Business model implications of privacy-preserving technologies in data marketplaces
The case of multi-party computation

Agahari, W.; Dolci, R.; de Reuver, G.A.

Publication date
2021

Document Version
Final published version

Published in
29th European Conference on Information Systems (ECIS 2021)

6-14-2021

Business model implications of privacy-preserving technologies in data marketplaces: The case of multi-party computation

Wirawan Agahari
Delft University of Technology, w.agahari@tudelft.nl

Riccardo Dolci
Delft University of Technology, riccardo.dolci3@gmail.com

Mark de Reuver
Delft University of Technology, g.a.dereuver@tudelft.nl

BUSINESS MODEL IMPLICATIONS OF PRIVACY-PRESERVING TECHNOLOGIES IN DATA MARKETPLACES: THE CASE OF MULTI-PARTY COMPUTATION

Research Paper

Wirawan Agahari, Delft University of Technology, Delft, the Netherlands, w.agahari@tudelft.nl

Riccardo Dolci, Delft University of Technology, Delft, the Netherlands, r.dolci@student.tudelft.nl

Mark de Reuver, Delft University of Technology, Delft, the Netherlands, g.a.dereuver@tudelft.nl

Abstract

Privacy-preserving technologies could allow data marketplaces to deliver technical assurances to companies on data privacy and control. However, how such technologies change the business model of data marketplaces is not fully understood. This paper aims to bridge this gap by focusing on multi-party computation (MPC) as a cryptographic technology that is currently being hyped. Based on interviews with privacy and security experts, we find that MPC enables data marketplaces to employ a "privacy-as-a-service" business model, which goes beyond privacy-preserving data exchange. Depending on the architecture, MPC could transform data marketplaces into data brokers or data aggregators. More complex architectures might lead to more robust security guarantees and lower trust requirements towards data marketplace operators. Furthermore, MPC enables new offerings of privacy-preserving analytics and services as new revenue sources. Our findings contribute to developing business models of privacy-preserving data marketplaces to unlock the potential of data sharing in a digitized economy.

Keywords: data marketplaces, multi-party computation, privacy-as-a-service, business model

1 Introduction

Data marketplaces are an important enabler for the data economy (Stahl, Schomm and Vossen, 2014). By facilitating business-to-business data sharing, data marketplaces empower companies to generate meaningful insights and stimulate innovation (van den Broek and van Veenstra, 2018; Virkar, Viale Pereira and Vignoli, 2019; Koutroumpis, Leiponen and Thomas, 2020). Data marketplaces enable reusing data, which is essential as most firms only utilize 10% of their own data (Manyika, 2015). However, most studies on data marketplaces are limited to pricing mechanisms (e.g., Muschalle, Stahl, Löser and Vossen, 2013; Fricker and Maksimov, 2017) and architectural design (Mišura and Žagar, 2016; Brandão, Mamede and Gonçalves, 2019). As a result, we know little about the business models of data marketplaces (Spiekermann, 2019; Fruhwirth, Rachinger and Prlja, 2020) or why they struggle to incentivize data sharing (Koutroumpis et al., 2020).

Multi-party computation (MPC) can potentially address barriers in data sharing via data marketplaces, such as privacy concerns (Khurana, Mishra and Singh, 2011; Sayogo et al., 2014) and fear of losing

control over sensitive data (Jarman, Luna-Reyes and Zhang, 2016; Klein and Verhulst, 2017). MPC is a class of privacy-preserving technologies (PPT) that allows multiple parties to jointly analyze data and generate meaningful insights without disclosing the input data (Choi and Butler, 2019; Zhao et al., 2019). In this way, MPC can balance the tension between sharing data to create value and protecting data as a competitive advantage (cf., Gast, Gundolf, Harms and Matos Collado, 2019). While the theoretical concept of MPC is not novel (Yao, 1982), recent advances in computational power and efficiency are bringing MPC increasingly closer to real-life applications.

We expect that MPC enables new architectural approaches for data marketplaces and changes the value proposition for actors in the ecosystem. Nevertheless, how MPC will change the business model of data marketplaces is unexplored. On the one hand, the few business model studies on data marketplaces do not consider privacy-preserving technologies or MPC (Spiekermann, 2019; Fruhwirth et al., 2020). On the other hand, most discussion on MPC focuses on technical aspects rather than business implications (e.g., Volgushev et al., 2019; Guo, Katz, Wang and Yu, 2020). While scholars are beginning to realize that MPC can create public value and solve societal problems (e.g., Bestavros, Lapets and Varia, 2017; Lapets et al., 2018), only a few studies consider how the technology can be used in data marketplaces (e.g., Roman and Vu, 2019; Koch, Krenn, Pellegrino and Ramacher, 2021).

This paper aims to examine how MPC, as one class of privacy-preserving technologies, can change the business model of data marketplaces. To conceptualize the business model construct, we use the framework by Al-Debei and Avison (2010). Specifically, we explore how MPC (1) creates new value propositions for actors within the data marketplace ecosystems; (2) changes the value architecture of data marketplaces; and (3) enables new ways for data marketplaces to capture value (i.e., value finance). To fulfill this objective, we conducted exploratory interviews with MPC experts and practitioners to gather a rich array of perspectives. We focused on commercial business-to-business (B2B) data sharing via data marketplaces and not about data sharing by individuals/consumers. We also focused on exploring the potential of MPC in data marketplaces and not arguing that MPC is the most appropriate solution, as there are several alternatives such as homomorphic encryption and differential privacy.

Our research contributes to understanding the emerging phenomena of data marketplaces and privacy-preserving technologies, particularly MPC. To our knowledge, our research is the first to connect MPC with business model concepts in a setting of data marketplaces. Such understanding is crucial because MPC is starting to gain attention and could be the key in the data economy. However, we primarily know about its technical aspect, while we also need business and societal insights to get the best out of it. Without such understanding, we might miss out on an opportunity in fulfilling the promise of the data economy (Zafrir, 2020).

We organize this paper as follows. Section 2 provides a background on data marketplaces, MPC and related privacy-preserving technologies, and business models. Next, section 3 presents our sampling strategy, data collection, and analysis approach. Then, we outline our findings in section 4 (value proposition), section 5 (value architecture), and section 6 (value finance). Finally, we conclude this paper by discussing key findings, implications, limitations, and future research in section 7.

2 Background and related work

2.1 Business model

The business model construct was first introduced in Information Systems (IS) literature during the advent of the Internet (Alt and Zimmermann, 2001). Currently, business models are commonly used to understand the impact of digital technologies (e.g., Athanasopoulou, de Reuver, Nikou and Bouwman, 2019; Bouwman, Nikou and de Reuver, 2019). We use the business model construct to understand the link between digital technology on the one hand and value creation on the other (cf., Chesbrough and Rosenbloom, 2002; Baden-Fuller and Haefliger, 2013). Digital technologies can be a driver as well as

an enabler for new business models (Bouwman, de Vos and Haaker, 2008; de Reuver, Bouwman and MacInnes, 2009).

