The business value of privacy-preserving technologies the case of multiparty computation in the telecom industry

Ofe, Hosea; Minnema, Harm; de Reuver, Mark

DOI
10.1108/DPRG-10-2021-0132

Publication date
2022

Document Version
Accepted author manuscript

Published in
Digital Policy, Regulation and Governance

Citation (APA)
Ofe, H., Minnema, H., & de Reuver, M. (2022). The business value of privacy-preserving technologies: the case of multiparty computation in the telecom industry. *Digital Policy, Regulation and Governance*, *24*(6), 541-557. https://doi.org/10.1108/DPRG-10-2021-0132

The Business Value of Privacy-Preserving Technologies: the case of multi-party computation in the telecom industry

Abstract

Purpose: This paper proposes a framework for how privacy-preserving technologies (PETs) create business value for organizations. The framework was developed by examining the literature on privacy and information technology's impact (symbolic and function). We evaluate the framework's applicability using Multi-Party Computation (MPC) as an instance of PETs, with expert interviews in the telecommunication industry.

Design/methodology/approach: In an illustrative case of four telecommunication companies, we conducted semi-structured interviews with experts and used Multi-party Computation(MPC) as an instance of PET.

Findings: The evaluation of the framework indicates that PETs create business value for organizations: enhancing customer interactions, sales, personalized services, predicting market trends, and collaboration among organizations. The findings show that business value of PETs is mainly driven by consumers and organizations willing to share data and collaborate.

Practical Implications: Our findings inform managers in exploring the business value of PETs for organizations. Our study also provides insights into which costs and risks to consider when implementing PETs.

Originality: This study is one of the few to propose a framework on how PETs create business value for organizations. Future research can use factors in the framework (e.g., customer interactions, sales, personalized services, and market trend prediction) to conduct a quantitative study on PETs' business value. Managers adopting PETs can use the framework to identify areas where PETs impact their organization.

Keywords: Privacy, business value, symbolic value, functional value, cost, trust, risk, privacy-enhancing technologies, multi-party computation

1 Introduction

Controlling sensitive information about oneself is of societal and scholarly importance. Privacy has long been a research focus (Acquisti *et al.*, 2013, Acquisti *et al.*, 2016, Posner, 1977, Smith *et al.*, 2011, Zöll *et al.*, 2021). A renewed interest in privacy is gaining traction as more data collection techniques become widespread and less observable to users. For instance, consumer preferences are tracked using cookies embedded in browsers. New business models are emerging that rely on monetizing personal data collected across platforms (Zuboff, 2015, van der Vlist and Helmond, 2021, Acquisti *et al.*, 2016).

The emergence of pervasive techniques for data collection has fueled the interest in privacy-preserving technologies (PETs). PETs are a broad range of technologies with capabilities that can, for instance, anonymize, conceal, compute, and encrypt sensitive information (Smith *et al.*, 2011). PETs are potentially valuable to attain compliance with data privacy regulations and adopt privacy-sensitive business models (Li and Sarkar, 2014, Borking, 2011, Zöll *et al.*, 2021). In addition, PETs could be valuable to address increasing privacy concerns such as identity theft and misuse of sensitive data when shared (Acquisti *et al.*, 2016). The focus on privacy may pressure organizations to consider adopting PETs. At the same time, the extent to which PETs are adopted and effectively utilized depends, more importantly, on their business value for organizations. For example, a study by Borking (2011) revealed that PETs adoption is problematic as they are of relatively limited use without a concrete business case. Also, while there is an increase in PETs' development and capabilities, most initiatives are found to stall at the pilot or experimentation phase without widespread commercial use (Goldberg, 2007, Danezis and Gürses, 2010).

Despite PETs' potential relevance, a concerted effort to examine PETs' business value and business cases for organizations remains lacking (Borking, 2011). Most studies highlight the potential benefits or harmful effects of privacy for consumers, e.g., in marketing (Wang *et al.*, 1998), protection of personal data in online transactions (Malhotra *et al.*, 2004, Van Dyke *et al.*, 2007, Paine *et al.*, 2007, Fogel and Nehmad, 2009), or sharing of individual location-based data(Chen *et al.*, 2008). These studies primarily seek to explain the motivation of PETs adoption through socially inclined factors such as legal requirements and benefits of privacy preservation

from consumers' perspectives. However, a holistic understanding of PETs' business value remains lacking.

Investing in PETs can be highly complex and challenging when relatively limited research and guidance on its potential business value exists for organizations. Fragmented and partial insights are found across different research streams. For example, economic studies point to potential legal and implementation costs for organizations in PETs adoption (Borking, 2011, Muris, 2004, Rossnagel, 2010). Technical research points to issues of alignment and interoperability of PETs (Goldberg, 2007, Borking, 2011). Furthermore, the concealment of relevant information by PETs is also argued to hinder the efficient allocation of assets and the usefulness of PETs (Acquisti, 2014, Muris, 2004). PETs can reduce data accuracy during processing (Zöll *et al.*, 2021). However, whether privacy initiatives offer clear business value has scarcely been addressed.

