conditions as the boundary conditions under which the relationship between MPC and the three antecedents holds, or, rather, that MPC has certainly no effect in settings with low readiness and benefits and high sensitivity (cf., Busse et al., 2017).

Appendix

Table 7 Grounded of categories and sub-categories

Category	Sub-category	Grounded	Code	Grounded
Perceived control	The relevance of perceived control	7	Control is important	5
			Less control, more complex	2
	Contract-based control	82	Audit mechanisms	8
			Authorization	22
			Contract	13
			OEMs as data controller (based on GDPR)	2
			Payment	3
			Data sharing agreements	34
	Structural-based control	14	Closed ecosystem	1
			Decentralized/distributed architecture	7
			Direct data sharing without intermediary	6
	Technology-based control	65	API for publishing data	7
			Attribute-based security	2
			Blockchain	2
			Data aggregation	8
			Privacy-enhancing technologies	24
			Strong security measures in place	7
			MPC could increase control over data, only share insights not input data	8
			MPC could restrict what others can do with the data	3
			MPC enable sharing data while preserving confidentiality	3
			MPC gives data owners more control over what can be done with the data	1
Trust	The relevance of trust	23	Trust is important in data-centric business models	6
			Trust is not the main problem in data sharing	8
			Trust should be discussed within the specific problem at hand	3
			A trusted infra is not the major inhibitor for business collaboration in data sharing	4
			Lack of trust is a data sharing challenge	2
	Trust in actors	48	Need to rely on intermediary	2
			OEMs do not want to collaborate with competitor	2
			OEMs consider sharing data with trusted parties	3
			Lack of consumers' trust towards OEMs	1
			MPC could increase trust between providers and buyers	3
			Not too much trust and data sharing between OEMs	1
			OEMs trust each other but they are in competition	4
			OEMs trust each other more than big tech companies	1
			Trust towards the operator of data sharing system	5
			Trust towards the partner	17
			What are the intended party do with the data	4
			OEMs share data with existing partners	4
			Sharing data with business partners within a group	1
	Trust in technology	4	Lack of technology trust	2
			MPC algorithm must be trustworthy	1
			MPC could influence trust in the system	1

Table 7 (continued)

Category	Sub-category	Grounded	Code	Grounded
Perceived risks	Competitiveness risk	89	data as a source of competitive advantage	13
			OEMs are very protective and selective about data sharing	3
			Confidentiality	6
			Intellectual property	4
			Fear of losing competitive advantage	27
			Knowledge spillover	17
			Competitiveness between OEMs	10
			Highly competitive data	4
			MPC could reduce knowledge spillover risk	2
			MPC enable data sharing in aggregated format	1
			MPC reduced data sharing risk	2
	Data misuse risk	18	Fear of data abuse by other parties	14
			Safety risk/afraid of car hacks	2
			With MPC, data users could give away their know-how to data owners	2
	End-users privacy risk	26	Risk of harming privacy of end-users	12
			German OEMs are very protective of customers' data	4
			Risk due to uncertainty about privacy questions	2
			Need to protect customer's interest in protecting data	4
			Data privacy	1
			The raw data are privacy-sensitive	3
	Reputation risk	12	Fear of damaging company's image and brand	8
			Risk of making bad decisions on data sharing	4

Table 7 (continued)