We see a business model as a description of how firms create, deliver, and capture value (Osterwalder and Pigneur, 2010; Teece, 2010). For this research, we build upon the Unified Business Model Framework by Al-Debei and Avison (2010) as our analytical lens for two reasons. First, this framework is structured based on existing business model frameworks, making it comprehensive and sufficiently broad to capture relevant business model aspects. Second, other studies have been implementing this framework to analyze business models of data intermediaries (e.g., Janssen and Zuiderwijk, 2014; Ranerup, Henriksen and Hedman, 2016; Susha, Flipsen, Agahari and de Reuver, 2020), of which data marketplaces are an instance.

The framework comprises four elements: *value proposition* (i.e., business logic for value creation by providing products and services for targeted segments), *value architecture* (i.e., technological and organizational architecture to provide products and services), *value network* (i.e., actors involved in creating value), and *value finance* (i.e., issues related to pricing and revenue models). Our focus in this research is to analyze value propositions, value architecture, and value finance of MPC for the three main actors in the value network of data marketplaces: data providers, data buyers, and data marketplace operators.

2.2 Data marketplaces

Data marketplaces are digital platforms managed by **data marketplace operators** that facilitate data sharing and trading between companies (Richter and Slowinski, 2019; Spiekermann, 2019; Koutroumpis et al., 2020). For clarity, we follow Spiekermann (2019) in describing two main actors in data marketplace ecosystems, namely **data providers** (i.e., companies that offer their data for free or for a fee) and **data buyers** (i.e., companies that want to acquire new data). Access to data, manipulation, and data use by data buyers is commonly governed by various standardized or negotiated licensing models (Schomm, Stahl and Vossen, 2013; Stahl, Schomm, Vossen and Vomfell, 2016). Both static and dynamic data streams can be shared and traded in data marketplaces through file downloads, Application Programming Interfaces (APIs), or customized web interfaces (Fricker and Maksimov, 2017; Spiekermann, 2019). On top of that, data marketplaces offer complementary applications and services such as data visualizations, data valuation, and data analytics (Schreieck, Hein, Wiesche and Krcmar, 2018; van den Broek and van Veenstra, 2018; Spiekermann, 2019). Hence, data marketplaces create value by lowering transaction costs, stimulating innovation by third-party developers, and generating network effects.

Spiekermann (2019) developed a business model taxonomy for data marketplaces based on eight attributes. According to this taxonomy, data marketplaces can offer direct data exchange (transaction-centric) or complementary services (data-centric). Regarding ownership, platforms are owned by data providers or independent third-party (neutral). Platform owners can be open to unknown participants (open), or only towards certain partners (closed), or somewhere in between (hybrid). In terms of architecture, data marketplaces can be centralized (i.e., central location for data storage), decentralized (i.e., data sellers keep their data), or hybrid. The data provided can be general (i.e., not focusing on specific areas) or domain-specific. Further, the data can be raw/unprocessed data, standardized/normalized data, aggregated data, or high-quality with quality assurance checks. Furthermore, pricing and revenue models include free of charge, fixed price/subscription, and pay-per-use.

Fruhwirth et al. (2020) developed archetypes of data marketplace business models. In a *centralized data trading* archetype, marketplaces are typically used to buy and sell data from diverse domains and origins, involving multiple data types and pricing. Building upon this archetype, the *centralized data trading with the smart contract* uses smart contracts between buyers and sellers. Meanwhile, *decentralized data trading* relies on decentralized infrastructure for buying and selling data. Finally, *personal data trading* are data marketplaces on which consumers sell their data to businesses.

2.3 Multi-party computation

MPC is a cryptographic technique through which two or more parties perform a joint computation, resulting in meaningful output without disclosing the input from the parties (Choi and Butler, 2019; Zhao et al., 2019). Through MPC, data buyers gain insights securely, while data providers attain security assurance because of sharing sensitive data. A typical MPC illustration is the millionaire's problem, a secure comparison function to determine which one of two millionaires is richest, without revealing the net worth to each other (Yao, 1982). 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 implement MPC in real-life applications.

Most MPC implementations make use of the secret-sharing technique since it is efficient and allows more actors to participate in the computation (Pedersen, Saygın and Savas, 2007). The idea is that each party split its data into multiple encoded parts known as secret shares. These shares are used for a specific computation and then recombined to get the final output. Hence, it is possible to compute the data without revealing any information about it.

MPC has been implemented in several use cases, such as auction-based pricing (Bogetoft et al., 2009), tax fraud detection (Bogdanov, Jõemets, Siim and Vaht, 2015), and satellite collision prevention (Hemenway, Lu, Ostrovsky and Welser IV, 2016). Recently, scholars are starting to explore the technical suitability of MPC in data marketplaces. For instance, Roman and Vu (2019) proposed architecture for data marketplaces by combining MPC with blockchain-based smart contracts. Meanwhile, Koch et al. (2021) used MPC to offer privacy-preserving distributed analytics in personal data marketplaces. Nevertheless, large scale implementations of MPC are hindered by, among others, usability issues (i.e., too complex to understand by non-experts), technical issues (i.e., performance limitations and scalability), and legal aspects (i.e., current regulations discourage cooperation) (Choi and Butler, 2019).

Besides MPC, other privacy-preserving technologies also exist, such as homomorphic encryption (Gentry, 2009; Naehrig, Lauter and Vaikuntanathan, 2011) and differential privacy (Dwork, 2006; Dwork and Roth, 2014). While these technologies looked similar to MPC in enabling analysis while protecting input data, there are differences between them (Apfelbeck, 2018). For instance, in homomorphic encryption, only one data seller is involved, whereas MPC requires multiple data providers to perform computation. Moreover, unlike MPC that 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., Pettai and Laud, 2015; Alter, Falk, Lu and Ostrovsky, 2018; Zhong, Sang, Zhang and Xi, 2020).

3 Research approach

We employed a qualitative approach through semi-structured interviews with experts and practitioners in the privacy and security domain. This approach is suitable because we wanted to investigate MPC from a business model perspective within the context of data marketplaces, which is exploratory in nature (Verschuren and Doorewaard, 2010).

We followed the judgment sampling strategy to select respondents (Sekaran and Bougie, 2016) with expertise on privacy and security in general, and MPC in particular, as the main criterion. We chose this sampling approach since we investigated new research areas, namely business model implications of MPC in data marketplaces (cf., Etikan, Musa and Alkassim, 2015). We started by using the references from section 2.3 as the primary source to identify key scholars who work on the topic of MPC. As a complement, we also look into relevant reports and white papers to gather additional business actors. Moreover, we used our personal network by, for instance, selecting experts from European projects on MPC. In addition, we employed the snowball sampling approach by asking interviewees to suggest additional experts. From this sampling approach, we interviewed 15 experts from academia, research institutions, and businesses who averaged nine years of experience in the privacy and security domain (see Table 1). Only one of our interviewees is female. The interviews

were conducted online from March until June 2020. The first author interviewed eight respondents (I-01 to I-06, I-12, and I-13), while the second author interviewed the others. I-14 was first interviewed by the second author and a second time by the first.