This paper proposes a framework for understanding PETs' business value. In particular, the overarching research question is: How can we understand the business value of privacy-enhancing technologies?. We do so by examining business literature on the impact of privacy and Information Technology on organizational performance. We conduct an illustrative case study using multi-party computation (MPC) as a specific instance of PETs within the telecommunication industry to evaluate the framework's applicability. MPC allows businesses to compute functions without revealing the underlying data (Ghanem and Moursy, 2019). MPC is one of the most prominent emerging types of PETs (Evans *et al.*, 2017), with capabilities of anonymizing, computing, and concealing sensitive data.

This paper makes three contributions. First, we provide a framework for understanding how PETs create business value. Second, by applying the framework to a case, we uncover specific instances of how PETs create business value, risks, and costs for organizations. Third, we provide recommendations for organizations on how to complement the utilization of PETs to enhance business value. Furthermore, we show how MPC as a specific instance of PET fosters data sharing.

1.1 Layout

The paper is structured as follows. Section 2 covers the literature review: privacy definitions, privacy research, and PETs. Section 3 focuses on framework development. We start the framework development by focusing on business values: symbolic and functional (Section 3.1). The costs and risks elements of our framework are addressed in sections 3.2 and 3.3, respectively. Building on elements discussed in sections 3.1, 3.2, and 3.3, we present an initial framework(see figure 1) for understanding PETs Business Value. In section 4, we use Multiparty Computation(MPC) as an illustrative instance of PET to evaluate our framework. We focus on the telecommunication industry as our research context. The results are presented in section 5, structured into business value, cost, and risks. We refine our initially proposed framework based on the results into a revised version(see figure 3). In section 6, we present a discussion of key findings, research and practical implications, limitations, and conclusions of our study

2 Privacy and Privacy-preserving Technologies

2.1 Defining Privacy

Privacy is a broad concept studied in different disciplines such as law, economics, political science, marketing, management, and information systems (Smith *et al.*, 2011, Pavlou, 2011). Closely related concepts to privacy include anonymity, secrecy, and confidentiality. Anonymity is "when someone is acting in a way that limits the availability of identifiers to others" (Smith *et al.*, 2011,p. 996). For example, anonymizing conceals identifiers through encryptions. Secrecy is the concealment of information. In secrecy, control of privacy is achieved through individuals determining what audiences can know. Confidentiality is the "controlled release of personal information to an information custodian under an agreement that limits the extent and conditions under which that information may be used or released further" (Smith *et al.*, 2011,p. 996). When referring to privacy, we mean "the ability of an individual to personally control information about one's self" (Stone *et al.*, 1983).

2.2 Privacy Research within IS

Since this paper seeks to understand PETs' business value, we limit ourselves to literature related to the business impacts of privacy. Research on privacy concerns focuses on consumer attitudes towards privacy practices. Privacy concerns include unauthorized personal information use, improper access or collection of personal information (Smith et al., 1996), and identity theft (Acquisti *et al.*, 2016). Taddicken (2014), in a study of 2730 internet users, found privacy concerns hardly impacted users' disclosure of their information. They found that disclosure of personal information was mediated by the relevance of its application for users and social relevance. Culnan (1993) found that consumers less sensitive to secondary use of their data are tolerant of an organization's privacy practices. At the organizational level, privacy practices enable transparency in addressing secondary data uses (Culnan, 1993). Instead, the focus is on examining organizational privacy practices and their relationship or individuals' perceptions and concerns about those practices (Smith *et al.*, 1996).

Another group of studies on privacy concerns focuses on its impact on consumers' data sharing and its economic impact on organizations. For example, privacy protection is argued by some to be informed mainly by legislative goals without clear benefits for businesses (e.g., Posner, 1977, Posner, 1981). This belief arises from the potential costs (e.g., legal and implementation costs) of ensuring privacy is argued to exceed benefits (Muris, 2004). For example, Zöll *et al.* (2021) point to losing vital or accurate information during data processing to ensure privacy. Inaccurate information creates inefficiencies in allocating assets (Acquisti, 2014, Muris, 2004). In their study of the cause and consequences of privacy concerns, Wirtz *et al.* (2007) found that consumers provide inaccurate or poor-quality information to organizations because of privacy concerns. Inaccurate information leads to uninformed decision-making and inefficient use of resources (Wirtz *et al.*, 2007). More recent studies have found the inability to download contact tracing apps due to privacy concerns regarding the COVID-19 pandemic (Chan and Saqib, 2021). Privacy concerns are also found to hinder users' engagement with social media-enabled apps (Jozani *et al.*, 2020).

Others argue that most businesses are honest, and sensitive data collected benefits consumers, e.g., through personalized services(Muris, 2004). Furthermore, by sharing personal information, e.g., location data, users may benefit from location-based services relevant in cases of emergency or help governmental agencies to curtail disease spread(Chen et al., 2008). According to Pavlou (2011), consumers will share their data if benefits are provided, and privacy protection does not guarantee that users share data. Other studies suggest that privacy concerns should focus on addressing misuse and inaccurate use of information rather than costly privacy mandates that hamper business competitiveness Muris (2004).