Category	Sub-category	Grounded	Code	Grounded
Conditions	Perceived benefits	166	Lack of clear business models for data sharing	5
			Data sharing is based on a value proposition for customers and business partners	20
			Data sharing is based on the use case	42
			Need to have something in return (benefit)	37
			MPC is not relevant for risk, only look at business as opportunities	1
			MPC is not viable yet	4
			MPC is still complete speculation at this point	3
			MPC is useful depending on the use case	10
			MPC needs to be able to perform complex calculations	2
			Benefit of using MPC is unclear	2
			Need to understand if MPC change business model and data sharing landscape	7
			Need to understand MPC in more detail	7
			Need to understand the mechanics of MPC in business ecosystems	8
			Need to understand the viability of MPC	3
			OEMs will use MPC if benefits are clear	1
			There can be a mismatch between data granularity needed and the 'insights' generated	1
			What kind of questions can MPC answer with aggregated statistics?	1
			Benefit/advantage of data sharing is unclear	11
			Value should come first, then the enabling technologies	1
	Organizational readiness	14	How to gather/collect the data	2
			How to make data usable	1
			Managerial maturity	2
			MPC increase responsibility of data owners to prepare data in the right way	4
			MPC puts back some burden of providing data to OEMs	2
			With MPC, data users still needs to do data cleaning	2
			With MPC, data standardization is required	1
	Perceived data sensitivity	29	data sharing depends on data type	8
			MPC is useful only to share non-core, non-sensitive, non-strategic data	2
			MPC would not change willingness to share strategically relevant data	1
			OEMs will only share some relevant information	1
			OEMs only willing to share generic, non-sensitive data	5
			OEMs only willing to share data that are normally open	2
			OEMs are unwilling to share business-sensitive data	10

Acknowledgements The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 825225–Safe Data-Enabled Economic Development (Safe-DEED). The work by the second author was supported by funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 871481–Trusted Secure Data Sharing Space (TRUSTS).

References

Abbas, A. E., Agahari, W., van de Ven, M., Zuiderwijk, A., & de Reuver, M. (2021). Business data sharing through data marketplaces: A systematic literature review. *Journal of Theoretical and Applied Electronic Commerce Research, 16*(7), 3321–3339. https://doi.org/10.3390/jtaer16070180

Agahari, W., Dolci, R., & de Reuver, M. (2021). Business model implications of privacy-preserving technologies in data marketplaces: The case of multi-party computation. *ECIS 2021 Research Papers, 59*. https://aisel.aisnet.org/ecis2021_rp/59

Agrawal, N., Binns, R., Van Kleek, M., Laine, K., & Shadbolt, N. (2021). Exploring design and governance challenges in the development of privacy-preserving computation. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3411764.3445677

Alter, G., Falk, B. H., Lu, S., & Ostrovsky, R. (2018). Computing statistics from private data. *Data Science Journal, 17*, 31. https://doi.org/10.5334/dsj-2018-031

Alvesson, M., & Sandberg, J. (2011). Generating research questions through problematization. *Academy of Management Review, 36*(2), 247–271. https://doi.org/10.5465/amr.2009.0188

Apfelbeck, F. (2018). *Evaluation of privacy-preserving technologies for machine learning*. Outlier Ventures. https://outlierventures.io/research/evaluation-of-privacy-preserving-technologies-for-machine-learning/

Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., Smart, N. P., & Wright, R. N. (2018). From keys to databases—real-world applications of secure multi-party computation. *The Computer Journal, 61*(12), 1749–1771. https://doi.org/10.1093/comjnl/bxy090

Arnaut, C., Pont, M., Scaria, E., Berghmans, A., & Leconte, S. (2018). Study on data sharing between companies in Europe. *A Study Prepared for the European Commission Directorate-General for Communications Networks, Content and Technology by Everis Benelux*, *24*. https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en

Asare, A. K., Brashear-Alejandro, T. G., & Kang, J. (2016). B2B technology adoption in customer driven supply chains. *Journal of Business & Industrial Marketing, 31*(1), 1–12. https://doi.org/10.1108/JBIM-02-2015-0022

Athanasopoulou, A., de Reuver, M., Nikou, S., & Bouwman, H. (2019). What technology enabled services impact business models in the automotive industry? An exploratory study. *Futures, 109*, 73–83. https://doi.org/10.1016/j.futures.2019.04.001

Azarm-Daigle, M., Kuziemsky, C., & Peyton, L. (2015). A review of cross organizational healthcare data sharing. *Procedia Computer Science, 63*, 425–432. https://doi.org/10.1016/j.procs.2015.08.363

Bachmann, R. (2001). Trust, power and control in trans-organizational relations. *Organization Studies, 22*(2), 337–365. https://doi.org/10.1177/0170840601222007