ID	Category	Role	Experience
I-01	Academia	PhD researcher in cryptography	2 years
I-02	Academia	PhD researcher in cryptography	2 years
I-03	Academia	PhD researcher in cryptography & cybersecurity	5 years
I-04	Academia	Research scientist in cryptography	5 years
I-05	Academia	PhD researcher in cryptography	2 years
I-06	Academia	Assistant professor in computational privacy	14 years
I-07	Academia	Professor in cryptography	20 years
I-08	Academia	Postdoctoral researcher in cryptography	6 years
I-09	Research Institution	Senior research scientist in data management	17 years
I-10	Research Institution	Cryptography specialist	7 years
I-11	Research Institution	Senior cryptography engineer	8 years
I-12	Research Institution	Senior research scientist in information security	15 years
I-13	MPC service provider	Chief Science Officer & Co-founder	15 years
I-14	MPC service provider	Chief Product Officer & founder	15 years
I-15	MPC service provider	Software Developer	2 years

Table 1. An overview of interviewees

There are advantages and shortcomings of our sampling strategy. On the one hand, we can immediately be focused on exploring potential MPC use cases in data marketplaces since our interviewees already have sufficient knowledge compared to data marketplace operators or industry experts. On the other hand, the knowledgeability of our interviewees might lead to a respondent bias in which they gave a positive view towards MPC, while data marketplace operators or industry experts might perceive this technology differently. Hence, we must interpret findings with caution since it is only valid to the population under study (Tongco, 2007).

Interviews lasted around one hour and started with a short presentation on the definition of data marketplaces and MPC. We also introduced a possible MPC implementation scenario in data marketplaces. During the presentation, we offered interviewees the opportunity to comment, which led to changes in the definition and the illustration of use-cases for the following interview. In this way, we ascertained that interviewees had a similar understanding of data marketplaces and MPC. After the presentation, we asked questions based on the interview protocol, which consisted of two parts. In the first part, we asked confirmatory questions on how MPC works, what it can and cannot do, and its comparison with similar technology like homomorphic encryption. In the second part, we asked exploratory questions on the value MPC offer to businesses, the potential of implementing MPC in data marketplaces, examples of real-life use-cases, and changes in the architecture of data marketplaces with MPC in place. After informed consent, interviews were recorded and transcribed anonymously. We also created notes to outline key insights and surprising remarks from the interviewees to support the analysis. We stored unique identifiers for each interviewee in a separate database, including sensitive information like name and company. To increase the validity of our findings (cf., Brink, 1993), we sent back transcripts to interviewees for approval.

We used Atlas.TI 8.0 software to individually code and analyze each interview transcript based on three coding steps: open coding, axial coding, and selective coding (Bryant and Charmaz, 2007). In open coding, we used an initial set of codes based on the Unified Business Model Framework to guide the analysis. However, we kept an open mind for additional insights, which were added as additional codes. Next, all codes were combined, resulting in a long list of often similar and overlapping codes.

After that, we compared findings between interviewees to assess consistency. Then, we merged and grouped commonalities into high-level concepts using axial coding. For instance, we grouped codes like "privacy-by-design", "protecting their own data", "sharing without sharing", and "data will not be revealed" into one broader category of "privacy". Finally, in selective coding, we referred back to the Unified Business Model framework (see Section 2.1) to structure each category into three overarching themes: value proposition, value architecture, and value finance. These three themes are described in Sections 4, 5, and 6, respectively. In each section, the bold text represents a code that is illustrated with a quote in italic.

4 Value proposition

This section elaborates our findings on the value derived from MPC by the three main actors in data marketplaces: data providers, data buyers, and data marketplace operators.

4.1 Data providers

Most interviewees described **privacy** as one value proposition of MPC for data providers in data marketplaces. By default, MPC will protect input data from data providers from being revealed to anyone. As a result, individuals' privacy (i.e., end-users of data providers) will not be harmed. According to one interviewee (I-14): *"when the data is at rest, it is already encrypted. Once we want to use it, we apply a business function to it, and only the pre-agreed outcomes are public. So, you keep everything encrypted for as long as possible."* Still, data buyers can obtain valuable insights from the computation. In this way, data providers are, in theory, not at risk of losing their data to, for instance, competitors. To illustrate this, one interviewee (I-13) mentioned: *"...what is different about MPC is that you do not decrypt. You still encrypt the data before you share it, but you are able to not decrypt it at any point and yet still … you get the insights, you get the results, you get the value from it. And neither party will need to decrypt anything. You just get the result at the end."* Hence, data providers could share more sensitive data that would not be possible to share before. *"The main thing that MPC could be useful for is to allow competitors, in a sense, to share the data for meaningful insights without actually sharing the data." (I-05)*

Next, MPC also allows data providers to keep **control** of their data. Data providers receive strong security guarantees on how their data is used since they need to approve any computation function that runs through MPC. Put differently, data providers can decide what kind of queries can be performed by data buyers. One interviewee (I-06) stated: *"MPC is about privacy for individuals to be in control of their data. So that is definitely providing privacy, but it means control over the data. What can be shared? What can be seen? What can be processed?"* Similarly, another interviewee (I-12) indicated that: *"In traditional data marketplaces, … you have the data you provided, and you lose control over it. With MPC, you can have sole control of what it is used for. You can allow only certain kinds of computations, and you can have some control over what aggregated values are revealed. So you remain in control."*

When it comes to trust, MPC enables **trustless** computation. Interviewees argued that mutually distrusting parties could collaborate using MPC to achieve a shared goal, which is performing joint computation to generate insights together. Put differently, data providers do not have to trust data buyers or other parties involved in the computation and still can get the output that they need. Thanks to the robust security guarantee of MPC, data providers can maintain the secrecy of their data while taking part in the computation. As illustrated by the following quote (I-11): "*MPC is basically a computation of data between mutually distrusting parties. The aim is to achieve a computation on sensitive data among parties who do not trust each other without leaking any information on the data or affecting the integrity of the result based on a publicly known function to compute."* Another interviewee (I-07) also supported this statement, saying that: *"The goal of MPC, essentially, is to achieve the same functionality without needing such a trusted party. In short, the aim is to execute a protocol among parties that do not necessarily trust each other."*

Finally, MPC enables a **distributed exchange of insights**. Data providers no longer need to transfer their input data centrally to data marketplace operators. As data stays with data providers, it is less likely that data will be transferred to another party for other purposes. One interviewee (I-02) argued that: *".. [MPC] has a lot of potential because it gives the opportunity to share your data without sharing it essentially. So you can circumvent all these privacy-preserving limitations from the law, and still use combined data."* Another interviewee (I-05) also expressed the same argument, saying that: *"you can compute functions without needing to disclose the inputs or any intermediate results to the other parties."*