Sharing personal data may also reduce frictions in the market and facilitate transactions (Acquisti *et al.*, 2016). Full disclosure of information between parties in a bilateral relationship is vital in boosting efficiencies and not harming parties' interests in bilateral trade (Calzolari and Pavan, 2006). Other studies have found that intrusion of consumers' privacy negatively affects consumer willingness to pay (Acquisti and Spiekermann, 2011). Preserving privacy is economically sound from a social welfare perspective for consumers. PETs can provide a competitive advantage for firms in price discrimination of personalized services and market segmentation (Lee *et al.*, 2011). Most studies focus on consumer reaction to privacy concerns, focusing less on potential benefits for organizations.

2.3 Capabilities of Privacy-Preserving Technologies

PETs represent a broad range of technologies utilized to preserve privacy. PETs can range from web-based anonymization tools such as Java Anon Proxy(JAP) to off-the-record messaging interactive anonymity tools such as Tor (Goldberg, 2007). PETs provide functionalities, e.g., anonymization, concealment of sensitive data, and optimization of data, allowing users to carry out privacy-preserve tasks (Schiffner *et al.*, 2018, Diaz and Gürses, 2012). The capabilities enable users to encrypt their Internet applications, conceal IP protocols, or anonymize a transaction's content (Goldberg, 2007). Two cryptographic methods are used in PETs: Private Set Intersection(PSI) and Homomorphic Encryption(HE). Private Set Intersection(PSI) refers to when two parties hold a private data set while wanting to find the intersection of their sets without revealing anything except the intersection itself. The most computationally efficient PSI protocols

use oblivious transfer, a mathematical algorithm used to encrypt data(Chen *et al.*, 2017). A simplified explanation of Oblivious Transfer is that Company A has multiple secret inputs. Company B can select one of them. The function of the protocol does not reveal which one of the secret inputs Company B selected, and it will also not reveal what the other inputs were(Evans *et al.*, 2017).

Homomorphic encryption(HE) allows participants to evaluate computations on encrypted data without decrypting it first. Computations through HE is considered efficient and simple (Ghanem and Moursy, 2019). The party with the smallest dataset sends its encrypted dataset to the party with the larger dataset" (Chen *et al.*, 2017). The party with the smaller dataset can then decrypt the result. Multiple parties hold their private share of a value to be recovered at the end of the computation using their encryption keys(Beaver *et al.*, 1990). This method protects against parties from obtaining the secret values from the output values unauthorized, thus making the transaction secure (Lam, 2020).

3 Framework development: business value

Since we seek to understand the business value of PETs, we use literature on IT impact on organizational performance and economic literature on privacy to inform our framework development. Business value describes "how and to what extent the application of IT within firms leads to improved business performance" (Melville *et al.*, 2004). Business value can be symbolic and functional(Grover *et al.*, 2018).

3.1 Symbolic Value and Functional Value

Symbolic values describe indirect benefits to businesses from positive signals that technology adoption conveys to interested stakeholders or consumers about a company(Grover *et al.*, 2018). Symbolic value build on signaling theory(Spence, 1978). Signaling theory posits that sharing positive information about a company positively affects its outlook (Connelly *et al.*, 2011, Spence, 1978). The positive outlook brings in benefits for the organization. For example, consumers associate with a company showing a positive attitude towards the environment (Hartmann and Apaolaza-Ibáñez, 2012). IT features such as transparency, quality-assured content, security, and signaling information transparency and privacy help build trust and

participation (Benlian and Hess, 2011). Tsai *et al.* (2011) found that consumers are even more willing(pay premiums) to purchase from businesses that display information on privacy protection. They suggest privacy protection can be a crucial selling point for companies to enhance their sales. Blockchain adoption in a supply chain has also been found to provide transparency in information sharing, providing favorable financing terms for businesses (Chod *et al.*, 2020). Consumers are more willing to consume or partake in products with high signaling potential (Bennett and Chakravarti, 2009). IT impact on organizations can also be indirect, through enhancing practices that facilitate information sharing (Mata *et al.*, 1995).

Organizations can directly benefit from utilizing technologies to enhance business performance. Improved business performance includes sales, service delivery, sales, and customer relations improvements (Soh and Markus, 1995, Melville *et al.*, 2004). For example, IT generates financial value through IT impact on complementary resources and information sharing (Kohli and Grover, 2008). Building on the resource-based Theory, Melville *et al.* (2004) conceptualized IT Value on organizational performance through IT's impact on business processes such as logistics, sales, and operational efficiency.

3.1.1 Potential Value of Shared Data

Data is a crucial asset of value for organizations. For example, businesses can extract value through insights from customers' data to target and predict market trends (Acquisti, 2014). Organizations can utilize customer purchasing history data to provide more personalized services (Acquisti and Varian, 2005). An example is comScore which analyzes web trends by combining survey and behavioral observations of millions of online consumers. They sell their data and the trends they observe to clients for market testing, segmentation analysis, and competitive intelligence (Acquisti, 2010). Acquisti and Varian (2005) found that additional consumer data benefits the company's profits when used to enhance personalized services. For instance, rich datasets provide information that improves the marketing capabilities of a company, boosting the ability to target markets or customers (Blattberg and Deighton, 1991).