Balson, D., & Dixon, W. (2020). *Cyber Information Sharing: Building Collective Security*. World Economic Forum. https://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf

Bergman, R., Abbas, A. E., Jung, S., Werker, C., & de Reuver, M. (2022). Business model archetypes for data marketplaces in the automotive industry. *Electronic Markets, 32*(2). https://doi.org/10.1007/s12525-022-00547-x

Bestavros, A., Lapets, A., & Varia, M. (2017). User-centric distributed solutions for privacy-preserving analytics. *Communications of the ACM, 60*(2), 37–39. https://doi.org/10.1145/3029603

Bogdanov, D., Jõemets, M., Siim, S., & Vaht, M. (2015). How the estonian tax and customs board evaluated a tax fraud detection system based on secure multi-party computation. In R. Böhme & T. Okamoto (Eds.), *Financial Cryptography and Data Security* (pp. 227–234). Springer. https://doi.org/10.1007/978-3-662-47854-7_14

Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J. D., Nielsen, J. B., Nielsen, K., Pagter, J., Schwartzbach, M., & Toft, T. (2009). Secure multiparty computation goes live. In R. Dingledine & P. Golle (Eds.), *Financial Cryptography and Data Security* (pp. 325–343). Springer. https://doi.org/10.1007/978-3-642-03549-4_20

Bonazzi, R., Fritscher, B., & Pigneur, Y. (2010). Business model considerations for privacy protection in a mobile location based context. *2010 14th International Conference on Intelligence in Next Generation Networks*, 1–8. https://doi.org/10.1109/ICIN.2010.5640885

Bons, R., Lee, R. M., & Wagenaar, R. W. (1998). Designing trustworthy interorganizational trade procedures for open electronic commerce. *International Journal of Electronic Commerce, 2*(3), 61–83. https://doi.org/10.1080/10864415.1998.11518316

Bons, R., Dignum, F., Lee, R. M., & Tan, Y.-H. (2000). A formal analysis of auditing principles for electronic trade procedures. *International Journal of Electronic Commerce, 5*(1), 57–82. https://doi.org/10.1080/10864415.2000.11044200

Bons, R., Lee, R. M., & Nguyen, V. H. (2012). Generating procedural controls to facilitate trade: The role of control in the absence of trust. *BLED 2012 – Special Issue*, *10*, 198–225. https://aisel.aisnet.org/bled2012_special_issue/10

Bruun, M. H., Andersen, A. O., & Mannov, A. (2020). Infrastructures of trust and distrust: The politics and ethics of emerging cryptographic technologies. *Anthropology Today, 36*(2), 13–17. https://doi.org/10.1111/1467-8322.12562

Bryant, A., & Charmaz, K. (2007). The SAGE handbook of grounded theory. *SAGE Publications Ltd*. https://doi.org/10.4135/9781848607941

Busse, C., Kach, A. P., & Wagner, S. M. (2017). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods, 20*(4), 574–609. https://doi.org/10.1177/1094428116641191

Chen, Y.-H., Lin, T.-P., & Yen, D. C. (2014). How to facilitate inter-organizational knowledge sharing: The impact of trust. *Information & Management, 51*(5), 568–578. https://doi.org/10.1016/j.im.2014.03.007

Choi, J. I., & Butler, K. R. B. (2019). Secure multiparty computation and trusted hardware: Examining adoption challenges and opportunities. *Security and Communication Networks, 2019*, 1368905. https://doi.org/10.1155/2019/1368905

European Commission. (2020). *A European strategy for data*. https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal, 23*(5), 401–417. https://doi.org/10.1111/j.1365-2575.2012.00402.x

Constant, D., Kiesler, S., & Sproull, L. (1994). What's mine is ours, or is it? A study of attitudes about information sharing. *Information Systems Research, 5*(4), 400–421. https://doi.org/10.1287/isre.5.4.400

Cropanzano, R., & Mitchell, M. S. (2005). Social exchange theory: An interdisciplinary review. *Journal of Management, 31*(6), 874–900. https://doi.org/10.1177/0149206305279602

Dahlberg, T., & Nokkala, T. (2019). *Willingness to share supply chain data in an ecosystem governed platform–An interview study*.

di Vimercati, S. D. C., Foresti, S., Livraga, G., & Samarati, P. (2021). Toward owners' control in digital data markets. *IEEE Systems Journal, 15*(1), 1299–1306. https://doi.org/10.1109/JSYST.2020.2970456

Docherty, I., Marsden, G., & Anable, J. (2018). The governance of smart mobility. *Transportation Research Part a: Policy and Practice, 115*, 114–125.