4.2 Data buyers

One value proposition for data buyers is **privacy**. The inquiry or insights that data buyers intend to gain could be sensitive that might reveal their competitive advantage or even the private information of their end-users. With MPC, data buyers can get results from the computation without revealing their query to data providers, preventing reverse engineering by data providers in the process. According to one interviewee (I-03): *"... maybe the buyers do not necessarily want to reveal that they are really interested in ... because their competitors might also realize that [it] is important. ... I think if some data market realized that you could ... allow the companies to maintain privacy over their data ... I feel like that is something that both buyers and sellers would want, especially if you had it at this meta-level where the buyers do not even have to reveal what it is they necessarily want."*

The second value is **data availability.** Through MPC, data providers may be willing to share more data through data marketplaces. As a result, data buyers would have access to more data and insights than before. As illustrated by one of the interviewees (I-13): *"[MPC] extends the opportunities in the marketplaces, because now I have the option of both controlling my data and allowing people to use it."* Ultimately, more data buyers would use data marketplaces, creating network effects for both sides of the market. *"MPC could increase the revenues, the number of clients of data marketplaces. They have to create a trusted environment within the infrastructure of the marketplace and an encrypted channel to access this environment." (I-14)*

4.3 Data marketplace operators

We found three value propositions of MPC for data marketplace operators. First, MPC allows data marketplace operators to offer "data insights" based on **privacy-preserving analytics** instead of traditional data exchange. This approach would transform the core offering of data marketplaces from one dataset to an aggregation of multiple datasets. As illustrated by one interviewee (I-12): *"…the value is not that much, I think, in the data itself. But the value that you can extract from combining multiple data sources. … it is actually the combination of one data provider and another one that actually gives you a value."*

Second, MPC could be valuable for data marketplace operators in **reducing the risk of data sharing**. Typically, data marketplaces comprise a centralized architecture, meaning that data providers upload their data and store it in a central repository of the operator. Such data transfer creates liability for data marketplace operators for storing data that they do not own. With MPC, data no longer needs to be transferred from data providers to data marketplace operators, as the computation is performed directly between data providers and data buyers. As a result, there will be no transfer of liability as well. Data providers remain in control of their data and approve each query. *"It does not matter how large or sophisticated a company you are, you may lose the data that's in your possession. So a marketplace provider that has a lot of sensitive data in its possession has a lot of liabilities. And if they use this [MPC]technology, they can start reducing those liabilities." (I-13)*

Third, MPC enables **new offerings of privacy-preserving applications and services**. Data marketplace operators could use MPC as building blocks to develop innovative applications and services without compromising privacy. In this way, data marketplace operators can strengthen their position as a platform that keeps the data secure. As one interviewee (I-13) put it: *"if I am a data market provider, I have my own services that are MPC compatible, and I give my customers software*

that can operate with those MPC services. And then they can use MPC to interact with my various offerings or products."

5 Value architecture

This section outlines how MPC affects the value architecture of data marketplaces. Specifically, we discuss new roles for data marketplace operators, different computation processes, and alternative architectural deployment scenarios.

5.1 New role for data marketplace operators

Based on our interviews, we identify two new roles of data marketplace operators with MPC in place. In the first role of **data brokering**, data marketplace operators no longer facilitate data exchange since data does not have to leave the premises of data providers. *"[Data marketplaces] could only provide the MPC protocols and the matchmaking service and never receive any actual data but just deploys the MPC protocols to the different parties, assigns them to different roles, and so on. … In this option, you believe that [data providers] compute the aggregated data and then directly send it to [data buyers] without going through [data marketplaces]. This would be technically possible." (I-01)* As a result, data marketplaces no longer have to store data, allowing them to focus on the coordination function like matchmaking (e.g., mediating between data providers and data buyers) and governing which use-cases and functions are allowed. *"So, you have the data exchange, and you have the market. And the market is being able to find each other and knowing what the other has. That is, of course, a function that can easily be centralized." (I-12)* Data marketplace operators will not be able to see the data, as the computation will be done in a peer-to-peer manner. *"It is important that even the data marketplaces cannot access the private data, but it remains an intermediary that makes the transaction happen. It is important that the data provider remains in full control [of] what [they] can show or not." (I-08)*

The second new role is a **data aggregator**. In this role, data marketplace operators already collect and hold some data that are not sensitive or already have aggregated data from some data providers. Those data can be cleaned and normalized so that data buyers can readily use them. Data marketplace operators would then use MPC in giving access to those ready-to-use data for data buyers. In this way, data marketplace operators can maintain control over their data and only reveal those insights that data buyers need. *"It could be that the data market already has data and want to exchange it with a client. But [data marketplaces are] also not willing to give up all the individual data. So [they] perform this sharing also in the MPC way. … [They could also] offer a service of exploring this data, but not the individual data sets, but with an MPC protocol where the output is predefined." (I-01)*

5.2 Computation processes

Interviewees suggested two possible approaches to implement MPC in data marketplaces. In the first approach, called **synchronous** computation, all participating parties (i.e., data providers and data buyers) need to be online simultaneously to conduct the computations. This scenario is the most common implementation of MPC. *"In the MPC case, you share the data, and you do the computation, but you have to communicate with the other nodes to perform this computation. In the end, you reveal the result. … In the MPC world, the data provider always has to be online and available since they do part of the computation; otherwise, it does not work." (I-04)* Synchronous computation only works if all participants have sufficient resources. *"If the companies who want to do MPC with each other are large organizations with IT departments and teams, and of course, they can all schedule something to happen at the same time."* (I-13)

For data providers that lack resources and computing power, MPC computations can run **asynchronous**ly. In this scenario, each data provider can participate (i.e., submit their data) at a different time, depending on their availability. A coordinating party in the center is needed to *"make it possible to do things in a different order or in a different schedule or not all at the same time." (I-13).*

This coordinating party, which could be the data marketplace operators, does not see the data during the computation, meaning that they do not have to be trusted. As argued by one interviewee (I-13), they are *"only sending back and forth encrypted data or random numbers that are completely meaningless"* due to the secret-sharing protocol employed by MPC.