A study by Calzolari and Pavan (2006) shows a Pareto improvement mathematically when two firms share unrestricted data. The study shows that data availability may reduce market

distortions and even increase consumer social welfare. Consumers may even suffer privacy costs when less personal information is shared with third parties. Consumers might want to share their data to receive product discounts and recommendations. Acquisti and Varian (2005) researched a two-period model. The companies could track consumers and gather other data from them. Consumers could hide and anonymize their behavior by using anonymous browsing, deleting cookies, and using anonymous payment tools. They concluded that data was valuable for merchants to provide consumers with enhanced personalized services. We assume that by adopting PETs, businesses are likely to benefit from their exposure to more data arising from more consumers and businesses willing to share their data. For example, they provide the potential positive signal that spurs consumers willing to share their data.

3.2 Willingness to Share Data

Extant literature on the role of technologies suggests that privacy protection potentially plays a vital role in enhancing the willingness of users to share data. For example, in e-commerce, perceived privacy empowerment by consumers(i.e., consumers feeling more in control of data) is found to positively influence trust towards those organizations (Van Dyke *et al.*, 2007). Studies have shown that emphasizing the branding of products based on their psychological benefits for users increases purchasing intention (Hartmann and Apaolaza-Ibáñez, 2012). Studies have found consumers to be more willing to allow their data to be used for advertising websites if they perceive having control over their data (Tucker, 2012). Research has found that customers are less sensitive and willing to share their data if organizations adopt practices that protect their data (Culnan, 1993). The perception of individuals and their concerns towards those privacy practices adopted by an organization thus help shape their intention to share information (Smith *et al.*, 1996).

3.3 Costs

Costs are considered across three overarching categories: legal, technological, and operational *costs*. Legal costs extend to but are not limited to human resources associated with complying with legal issues arising from the adoption of PETs. For example, in contrast to the implementation and use of general-purpose technologies, PETs are designed to adhere to laws

and regulations regarding collecting and protecting sensitive data. For example, the General Data Protection Regulation(GDPR) is crucial. The EU Charter of Fundamental Rights stipulates that it is impossible to simply share all data because of the right to protect personal data for all EU citizens(European Commission, 2020). Organizations incur costs in ensuring compliance with these regulations, such as time and legal and technical expertise in implementing and designing PETs. Implementation costs include but are not limited to operating and maintaining different software and hardware. For example, organizations would consider supporting contracts, warranties, licenses, and upgrade costs. PETs are generally complex in their implementation, as technical problems, possible data leakages, plug-ins, or installation constantly need to be handled to ensure interoperability (Rossnagel, 2010, Borking, 2011). These costs can be further complicated when interoperability with other legacy systems and infrastructures is critical to the success of the PET.

3.4 Risks

Technologies generally have unintended uses or consequences for organizations (Wimelius, 2011). Prior literature suggests that data accuracy might be lost during data processing (Zöll et al., 2021), or relevant information for market analysis is concealed (Acquisti, 2014, Muris, 2004). The risks of PETs are hardly pre-determined since how MPC is used in the organization might depend on the organization's context. For example, risks such as potential *data leaks* from a data breach involving personal data are likely to be important. Encryption and anonymization help reduce the risks of data leaks and thus reduce sensitive data exposure. However, sensitive data can be revealed through regression and data mining techniques (Li & Sarkar, 2014). The potential risk posed by PETs can also be endogenous within the organization, for instance, through accidental leaks of sensitive data by employees, the transmission of data to wrong parties, or even "abuse or misuse of the privacy-intrusive capabilities of technologies" (Klitou, 2014).