Du, T. C., Lai, V. S., Cheung, W., & Cui, X. (2012). Willingness to share information in a supply chain: A partnership-data-process perspective. *Information & Management, 49*(2), 89–98. https://doi.org/10.1016/j.im.2011.10.003

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, *9*(3–4), 211–407. https://doi.org/10.1561/0400000042

Dwork, C. (2006). Differential privacy. In M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Eds.), *Automata, Languages and Programming* (pp. 1–12). Springer. https://doi.org/10.1007/11787006_1

Emerson, R. M. (1976). Social exchange theory. *Annual Review of Sociology, 2*(1), 335–362. https://doi.org/10.1146/annurev.so.02.080176.002003

Emsley, D., & Kidon, F. (2007). The relationship between trust and control in international joint ventures: Evidence from the airline industry*. *Contemporary Accounting Research, 24*(3), 829–858. https://doi.org/10.1506/car.24.3.7

Eurich, M., Oertel, N., & Boutellier, R. (2010). The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain. *Electronic Commerce Research, 10*(3), 423–440. https://doi.org/10.1007/s10660-010-9062-0

Fruhwirth, M., Rachinger, M., & Prlja, E. (2020). Discovering business models of data marketplaces. *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Fu, H.-P., Chang, T.-H., Ku, C.-Y., Chang, T.-S., & Huang, C.-H. (2014). The critical success factors affecting the adoption of inter-organization systems by SMEs. *Journal of Business & Industrial Marketing, 29*(5), 400–416. https://doi.org/10.1108/JBIM-04-2012-0070

Garrido, G. M., Sedlmeir, J., Uludağ, Ö., Alaoui, I. S., Luckow, A., & Matthes, F. (2021). Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. *ArXiv:2107.11905 [Cs]*. http://arxiv.org/abs/2107.11905

Gartner. (2021). *Gartner says digital ethics is at the peak of inflated expectations in the 2021 gartner hype cycle for privacy*. https://www.gartner.com/en/newsroom/press-releases/2021-09-30-gartner-says-digital-ethics-is-at-the-peak-of-inflate

Gast, J., Gundolf, K., Harms, R., & Matos Collado, E. (2019). Knowledge management and coopetition: How do cooperating competitors balance the needs to share and protect their knowledge? *Industrial Marketing Management, 77*, 65–74. https://doi.org/10.1016/j.indmarman.2018.12.007

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, 169–178*,. https://doi.org/10.1145/1536414.1536440

Gkeredakis, M., & Constantinides, P. (2019). Phenomenon-based problematization: Coordinating in the digital era. *Information and Organization, 29*(3), 100254.

Goldbach, T., Benlian, A., & Buxmann, P. (2018). Differential effects of formal and self-control in mobile platform ecosystems: Multimethod findings on third-party developers' continuance intentions and application quality. *Information & Management, 55*(3), 271–284. https://doi.org/10.1016/j.im.2017.07.003

Günther, W. A., Mehrizi, M. H. R., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. *The Journal of Strategic Information Systems, 26*(3), 191–209.

Hall, H., & Widén-Wulff, G. (2008). Social exchange, social capital and information sharing in online environments: Lessons from three case studies. In M.-L. Huotari & D. Elisabeth (Eds.), *From Information Provision to Knowledge Production* (p. 21). University of Oulu.