5.3 MPC deployment scenario

Most interviewees distinguish different architectures for deploying MPC, with different roles for data marketplace operators. In the first scenario of **peer-to-peer**, the MPC software is installed at data providers and data buyers to allow distributed computations. *"… everybody installs a program, … [then] all [of them] start this protocol together, and it takes [as] many rounds [as] it takes to get to completion. Then, they all get an output, and there was no intermediary whatsoever." (I-03)* Since participants conduct the computations by themselves, data marketplace operators do not see the data nor participate in the computation. Instead, their role could be *"… to provide the whole setup, the expertise on how to deploy the MPC protocols, [and] how to design them." (I-01)*

In the second scenario, intermediaries assist in coordinating the MPC process. Here, data marketplace operators provide both MPC software and computational infrastructure (i.e., computing server) as services offered to data providers and consumers. This computational infrastructure could involve **a single computing server** offered directly by the operator. *"You have one centralized person … [then] everybody has to mask their input in some way. Basically, this person is serving as like a router. They are really running this thing, but it is all being run through this central router, but it is all encrypted. So, the central router does not learn anything." (I-03)*

Alternatively, it is also possible to have **multiple independent computing servers** deployed by multiple entities. In this scenario, data marketplace operators establish a consortium in which each company provides a server for the computation. As described by one interviewee (I-15): *"It could also be the case where a data marketplace is set up by different companies, and one company owns one of the engines, and another company owns the other one. So, they can create a sort of solid data foundation together, which is the MPC engine."* In this way, we can *"split [the] trust and you do not have to trust everyone fully, but if at least one of these [computing servers that] you trust behave honestly, then [it will be] fine." (I-01)* One interviewee (I-02) illustrated that: *"Let us say you have three computing servers, and the guys who want to share the data do a secret sharing that they share the input data amongst all of these three computing servers. And then you do not have to be present during the computation but only the three computing servers to do the computation."*

5.4 The relation between roles, computation processes, and deployment scenario

We found that all three MPC deployment scenarios are suitable for the data brokering model. As described in Section 5.1, this model focuses on providing a matchmaking service between data providers and data buyers rather than facilitating data exchange between both parties. Hence, data marketplace operators could opt for peer-to-peer architecture and provide technical expertise to install MPC protocols on the client side. In this way, data is exchanged directly between data providers and data buyers without involving the operator. However, data marketplace operators could also offer computational infrastructure as a service to ease the burden for data providers and consumers. In this regard, the intermediary architecture (either single or multiple servers) would be more suitable. While this architecture requires data marketplace operators to be involved in the computation, they would not be able to see the data as it remains encrypted throughout the process, and only data buyers can access the computation results.

Meanwhile, a peer-to-peer architecture is best suited for the data aggregator model. This model implies that data marketplace operators already own a wide range of data collected from various data providers. In other words, data marketplace operators are transforming into "data providers" that monetize their data. To do this, data marketplace operators could deploy MPC protocols on their side

and offer technical expertise for the data consumer side. In this way, both parties could perform MPC to generate meaningful insights sold to data buyers.

In terms of the computation type, synchronous computation is most compatible with the peer-to-peer architecture. MPC protocols generally require all parties to be online and present at the same time. Peer-to-peer architecture would make this possible, as the MPC protocol would be installed at all parties, allowing them to be connected and present during the computation. The synchronous computation can be organized independently without the need to have a trusted third party in the middle. Nevertheless, it is possible to implement multiple computing servers as intermediaries to facilitate synchronous computation. In this setting, all participating parties do not need to be present simultaneously, but only the multiple servers in the middle. For asynchronous computation, intermediaries have to be present to coordinate the computation process between all parties to participate at different points in time. For this reason, the intermediary architecture (either single or multiple computing server) is the most suitable approach for synchronous computation.

Table 2 summarizes the relationship between the three variables described in this section.

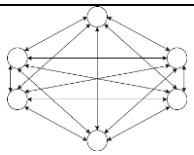
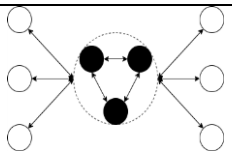
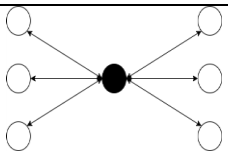
Aspect	**MPC deployment scenario in data marketplaces**		
	Peer-to-peer	**Intermediaries with multiple computing servers**	**Intermediaries with a single computing server**
Illustration			
Role of data marketplace operators	Data broker & Data aggregator	Data broker	Data broker
Computation process	Synchronous	Synchronous & Asynchronous	Asynchronous

Table 2. The relation between data marketplace roles and computation process in three MPC deployment scenarios

6 Value finance

This section described the value finance element in terms of new revenue sources that MPC enables in data marketplaces. Most of our interviewees suggest that, with MPC in place, data marketplace operators could generate revenue by offering MPC-as-a-service and MPC-based services.

In the **MPC-as-a-service** model, data marketplace operators can offer technical expertise to data providers and consumers since the technology is relatively new for businesses. Examples include MPC software installation support and leasing the computational infrastructure to data providers and data buyers. *"… the data market [could] also offer an MPC node as a service. You pay the data market, for example, to also provide computing resources. And this is also a place where you could install an MPC node …" (I-04).* This approach would benefit data providers and data buyers as they can reduce the cost of deploying the infrastructure. *"I think there has to be something like an automated setup that allows these smaller companies to quickly rent the capabilities from a cloud provider. … the data market needs to ensure that this all happens smoothly and that the smaller companies providing the data do not need their own infrastructure but can rent it on-demand …" (I-05)*

In the **MPC-based services** model, MPC is used as building blocks to develop privacy-preserving applications and services, either by data marketplace operators or by third-party service providers. In this regard, data marketplace operators could offer not only *"a simple exchange of data, but [could also offer] a service on exchange data that create new data." (I-09)* One possible service mentioned by interviewees is **privacy-preserving data valuation.** Data providers and data buyers could use

MPC to explore whether there is a value for both parties to collaborate (e.g., combining datasets). The computation would only reveal the newness of the insights, in the form of a yes/no answer, rather than revealing the datasets. *"What we are doing is essentially helping them take pieces of their workflow, like for example, this notion of identifying whether or not there is value in data between two participants in the marketplace." (I-13)*

Another possible service is **privacy-preserving analytics** that delivers aggregated data insights without giving away the input data. *"I think that the aggregation of the data could be interesting for a data buyer. … [MPC] can ensure that the buyer can receive only the aggregation without knowing the original inputs." (I-10)* Current data marketplaces typically only allow data buyers to choose between acquiring all data or not acquiring anything at all. With MPC in place, data buyers can pay only for the insights/aggregation from multiple data providers instead of paying for an entire dataset. *"Now, there is an option in between everything or nothing. Right? They can buy this aggregated pickup location that is in the combination of three companies, rather than just having to pay exorbitant amounts to get everybody's full database. … If you are a buyer, you want to be able to pay for just the insight and not the entire database. And I think this is a really good way to do it." (I-03)*

7 Discussion and conclusion

When used in data marketplaces, MPC creates new *value propositions* for data providers and data buyers by facilitating a **distributed, trustless, and privacy-preserving data sharing** that maintains **control** over their data. This is important as both data providers and data buyers need to ensure no leakage of end-users personal data or other sensitive data while participating in data marketplaces. In this way, we extend the work of Conger (2009) and Bonazzi, Fritscher and Pigneur (2010), who argued that (1) end-users are pushing companies for strong privacy protection, and (2) companies are morally obliged to adopt privacy-preserving technologies to protect the privacy of end-users. We demonstrated that adopting MPC could allow data marketplace operators, data providers, and data buyers to fulfill this moral obligation of protecting the privacy of end-users while still able to create value from data. Furthermore, we complement the work by Bonazzi et al. (2010) and Conger, Pratt and Loch (2013) by exploring how MPC could address privacy problems in data sharing and enable privacy-friendly business models in data marketplaces.