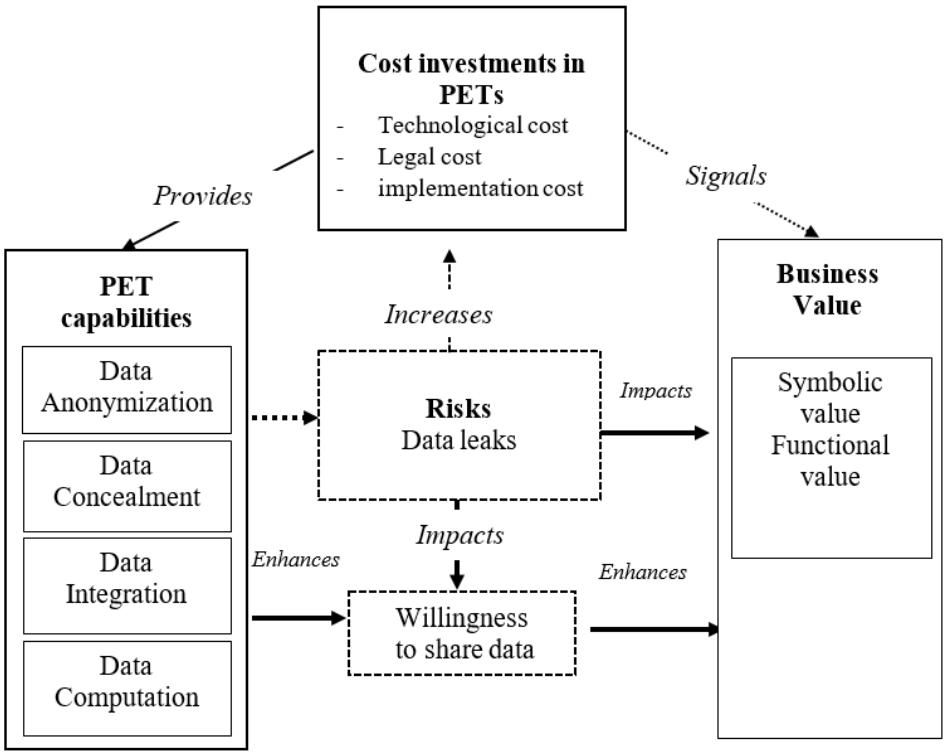

Figure 1: Business Value of PETs

4 Illustrative case

The purpose of the case is to evaluate the applicability of the framework. For this, we selected MPC and the telecommunications industry. We examined the literature on MPC and interviewed experts in telecommunications.

4.1 Multiparty Computation(MPC)

We use MPC as the core technology to evaluate the framework's applicability. MPC enables anonymization, combining, and computation of data from multiple actors. The origin of MPC lies with the millionaire's problem. Two millionaires wanted to know who was the richest securely. They used a specific comparison function to determine who was the richest (Yao, 1982). The two critical aspects of the algorithm had to ensure the privacy of the inputs from the millionaires and safeguard the data against adversaries. Goldreich (1987) and further work by

Goldreich *et al.* (2019) developed the two-party computation protocol into a multi-party one. Yao (1982) and Goldreich (1987) both used Oblivious Transfer(Evans *et al.*, 2017) as a cryptographic technique within their protocols. A simplified explanation of Oblivious Transfer is that Company A has multiple secret inputs. Company B can select one of them. The function of the protocol will not reveal which one of the secret inputs Company B selected, and it will also not reveal what the other inputs were(Evans *et al.*, 2017).

In oblivious transfer became the cornerstone for MPC technology. Multiple parties hold their private share of a value to recover by the participants at the end of the computation. The participants recover their value share using their encryption keys(Beaver *et al.*, 1990). These original schemes have evolved into the current technology of MPC. Lindell and Pinkas (2009,p. 5) state the requirements for such a secure computation are the following: 1) Privacy, 2) Correctness, 3) Independence of inputs, 4) Fairness, and 5) Guaranteed output delivery. These requirements should ensure the correct outcome for parties regardless of dishonest parties (Lam, 2020). Figure 2 shows a general MPC process. Multiple data providers send their encrypted data to the MPC engine. The MPC engine computes and sends the computation results to the authorized parties to receive the data.

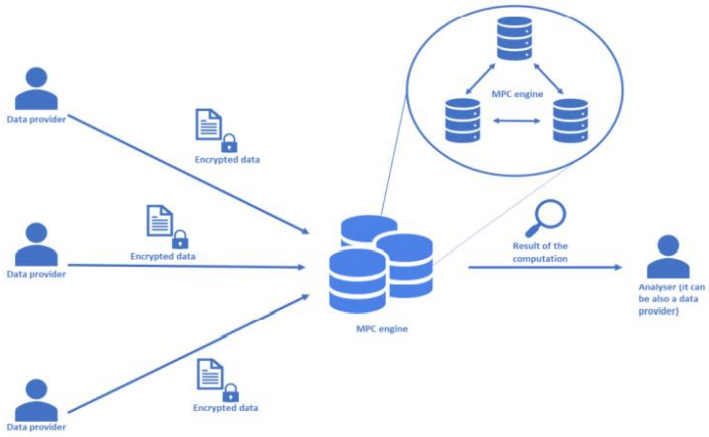

Figure 2: General MPC process (Dolci, 2020,p. 16)

4.2 Research context

We used telecom companies as the context for evaluating the framework applicability. Telecom companies generate and hold sensitive data and are potential candidates for adopting MPC. In addition, telecom companies rely on data as a core aspect of their businesses. They are thus suitable actors in ensuring that privacy issues are addressed. We used semi-structured interviews with recommended experts who had insights into the framework's categories. The semi-structured interviews allowed open questions to stimulate discussions that could enrich the framework. Details of the experts interviewed are provided in table 1.

Insert table 1 here

4.3 Framework Evaluation

A general background of MPC was discussed with experts to ensure a common understanding of MPC. The interview was framed broadly to enable experts to share their opinions on business impacts, cost, and risk of MPC for their organization. For example, experts were asked to provide insights into (1) how/why MPC might affect domains in their organization? (2) What aspect of MPC impact was most important for their company and why? (3) Which aspects were missing or should be excluded from the framework and why? (4) Are there any insights that you believe to be relevant for the economic impact of MPC that was not discussed yet?