Harris, D., Khan, L., Paul, R., & Thuraisingham, B. (2007). Standards for secure data sharing across organizations. *Computer Standards & Interfaces, 29*(1), 86–96. https://doi.org/10.1016/j.csi.2006.01.004

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). Capturing value from big data – a taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management, 36*(10), 1382–1406. https://doi.org/10.1108/IJOPM-02-2014-0098

Hastings, M., Hemenway, B., Noble, D., & Zdancewic, S. (2019). SoK: General purpose compilers for secure multi-party computation. *IEEE Symposium on Security and Privacy (SP), 2019*, 1220–1237. https://doi.org/10.1109/SP.2019.00028

Helminger, L., & Rechberger, C. (2022). Multi-party computation in the GDPR. *Privacy Symposium 2022-Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)*.

Hemenway, B., Lu, S., Ostrovsky, R., & Welser IV, W. (2016). High-precision secure computation of satellite collision probabilities. In V. Zikas & R. De Prisco (Eds.), *Security and Cryptography for Networks* (pp. 169–187). Springer International Publishing. https://doi.org/10.1007/978-3-319-44618-9_9

Jernigan, S., Kiron, D., & Ransbotham, S. (2016). Data sharing and analytics are driving success with IoT. *MIT Sloan Management Review*, *58*(1).

Johnson, M. E. (2009). Managing information risk and the economics of security. In *Managing Information Risk and the Economics of Security* (pp. 1–16). Springer. https://doi.org/10.1007/978-0-387-09762-6_1

Kagal, L., Finin, T., & Joshi, A. (2001). Trust-based security in pervasive computing environments. *Computer, 34*(12), 154–157. https://doi.org/10.1109/2.970591

Kaiser, C., Stocker, A., Viscusi, G., Fellmann, M., & Richter, A. (2021). Conceptualising value creation in data-driven services: The case of vehicle data. *International Journal of Information Management, 59*, 102335. https://doi.org/10.1016/j.ijinfomgt.2021.102335

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing, 72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Kanger, L., & Pruulmann-Vengerfeldt, P. (2015). Social need for secure multiparty computation. *Applications of Secure Multiparty Computation, 43–57*,. https://doi.org/10.3233/978-1-61499-532-6-43

Kembro, J., Näslund, D., & Olhager, J. (2017). Information sharing across multiple supply chain tiers: A Delphi study on antecedents. *International Journal of Production Economics, 193*, 77–86. https://doi.org/10.1016/j.ijpe.2017.06.032

Kerber, W. (2018). Data governance in connected cars: The problem of access to in-vehicle data. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 9*, 310.

Klein, T., & Verhulst, S. (2017). *Access to new data sources for statistics: Business models and incentives for the corporate sector* (SSRN Scholarly Paper ID 3141446). Social Science Research Network. https://doi.org/10.2139/ssrn.3141446

Koch, K., Krenn, S., Pellegrino, D., & Ramacher, S. (2021). Privacy-preserving analytics for data markets using MPC. In M. Friedewald, S. Schiffner, & S. Krenn (Eds.), *Privacy and Identity Management* (pp. 226–246). Springer International Publishing. https://doi.org/10.1007/978-3-030-72465-8_13

Kolekofski, K. E., & Heminger, A. R. (2003). Beliefs and attitudes affecting intentions to share information in an organizational setting. *Information & Management, 40*(6), 521–532. https://doi.org/10.1016/S0378-7206(02)00068-X

Koutroumpis, P., Leiponen, A., & Thomas, L. D. (2020). Markets for data. *Industrial and Corporate Change, 29*(3), 645–660.

Lapets, A., Jansen, F., Albab, K. D., Issa, R., Qin, L., Varia, M., & Bestavros, A. (2018). Accessible privacy-preserving web-based data analysis for assessing and addressing economic inequalities. *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, 1–5. https://doi.org/10.1145/3209811.3212701

Lee, R. M. (Eds). (1998). Distributed electronic trade scenarios: Representation design prototyping. *International Journal of Electronic Commerce*, *3*(2), 105–136. https://doi.org/10.1080/10864415.1998.11518336