Regarding the *value architecture*, we found that MPC can substantially transform data marketplaces into either **data brokers** (i.e., only as a matchmaker between data providers and data buyers) or **data aggregators** (i.e., only as a reseller of data collected from various sources). MPC could also transform data marketplaces into either a **peer-to-peer model** (i.e., distributed architecture with MPC deployment in all data providers and data buyers) or **an intermediary model** (i.e., a centralized architecture where MPC is deployed centrally to orchestrate the computation). Each architecture pose trade-offs between trust requirements, complexity, and security guarantee, which are important for data marketplace operators as any architectural decisions will affect the viability of the platform and incentives for participants to join (Tiwana, 2014). On the one hand, **a peer-to-peer model** could provide a robust security guarantee and lower trust requirements at the expense of higher complexity and effort for all parties involved. On the other hand**, a single intermediary model** could compromise security guarantees and trust requirements due to lower cost and complexity since the MPC protocol and infrastructure need to be deployed centrally. **Multiple server architecture** is a middle-ground alternative where each computing server is offered by an independent and unrelated entity that acts as intermediaries that perform MPC. This approach could ease the onboarding process for data providers and data buyers but increase the complexity for data marketplace operators. Hence, we expand the work of Alter et al. (2018), who review three different MPC architecture (i.e., single cloud, multiple cloud providers, private servers) and its trade-off in terms of trust requirements, performance, involvement of data owners, and scalability. We demonstrated that these MPC architectures are, in theory, also applicable within the context of data marketplaces. Nevertheless, since most MPC implementations in data marketplaces are still in the proof-of-concept phase, further research is

required to investigate whether (1) those architectures are indeed applicable in practice and (2) the trade-offs are valid.

Regarding *value finance*, two important findings emerged. First, MPC enables new revenue sources for data marketplaces in the form of **MPC-as-a-service** (i.e., leasing MPC infrastructure and software) and **MPC-based services** (i.e., applications and services based on MPC to increase the value of data). To generate revenue from these new offerings, data marketplace operators can use a **subscription** model (i.e., monthly or yearly payments) or a **pay-per-use** model (i.e., only pay when needed). Second, MPC shifts the core value of data marketplaces **from offering data to insights** (i.e., combining multiple datasets), allowing data buyers to look for something different (e.g., "what kind of insights that are available in data marketplaces?" or "what kind of query that can I request in data marketplaces?"). In this way, data buyers could better assess the quality of the data based on the usefulness of the insights, protecting them from the risk of purchasing data with unclear quality (Koutroumpis et al., 2020). Furthermore, like the decision on architectures, data marketplace operators should carefully choose their monetization strategy as it will determine the adoption and viability of the platform (Cusumano, Gawer and Yoffie, 2019).

An unexpected finding was that MPC could be implemented in a wide range of services and functionalities within data marketplaces, suggesting that the value of MPC could go beyond the obvious use-case of data exchange. Specifically, MPC enables data marketplace operators to facilitate the creation of new privacy-preserving service offerings by providing an environment for third-party development. In this regard, MPC could be viewed as a boundary resource in the privacy-preserving data marketplaces, which according to Ghazawneh and Henfridsson (2013), is "the software tools and regulations that serve as the interface for the arm's-length relationship between the platform owner and the application developer." Put differently, MPC could make data marketplaces extensible in a way that resembles other digital platforms (Tiwana, Konsynski and Bush, 2010). By leveraging MPC as generic and reusable components, data marketplaces could become "real" digital platforms that go beyond matchmaking features, creating values for participants through innovation from third-party service providers in an unforeseeable way (Tilson, Lyytinen and Sørensen, 2010; Kallinikos, Aaltonen and Marton, 2013). Such a mechanism would ultimately attract data providers and data buyers to participate in data marketplaces, creating network effects.

Overall, these findings suggest privacy as the core value of MPC that enables new business models in data marketplaces. Hence, we argue that data marketplace operators could orchestrate their platform to become privacy-preserving data marketplaces that employ *privacy-as-a-service* as their business model. By leveraging MPC extensions, privacy becomes the core value of data marketplaces that is delivered to both data providers and data buyers through, for instance, privacy-preserving analytics. However, MPC extensions could go beyond data exchange by allowing third-party service providers to develop privacy-preserving applications and services. In this way, MPC serves as a control mechanism for data marketplace operators to ensure that participants behave in line with the goal of data marketplaces, which is secure data sharing that protects the privacy of end-users (cf., Tiwana, 2014; Goldbach, Benlian and Buxmann, 2018).

It is worth noting that privacy is generally discussed within the context of end-users and not about business-to-business relationships. Nevertheless, as Conger (2009) argued, the involvement of companies in data sharing might pose risks that go beyond the control of their end-users, such as leakage of personal data. Given the strong push from end-users (Conger, 2009; Bonazzi et al., 2010), companies need to put more effort into protecting the privacy of end-users before deciding to take part in data sharing. We argue that MPC could be positioned as a way for data marketplace operators to help companies fulfill this goal by facilitating the sharing of "data insights" instead of individual-level data (Elliot and Quest, 2020).

In view of our research limitations, we propose three suggestions for future research. First, our samples are limited to MPC experts, making it possible that our findings only tell one side of the story. Hence, further research should incorporate the view of data providers, data buyers, and data marketplace operators and explore other aspects such as the impact of MPC on willingness to share

data. In this way, we can get a complete view of MPC implications in data marketplaces. Second, we only focus on MPC as one class of privacy-preserving technologies (PPT), while there are other solutions such as differential privacy and homomorphic encryption (see Section 2.3). Therefore, future research should either (1) explore the business model implications of other PPT or (2) analyze the implication of MPC in combination with other PPT. Lastly, our interviews were based on a thought experiment given the lack of real-life implementation of MPC in data marketplaces. We suggest scholars extend our study by exploring new business models based on a working prototype (or even a real-life application) of privacy-preserving data marketplaces based on MPC.

To sum up, our study provides several theoretical and practical contributions. First, this research sets the basis for understanding the business model implications of privacy-preserving technologies within the context of MPC and data marketplaces. This is important because, so far, we have lacked an understanding of how MPC creates value in the currently emerging area of data marketplaces. Second, we extend the applicability of the Unified Business Model framework (Al-Debei and Avison, 2010) into the context of data marketplaces and MPC. We demonstrate that this framework helps us in analyzing the changes caused by MPC implementation in data marketplaces. Third, we show that data marketplace operators could implement MPC to actively promote privacy as their core value instead of waiting for demands from data providers and data buyers. Finally, we infer from the study that in designing business models for data marketplaces, operators should not only consider the transaction capabilities but also innovation capabilities of data marketplaces as digital platforms (Gawer, 2014; Cusumano et al., 2019). We demonstrate that MPC could be beneficial as an extension to allow the generativity of data marketplaces and go beyond mere matchmaking.