These questions were broadly intended to allow experts to discuss business impacts, risk, and cost aspects. For example, questions 1 and 2 were used to stimulate a discussion on potential business value, costs, and risk of MPC specific to different telecom companies. The questions are asked before presenting the framework not to direct them to the already found categories. Experts are asked about their domain to get another point of view on the matter, which could provide new insights into business impact, risk, and cost based on domain(e.g., legal,

technological) expertise. Upon presenting the framework(question 3), experts are asked about their opinion on the framework within telecom companies, if applicable to their expertise. Further interactions or insights from the experts are discussed in question 4. The framework was intentionally not presented before to counter confirmation biases and let the interviewee develop their interpretations. To ensure rigor in our interpretation of interviewees' responses, the authors reflected on the initial framework's constructs to ensure alignment with the framework's constructs. For example, the second author performed the initial interpretation, which the first author subsequently checked.

5 Results

Evaluation of the framework shows that MPC offers potential business value for organizations. The potential business value of MPC included enhancing personalized services**,** predicting market trends, and exploring new markets. MPC's business value for organizations was based on consumers' and organizations' willingness to share data. We describe these four points subsequently.

5.1 Business Value of PETs

Evaluation of the framework indicated that MPC contributes to business performance broadly in enhancing **consumer interaction** and **sales**. From the experts, MPC offers potential business value for telecommunication companies in sales and consumer interaction by enabling better personalizing services, market trends prediction, and exploring new markets and opportunities to collaborate**.** Interviewees indicated that addressing specific market trends and consumers was an essential business value for MPC. For instance, E1, when asked about the most important aspect of MPC's impact on a telecommunication company, stated, 'well, it's always the higher revenue from the new markets you can target.' Furthermore, E1 stated: 'Sometimes you do extensive advertising trying to approach a huge amount of markets or give leaflets in the area that you don't have but has potential. Through MPC and the appropriate collaboration, you can improve this based on the additional information on the consumer.'

Experts indicated that value would be generated for the organization based on **personalized services.** For example, E4 agreed that "MPC could lead to more personalized

services. The more information companies have from a person, the more they can provide a personal service". The exposure to more data will boost the ability to address specific target markets or specific consumers. E3 indicated that "the biggest impact will be addressing specific target markets or specific consumers. It would be great to target geographical areas where we don't have a large market share with specific products". Furthermore, E3 stated, "Suppose companies can provide consumers with the needs they deem relevant. It is possible to bind a consumer to our company. A satisfied consumer will not easily switch to another provider. Brand loyalty is a term that is used in this context." This indicates that MPC could be potential of value in providing target services considered valuable for the consumers.

MPC also enables organizations to **predict market trends**. This is based on additional information on consumers combined with datasets with other complementary actors for market analysis. The ability to predict trends would be improved because of the additional data. For instance, when asked about how they will benefit from MPC, E4 stated, 'To combine with other organizations and work together with them. Marketing as well marketing campaigns and we could even produce new services and new products or play into trends.' The same goes for selling data. They say it would be a possibility, but companies would probably only work with complementary parties. 'Well, in terms of banks, I don't see them ever selling their data. Not ever. In terms of sharing anonymized data, yes, in the future, they maybe will with some specific organizations, mostly public sectors. But I can see smaller companies doing so' [E4].

The benefit gained from predicting trends is also possible because MPC improves the ability to target **new markets.** New data sets can be combined with complementary actors without revealing sensitive data. For example, when asked about how they will benefit from MPC, E3 indicated that "telecommunication companies are quite generic in their marketing because they often supply the whole market and make products for all markets. And it's pretty often consumer marketing. So you could do more targeted marketing if you could share more data".

The capability of MPC to prevent the disclosure of sensitive data also meant organizations could make revenue from **data sales** since data could not be disclosed beyond that. However, the sale of data fostered by MPC could only be valuable when data sales were combined with other complementary services. For example, telecom and large companies benefit from data

sales only when they team with complementary companies rather than competitors. Respondents indicated that small organizations are more likely to trade their data than large companies. “Large telecom and banks will almost in no circumstance sell or trade their data. Especially not to competitors. We will work together with complementary companies. They saw that small businesses might do this “E2

5.2 Cost of PETs

As far as costs are concerned, experts indicated that **legal costs, technology costs, and organizational costs** are relevant for MPC implementation. For example, E1 stated that “legal costs would not be high based on the vast size of their company.” There are two ways the legal costs are influenced. The first is making the data GDPR compliant. The second is making sure all the internal processes are done correctly due to the sensitivity of the data, ‘legal costs will indeed go up. Because the data needs to comply with GDPR, and those rules are quite strict’ [E3].

Technology costs included implementation costs that included recruiting new employees with expert knowledge of the technology and ensuring interoperability with technical systems. E4 stated that “It[MPC] gets costly because it has to be implemented into your CRM (customer relationship management) systems, your provisioning systems, and the whole machinery.” Another cost includes **operational costs**. E2 indicated that “you need to make sure you have the platform working. You need to have the systems in place. Running this system and developing it could be a cost element[….] people need to rely on it, so it needs to be working 100% all the time. There might be some quality issues related to that. Or quality requirements that you have to fulfill. That will increase costs”.