Li, J., Sikora, R., Shaw, M. J., & Tan, G. W. (2006). A strategic analysis of inter organizational information sharing. *Decision Support Systems, 42*(1), 251–266. https://doi.org/10.1016/j.dss.2004.12.003

Li, H., Chen, Q., Zhu, H., Ma, D., Wen, H., & Shen, X. S. (2020). Privacy leakage via de-anonymization and aggregation in heterogeneous social networks. *IEEE Transactions on Dependable and Secure Computing, 17*(2), 350–362. https://doi.org/10.1109/TDSC.2017.2754249

Lumineau, F., Schilke, O., & Wang, W. (2020). *Organizational trust in the age of the fourth industrial revolution: Shifts in the nature, production, and targets of trust*. https://doi.org/10.13140/RG.2.2.20789.50401

Lundy-Bryan, L. (2021). *Privacy enhancing technologies: Part 2- The coming age of collaborative computing* (Lunar Insight Series). Lunar Ventures.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing, 58*(3), 20–38. https://doi.org/10.1177/002224299405800302

Mosterd, L., Sobota, V. C. M., van de Kaa, G., Ding, A. Y., & de Reuver, M. (2021). Context dependent trade-offs around platform-to-platform openness: The case of the Internet of Things. *Technovation, 108*, 102331. https://doi.org/10.1016/j.technovation.2021.102331

Mukhopadhyay, S., de Reuver, M., & Bouwman, H. (2016). Effectiveness of control mechanisms in mobile platform ecosystem. *Telematics and Informatics, 33*(3), 848–859. https://doi.org/10.1016/j.tele.2015.12.008

Müller, J. M., Veile, J. W., & Voigt, K.-I. (2020). Prerequisites and incentives for digital information sharing in Industry 4.0 – An international comparison across data types. *Computers & Industrial Engineering, 148*, 106733. https://doi.org/10.1016/j.cie.2020.106733

Naehrig, M., Lauter, K., & Vaikuntanathan, V. (2011). Can homomorphic encryption be practical? *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, 113–124. https://doi.org/10.1145/2046660.2046682

Nicolaou, A. I., & McKnight, D. H. (2006). Perceived information quality in data exchanges: Effects on risk, trust, and intention to use. *Information Systems Research, 17*(4), 332–351. https://doi.org/10.1287/isre.1060.0103

Nokkala, T., Salmela, H., & Toivonen, J. (2019). Data governance in digital platforms. *AMCIS 2019 Proceedings*. https://aisel.aisnet.org/amcis2019/ebusiness/ebusiness/12

Noorian, Z., Iyilade, J., Mohkami, M., & Vassileva, J. (2014). Trust mechanism for enforcing compliance to secondary data use contracts. *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, 519–526. https://doi.org/10.1109/TrustCom.2014.66

Opriel, S., Fraunhofer, I., Skubowius, G. E., Fraunhofer, I. M. L., & Lamberjohann, M. (2021). How usage control fosters willingness to share sensitive data in inter-organizational processes of supply chains. *International Scientific Symposium on Logistics*, 91.

Otto, B., Steinbuß, S., Teuscher, A., & Lohmann, S. (2019). *Reference architecture model—International data spaces (Version 3.0)*. International Data Spaces Association. https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37–59. https://doi.org/10.1287/isre.1040.0015

Penttinen, E., Halme, M., Lyytinen, K., & Myllynen, N. (2018). What influences choice of business-to-business connectivity platforms? *International Journal of Electronic Commerce, 22*(4), 479–509. https://doi.org/10.1080/10864415.2018.1485083

Pettai, M., & Laud, P. (2015). Combining differential privacy and secure multiparty computation. *Proceedings of the 31st Annual Computer Security Applications Conference*, pp. 421–430. https://doi.org/10.1145/2818000.2818027

Priego, L. P., Osimo, D., & Wareham, J. D. (2019). Data sharing practice in big data ecosystems. *SSRN Electronic Journal*.

Ratnasingam, P., Pavlou, P. A., & Tan, Y.-H. (2002). *The importance of technology trust for B2B electronic commerce* (SSRN Scholarly Paper ID 2380727). Social Science Research Network. https://papers.ssrn.com/abstract=2380727

Recker, J. (2013). *Scientific research in information systems: A beginner's guide*. Springer.