Acknowledgments

The work leading to this paper has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 825225.

References

Al-Debei, M. M. and D. Avison. (2010). "Developing a unified framework of the business model concept." *European Journal of Information Systems*, *19*(3), 359–376.

Alt, R. and H.-D. Zimmermann. (2001). "Preface: introduction to special section–business models." *Electronic Markets*, *11*(1), 3–9.

Alter, G., B. H. Falk, S. Lu and R. Ostrovsky. (2018). "Computing Statistics from Private Data." *Data Science Journal*, *17*(0), 31.

Apfelbeck, F. (2018). "Evaluation of Privacy-Preserving Technologies for Machine Learning." Retrieved from https://outlierventures.io/research/evaluation-of-privacy-preserving-technologies-for-machine-learning/

Athanasopoulou, A., M. de Reuver, S. Nikou and H. Bouwman. (2019). "What technology enabled services impact business models in the automotive industry? An exploratory study." *Futures*, *109*, 73–83.

Baden-Fuller, C. and S. Haefliger. (2013). "Business models and technological innovation." *Long Range Planning*, *46*(6), 419–426.

Bestavros, A., A. Lapets and M. Varia. (2017). "User-centric distributed solutions for privacy-preserving analytics." *Communications of the ACM*, *60*(2), 37–39.

Bogdanov, D., M. Jõemets, S. Siim and M. Vaht. (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). Berlin, Heidelberg: Springer.

Bogetoft, P., D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, … T. Toft. (2009). "Secure Multiparty Computation Goes Live." In: R. Dingledine & P. Golle (Eds.), *Financial Cryptography and Data Security* (pp. 325–343). Berlin, Heidelberg: Springer.

Bonazzi, R., B. Fritscher and Y. Pigneur. (2010). "Business model considerations for privacy protection in a mobile location based context." In: *2010 14th International Conference on Intelligence in Next Generation Networks* (pp. 1–8).

Bouwman, H., H. de Vos and T. Haaker. (2008). *Mobile service innovation and business models*. Springer Science & Business Media.

Bouwman, H., S. Nikou and M. de Reuver. (2019). "Digitalization, business models, and SMEs: How do business model innovation practices improve performance of digitalizing SMEs?" *Telecommunications Policy*, *43*(9), 101828.

Brandão, A., H. S. Mamede and R. Gonçalves. (2019). "Trusted Data's Marketplace." In: Á. Rocha, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *New Knowledge in Information Systems and Technologies* (pp. 515–527). Cham: Springer International Publishing.

Brink, H. I. L. (1993). "Validity and reliability in qualitative research." *Curationis*, *16*(2), 35–38.

Bryant, A. and K. Charmaz. (2007). *The SAGE Handbook of Grounded Theory*. 1 Oliver's Yard, 55 City Road, London England EC1Y 1SP United Kingdom: SAGE Publications Ltd.

Chesbrough, H. and R. S. Rosenbloom. (2002). "The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies." *Industrial and Corporate Change*, *11*(3), 529–555.

Choi, J. I. and K. R. B. Butler. (2019). "Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities." *Security and Communication Networks*, *2019*, 1368905.

Conger, S. (2009). "Personal Information Privacy: A Multi-Party Endeavor." *Journal of Electronic Commerce in Organizations (JECO)*, *7*(1), 71–82.

Conger, S., J. H. Pratt and K. D. Loch. (2013). "Personal information privacy and emerging technologies." *Information Systems Journal*, *23*(5), 401–417.

Cusumano, M. A., A. Gawer and D. B. Yoffie. (2019). *The Business of Platforms: Strategy in the Age of Digital Competition, Innovation, and Power*. New York: Harper Business.

de Reuver, M., H. Bouwman and I. MacInnes. (2009). "Business models dynamics for start-ups and innovating e-businesses." *International Journal of Electronic Business*, *7*(3), 269–286.

Dwork, C. (2006). "Differential Privacy." In: M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Eds.), *Automata, Languages and Programming* (pp. 1–12). Berlin, Heidelberg: Springer.

Dwork, C. and A. Roth. (2014). "The Algorithmic Foundations of Differential Privacy." *Foundations and Trends® in Theoretical Computer Science*, *9*(3–4), 211–407.

Elliot, D. and L. Quest. (2020, January 14). "It's time to redefine how data is governed, controlled and shared. Here's how." Retrieved from https://www.weforum.org/agenda/2020/01/future-of-data-protect-and-regulation/

Etikan, I., S. A. Musa and R. S. Alkassim. (2015). "Comparison of Convenience Sampling and Purposive Sampling." *American Journal of Theoretical and Applied Statistics*, *5*(1), 1.

Fricker, S. A. and Y. V. Maksimov. (2017). "Pricing of data products in data marketplaces." In: *International Conference of Software Business* (pp. 49–66). Springer.

Fruhwirth, M., M. Rachinger and E. Prlja. (2020). "Discovering Business Models of Data Marketplaces." In: *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

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

Gawer, A. (2014). "Bridging differing perspectives on technological platforms: Toward an integrative framework." *Research Policy*, *43*(7), 1239–1249.

Gentry, C. (2009). "Fully homomorphic encryption using ideal lattices." In: *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169–178). New York, NY, USA: Association for Computing Machinery.

Ghazawneh, A. and O. Henfridsson. (2013). "Balancing platform control and external contribution in third-party development: the boundary resources model." *Information Systems Journal*, *23*(2), 173–192.

Goldbach, T., A. Benlian and P. Buxmann. (2018). "Differential effects of formal and self-control in mobile platform ecosystems: Multi-method findings on third-party developers' continuance intentions and application quality." *Information & Management*, *55*(3), 271–284.

Guo, C., J. Katz, X. Wang and Y. Yu. (2020). "Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers." In: *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 825–841).

Hemenway, B., S. Lu, R. Ostrovsky and W. Welser IV. (2016). "High-Precision Secure Computation of Satellite Collision Probabilities." In: V. Zikas & R. De Prisco (Eds.), *Security and Cryptography for Networks* (pp. 169–187). Cham: Springer International Publishing.

Janssen, M. and A. Zuiderwijk. (2014). "Infomediary Business Models for Connecting Open Data Providers and Users." *Social Science Computer Review*, *32*(5), 694–711.

Jarman, H., L. F. Luna-Reyes and J. Zhang. (2016). "Public Value and Private Organizations." In: H. Jarman & L. F. Luna-Reyes (Eds.), *Private Data and Public Value: Governance, Green Consumption, and Sustainable Supply Chains* (pp. 1–23). Cham: Springer International Publishing.

Kallinikos, J., A. Aaltonen and A. Marton. (2013). "The Ambivalent Ontology of Digital Artifacts." *MIS Quarterly*, *37*(2), 357–370.

Khurana, M., P. Mishra and A. R. Singh. (2011). "Barriers to Information Sharing in Supply Chain of Manufacturing Industries." *International Journal of Manufacturing Systems*, *1*, 9–29.