5.3 Risks

Interviewees indicated that MPC is vulnerable to **data leaks.** E3 stated, “data leaks are a big risk, and also your **reputation** will be at risk even if you meet all the GDPR requirements.” The reputational risk is pronounced in the context of telecom firms since they handle data. Experts indicated that data leaks open the company to fines and legal suits. The fines can, for instance, come from not complying with GDPR anymore. ‘The customer may not have given consent to have this data shared with another company. That will be a non-compliance of GDPR, and that

will result in fines' [E3]. This aspect is therefore still included in the framework. To deal with data leaks, interviewees indicated a need to ensure MPC is reliable for companies.

Furthermore, "people need to be able to rely on it[MPC]. So it needs to be working 100 percent all the time[….]. You need to be very careful and very clear about what is happening. It is sometimes difficult to change the perception of some things. Some people do not like that anything is done with their data which can be very difficult to counter." [E3]

Experts also indicated that **trust** among partners using any shared data was critical. For example, other parties could use the data for other secondary uses beyond what was initially allowed when consent was granted for the data. Stating E1' You never trust the other party fully, never, no matter what. So you have to trust the application and internal processes.' The computations should be made with complementary companies and not competing companies. However, a company could take a risk and collaborate with a competitor if they estimate to come out on top. This could result in a profit and cost market share if the competitor benefits more than predicted. Another risk is that big companies could use their scale to their advantage. They have more data and can acquire more data to grasp a more significant market share. The niches could then still be targeted by smaller companies. The smaller companies should ask how they want to work with more prominent companies.

5.4 Summary of Results

Based on the evaluation of the framework and the results, we refine the initially proposed framework by providing specific ways in which PETs create business value for organizations. For example, through the interviews, we identify specific aspects of symbolic and functional value that contribute to the business value of MPC. In addition, through interviews and results, we identified new risks (e.g., reliability on MPC and reputational risk) that were not initially included in our framework. These new considerations served as a basis for us to refine the framework.

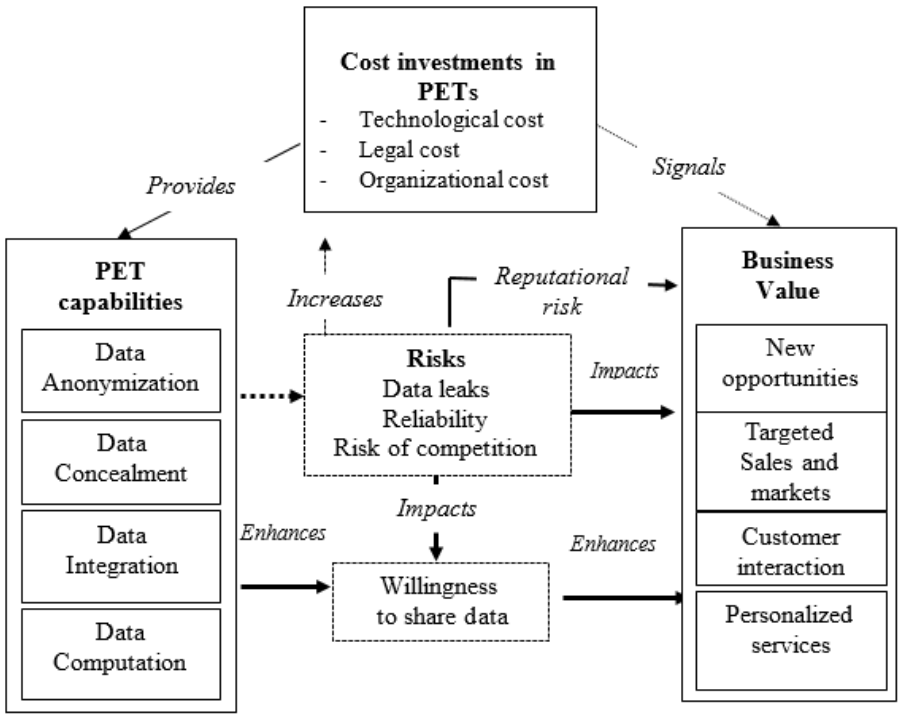

Figure 3: Refined Framework of PET Business Value

6 Discussion

Investing in PETs is critical as more pervasive and intrusive technologies collect sensitive consumer data. Little research has explored the business value of PETs for organizations. This paper explored the business value of PETs. We did so by proposing a framework, drawing insights from the literature on privacy and information technology's impact (symbolic and functional) on the performance of organizations. To evaluate the framework's applicability, we use an illustrative case based on multi-party computation (MPC) use within the telecommunications industry. Our proposed framework provides factors relevant to advance knowledge on PETs' business value. Our framework's factors (e.g., trend prediction, personalized services, targeted sales, customer interactions, and brand reputation) form a basis for future quantitative studies examining PETs' business value. Future studies can extend the framework to consider other factors since privacy concerns vary across contexts (Bansal and Zahedi, 2008, Acquisti *et al.*, 2016). We next discuss the findings from the framework evaluation.