Reimsbach-Kounatze, C. (2021). *Enhancing access to and sharing of data: Striking the balance between openness and control over data*. 25–68. https://doi.org/10.5771/9783748924999-25

Richter, H., & Slowinski, P. R. (2019). The data sharing economy: On the emergence of new intermediaries. *IIC-International Review of Intellectual Property and Competition Law, 50*(1), 4–29. https://doi.org/10.1007/s40319-018-00777-7

Roman, D., & Vu, K. (2019). Enabling data markets using smart contracts and multi-party computation. In W. Abramowicz & A. Paschke (Eds.), *Business Information Systems Workshops* (pp.

258–263). Springer International Publishing. https://doi.org/10.1007/978-3-030-04849-5_23

Roseman Labs. (2022). *Easier, safer and more collaboration on healthcare data*. Roseman Labs. https://rosemanlabs.com/blog/zorg_whitepaper.html

Samaddar, S., Nargundkar, S., & Daley, M. (2006). Inter-organizational information sharing: The role of supply network configuration and partner goal congruence. *European Journal of Operational Research, 174*(2), 744–765. https://doi.org/10.1016/j.ejor.2005.01.059

Sangers, A., van Heesch, M., Attema, T., Veugen, T., Wiggerman, M., Veldsink, J., Bloemen, O., & Worm, D. (2019). Secure multiparty pagerank algorithm for collaborative fraud detection. In I. Goldberg & T. Moore (Eds.), *Financial Cryptography and Data Security* (pp. 605–623). Springer International Publishing. https://doi.org/10.1007/978-3-030-32101-7_35

Saprikis, V., & Vlachopoulou, M. (2012). Determinants of suppliers' level of use of B2B e-marketplaces. *Industrial Management & Data Systems, 112*(4), 619–643. https://doi.org/10.1108/02635571211225512

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.

Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*(11), 612–613. https://doi.org/10.1145/359168.359176

Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2019). Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. *IEEE Transactions on Information Forensics and Security, 14*(2), 331–346. https://doi.org/10.1109/TIFS.2018.2850312

Son, J.-Y., Tu, L., & Benbasat, I. (2006). A descriptive content analysis of trust-building measures in B2B electronic marketplaces. *Communications of the Association for Information Systems*, *18*. https://doi.org/10.17705/1CAIS.01806

Spiekermann, M. (2019). Data marketplaces: Trends and monetisation of data goods. *Intereconomics, 54*(4), 208–216. https://doi.org/10.1007/s10272-019-0826-z

Spiekermann, S. (2005). *Perceived control: Scales for privacy in ubiquitous computing* (SSRN Scholarly Paper ID 761109). Social Science Research Network. https://doi.org/10.2139/ssrn.761109

Stefansson, G. (2002). Business-to-business data sharing: A source for integration of supply chains. *International Journal of Production Economics, 75*(1), 135–146. https://doi.org/10.1016/S0925-5273(01)00187-6

Subramanian, H. (2017). Decentralized blockchain-based electronic marketplaces. *Communications of the ACM, 61*(1), 78–84. https://doi.org/10.1145/3158333

Sun, S., Cegielski, C. G., Jia, L., & Hall, D. J. (2018). Understanding the factors affecting the organizational adoption of big data. *Journal of Computer Information Systems, 58*(3), 193–203. https://doi.org/10.1080/08874417.2016.1222891

Svahn, F., Mathiassen, L., & Lindgren, R. (2017). Embracing digital innovation in incumbent firms: How volvo cars managed competing concerns. *MIS Quarterly, 41*(1), 239–253. https://doi.org/10.25300/MISQ/2017/41.1.12

Svensson, R. B., & Taghavianfar, M. (2020). Toward becoming a data-driven organization: Challenges and benefits. In F. Dalpiaz, J. Zdravkovic, & P. Loucopoulos (Eds.), *Research Challenges in Information Science* (pp. 3–19). Springer International Publishing. https://doi.org/10.1007/978-3-030-50316-1_1

Tiwana, A. (2014). *Platform ecosystems: Aligning architecture, governance, and strategy*. Elsevier.