Klein, T. and S. Verhulst. (2017). *Access to New Data Sources for Statistics: Business Models and Incentives for the Corporate Sector* (SSRN Scholarly Paper No. ID 3141446). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=3141446

Koch, K., S. Krenn, D. Pellegrino and S. Ramacher. (2021). "Privacy-preserving Analytics for Data Markets using MPC." *ArXiv Preprint ArXiv:2103.03739*.

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

Lapets, A., F. Jansen, K. D. Albab, R. Issa, L. Qin, M. Varia and A. Bestavros. (2018). "Accessible Privacy-Preserving Web-Based Data Analysis for Assessing and Addressing Economic Inequalities." In: *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies* (pp. 1–5). New York, NY, USA: Association for Computing Machinery.

Manyika, J. (2015). *The Internet of Things: Mapping the value beyond the hype*. McKinsey Global Institute.

Mišura, K. and M. Žagar. (2016). "Data marketplace for Internet of Things." In: *2016 International Conference on Smart Systems and Technologies (SST)* (pp. 255–260).

Muschalle, A., F. Stahl, A. Löser and G. Vossen. (2013). "Pricing Approaches for Data Markets." In: M. Castellanos, U. Dayal, & E. A. Rundensteiner (Eds.), *Enabling Real-Time Business Intelligence* (pp. 129–144). Berlin, Heidelberg: Springer.

Naehrig, M., K. Lauter and V. Vaikuntanathan. (2011). "Can homomorphic encryption be practical?" In: *Proceedings of the 3rd ACM workshop on Cloud computing security workshop* (pp. 113–124). New York, NY, USA: Association for Computing Machinery.

Osterwalder, A. and Y. Pigneur. (2010). *Business model generation: a handbook for visionaries, game changers, and challengers*. John Wiley & Sons.

Pedersen, T. B., Y. Saygın and E. Savas. (2007). "Secret Sharing vs. Encryption-based Techniques For Privacy Preserving Data Mining."

Pettai, M. and P. Laud. (2015). "Combining Differential Privacy and Secure Multiparty Computation." In: *Proceedings of the 31st Annual Computer Security Applications Conference* (pp. 421–430). New York, NY, USA: Association for Computing Machinery.

Ranerup, A., H. Z. Henriksen and J. Hedman. (2016). "An analysis of business models in Public Service Platforms." *Government Information Quarterly*, *33*(1), 6–14.

Richter, H. and P. R. Slowinski. (2019). "The data sharing economy: on the emergence of new intermediaries." *IIC-International Review of Intellectual Property and Competition Law*, *50*(1), 4–29.

Roman, D. and K. Vu. (2019). "Enabling Data Markets Using Smart Contracts and Multi-party Computation." In: W. Abramowicz & A. Paschke (Eds.), *Business Information Systems Workshops* (pp. 258–263). Cham: Springer International Publishing.

Sayogo, D. S., J. Zhang, T. A. Pardo, G. K. Tayi, J. Hrdinova, D. F. Andersen and L. F. Luna-Reyes. (2014). "Going Beyond Open Data: Challenges and Motivations for Smart Disclosure in Ethical Consumption." *Journal of Theoretical and Applied Electronic Commerce Research*, *9*(2), 1–16.

Schomm, F., F. Stahl and G. Vossen. (2013). "Marketplaces for data: an initial survey." *ACM SIGMOD Record*, *42*(1), 15–26.

Schreieck, M., A. Hein, M. Wiesche and H. Krcmar. (2018). "The challenge of governing digital platform ecosystems." In: *Digital marketplaces unleashed* (pp. 527–538). Springer.

Sekaran, U. and R. Bougie. (2016). *Research Methods For Business: A Skill Building Approach*. John Wiley & Sons.

Spiekermann, M. (2019). "Data marketplaces: Trends and monetisation of data goods." *Intereconomics*, *54*(4), 208–216.

Stahl, F., F. Schomm and G. Vossen. (2014). "Data Marketplaces: An Emerging Species." In: *Databases and Information Systems VIII* (Vol. 270, pp. 145–158).

Stahl, F., F. Schomm, G. Vossen and L. Vomfell. (2016). "A classification framework for data marketplaces." *Vietnam Journal of Computer Science*, *3*(3), 137–143.

Susha, I., M. Flipsen, W. Agahari and M. de Reuver. (2020). "Towards Generic Business Models of Intermediaries in Data Collaboratives: From Gatekeeping to Data Control." In: G. Viale Pereira, M. Janssen, H. Lee, I. Lindgren, M. P. Rodríguez Bolívar, H. J. Scholl, & A. Zuiderwijk (Eds.), *Electronic Government* (pp. 304–315). Cham: Springer International Publishing.

Teece, D. J. (2010). "Business models, business strategy and innovation." *Long Range Planning*, *43*(2–3), 172–194.

Tilson, D., K. Lyytinen and C. Sørensen. (2010). "Research Commentary—Digital Infrastructures: The Missing IS Research Agenda." *Information Systems Research*, *21*(4), 748–759.

Tiwana, A. (2014). *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*. Elsevier.

Tiwana, A., B. Konsynski and A. A. Bush. (2010). "Research Commentary—Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics." *Information Systems Research*, *21*(4), 675–687.

Tongco, M. D. C. (2007). "Purposive Sampling as a Tool for Informant Selection." *Ethnobotany Research & Applications*, *5*.

van den Broek, T. and A. F. van Veenstra. (2018). "Governance of big data collaborations: How to balance regulatory compliance and disruptive innovation." *Technological Forecasting and Social Change*, *129*, 330–338.

Verschuren, P. and H. Doorewaard. (2010). *Designing a research project* (Vol. 2). The Hague: Eleven International Publishing.

Virkar, S., G. Viale Pereira and M. Vignoli. (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). Cham: Springer International Publishing.

Volgushev, N., M. Schwarzkopf, B. Getchell, M. Varia, A. Lapets and A. Bestavros. (2019). "Conclave: secure multi-party computation on big data." In: *Proceedings of the Fourteenth EuroSys Conference 2019* (pp. 1–18). New York, NY, USA: Association for Computing Machinery.

Yao, A. C. (1982). "Protocols for secure computations" (pp. 160–164). Presented at the 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), IEEE.

Zafrir, N. (2020, January 17). "Beyond trust: Why we need a paradigm shift in data-sharing." Retrieved from https://www.weforum.org/agenda/2020/01/new-paradigm-data-sharing/

Zhao, C., S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li and Y. Tan. (2019). "Secure Multi-Party Computation: Theory, practice and applications." *Information Sciences*, *476*, 357–372.

Zhong, H., Y. Sang, Y. Zhang and Z. Xi. (2020). "Secure Multi-Party Computation on Blockchain: An Overview." In: H. Shen & Y. Sang (Eds.), *Parallel Architectures, Algorithms and Programming* (pp. 452–460). Singapore: Springer.