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research commentary—platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research, 21*(4), 675–687. https://doi.org/10.1287/isre.1100.0323

van den Broek, T., & van Veenstra, A. F. (2018). Governance of big data collaborations: How to balance regulatory compliance and disruptive innovation. *Technological Forecasting and Social Change, 129*, 330–338. https://doi.org/10.1016/j.techfore.2017.09.040

van Egmond, M. B., Spini, G., van der Galien, O., IJpma, A., Veugen, T., Kraaij, W., Sangers, A., Rooijakkers, T., Langenkamp, P., Kamphorst, B., van de L'Isle, N., & Kooij-Janic, M. (2021). Privacy-preserving dataset combination and Lasso regression for healthcare predictions. *BMC Medical Informatics and Decision Making, 21*(1), 266. https://doi.org/10.1186/s12911-021-01582-y

van de Ven, M., Abbas, A. E., Kwee, Z., & de Reuver, M. (2021). Creating a taxonomy of business models for data marketplaces. *34th Bled EConference: Digital Support from Crisis to Progressive Change*, 313–325.

Verschuren, P., & Doorewaard, H. (2010). *Designing a research project* (Vol. 2). Eleven International Publishing.

Virkar, S., Viale Pereira, G., & Vignoli, M. (2019). Investigating the social, political, economic and cultural implications of data trading. In I. Lindgren, M. Janssen, H. Lee, A. Polini, M. P. Rodríguez Bolívar, H. J. Scholl, & E. Tambouris (Eds.), *Electronic Government* (pp. 215–229). Springer International Publishing. https://doi.org/10.1007/978-3-030-27325-5_17

White, A., Daniel, E., Ward, J., & Wilson, H. (2007). The adoption of consortium B2B e-marketplaces: An exploratory study. *The Journal of Strategic Information Systems, 16*(1), 71–103. https://doi.org/10.1016/j.jsis.2007.01.004

Wiener, M., Mahring, M., Remus, U., & Saunders, C. (2016). Control configuration and control enactment in information systems projects: Review and expanded theoretical framework. *Management Information Systems Quarterly, 40*(3), 741–774.

Yao, A. C. (1982). Protocols for secure computations. *23rd Annual Symposium on Foundations of Computer Science (Sfcs 1982)*, 160–164. https://doi.org/10.1109/SFCS.1982.38

Yao, A. C. (1986). How to generate and exchange secrets. *27th Annual Symposium on Foundations of Computer Science (Sfcs 1986)*, 162–167. https://doi.org/10.1109/SFCS.1986.25

Zaheer, N., & Trkman, P. (2017). An information sharing theory perspective on willingness to share information in supply chains. *The International Journal of Logistics Management, 28*(2), 417–443. https://doi.org/10.1108/IJLM-09-2015-0158

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & Tan, Y. (2019). Secure multi-party computation: Theory, practice and applications. *Information Sciences, 476*, 357–372. https://doi.org/10.1016/j.ins.2018.10.024

Zhong, H., Sang, Y., Zhang, Y., & Xi, Z. (2020). Secure multi-party computation on blockchain: An overview. In H. Shen & Y. Sang (Eds.), *Parallel Architectures, Algorithms and Programming* (pp. 452–460). Springer. https://doi.org/10.1007/978-981-15-2767-8_40

Zöll, A., Olt, C., & Buxmann, P. (2021). Privacy-sensitive business models: Barriers of organizational adoption of privacy-enhancing technologies. *ECIS 2021 Research Papers*. https://aisel.aisnet.org/ecis2021_rp/34

Zrenner, J., Möller, F. O., Jung, C., Eitel, A., & Otto, B. (2019). Usage control architecture options for data sovereignty in business ecosystems. *Journal of Enterprise Information Management, 32*(3), 477–495. https://doi.org/10.1108/JEIM-03-2018-0058