6.1 The Business Value of PETs

Evaluation of the framework suggests that MPC provides business value for organizations. The business value is based on MPC enhancing the willingness of consumers and organizations to share data after MPC is adopted. For example, respondents indicated MPC would create opportunities to collaborate with others since exchanged data would not be exploited negatively. Using MPC, interviewees indicated that consumers would be more willing to share their data and interact with the company since their privacy is protected and anonymized. The exchange of business and personal data is valuable for companies to explore new opportunities and insights into consumers, market trends, and personalized services. Consistent with prior studies, e.g., Acquisti and Varian (2005), the provision of more personalized services is a benefit when consumers share data. The possibilities (e.g., sharing and computing data anonymously) and perceptions of bad actors or competitors not likely to exploit the data spur organizations to consider MPC valuable. For example, by having the expectations that consumers are more willing to share their data because of the assumed empowerment of control over their data.

MPC's capability to conceal sensitive data potentially provides opportunities for organizations to engage in the sale of data. The opportunity for data sales arises from users being more willing to interact and share data with the organization. Even if such data is shared, it still needs other complementary resources. For example, some respondents indicated that sales from data needed to be combined with complementary services that could help the organization. Organizations will use the data to predict market trends or develop more targeted adverts for consumers.

6.2 The Costs of PETs

Our results show that MPC adoption entails considering the costs involved. These costs stem from implementation legal and operational efforts. Legal costs are primarily due to the need for an organization to ensure that they comply with GDPR and other legal requirements. Failure to meet such legal requirements was argued could result in fines. These findings are consistent with prior studies showing that implementing PETs entails complying with legal and technological costs to ensure interoperability (Borking, 2011).

6.3 The Risks of PETs

Evaluation of the framework shows that PETs are also vulnerable to risks. Most experts indicated that data leaks were critical. The possibility of data leaks meant that organizations had to ensure the technology was up-to-date. A key consequence of data leaks was the reputational damage to the company's image. An effect is that the company will incur legal fines, which become even more costly for the company's image when the leaks directly affect sensitive consumer data. One can argue that anonymizing could help reduce the sensitivity of the data leaked. However, this is generally not the case, as new de-anonymizing methods are increasingly applied to leaked data. The experts' concerns about data leaks are similar to the findings of previous studies. For example, based on a real-world social network dataset Li *et al.* (2017) found that 39.9 percent of sensitive information about users was disclosed through de-anonymization using a Novel Heterogeneous De-anonymization Scheme (NHDS).

6.4 Research and Practical Implications

The results of our study have implications for research exploring the business value of privacy-preserving technologies. First, we find that while MPC is considered valuable, its value is likely to arise not directly from the technology itself but from the impact or perception it creates for users to be willing to share their data. This means that research focusing on the business value of privacy-preserving technologies should look beyond its immediate implementation when assessing its economic impact. Instead, emphasis should be put on signaling to consumers and other organizations that their data is protected. In this way, organizations might be willing to collaborate with other organizations since they believe their data is protected. Furthermore, with the implementation of MPC, it is essential to note that MPC does not resolve all risks associated with data sharing. Data could equally be leaked, creating potential reputational risks for the organization. Thus, research exploring new risks that are created with the implementation of privacy-preserving technologies is essential to advance understanding of the business value of PETs. PETs do not entirely solve concerns around risk or trust needed to stimulate data sharing.

The results of our study have implications for organizations considering PETs. Practitioners can use the framework provided in this study as an initial starting point to guide their decision on implementing privacy-preserving technologies. While MPC provides organizations the assurance of protecting sensitive data, trust remains a paramount concern that hampers organizations from sharing data. Respondents indicated that trust between parties sharing data is needed, irrespective of MPC implementation. For example, respondents indicated that even in concealing sensitive data, organizations could use shared data for purposes beyond what was stipulated by the partner. Thus, besides MPC's technical capabilities, trust-building measures among organizations are needed for generating business value from PETS. Accordingly, our study suggests that practitioners must also consider risks such as data leaks, which negatively affect their organization's reputation.

6.5 Conclusions, research limitations, and future research

This paper proposed a framework to study the business value of PETs for organizations. We evaluated the framework applicability using MPC as a specific instance of PET in the context of the telecommunication industry. We identified specific instances of how MPC creates value. The findings show that MPC's business value is mainly driven by the exposure of more data for organizations to leverage to enhance personalized services and predict market trends. The finding also shows the risk and cost associated with MPC adoption.

Our study was limited to the telecom sector and focused on MPC as an instance of PET. Thus, our results should be interpreted with some caution. Further studies should be conducted to explore the benefits of other PETs and MPC. Future research could assess if this framework is also helpful for implementing other types of PETs. Our framework provides factors to be used in future studies on quantifying the impact of PETs. We hope our framework provides an overarching reference for organizations considering the adoption of PETs.

7 References

Acquisti, A. (2010). The economics of personal data and the economics of privacy.
Acquisti, A. (2014). The economics and behavioral economics of privacy. *Privacy, big data, and the public good: Frameworks for engagement,* 1**,** pp. 76-95.
Acquisti, A., John, L. K. & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies,* 42 (2)**,** pp. 249-274.
Acquisti, A. & Spiekermann, S. (2011). Do interruptions pay off? Effects of interruptive ads on consumers' willingness to pay. *Journal of Interactive Marketing,* 25 (4)**,** pp. 226-240.
Acquisti, A., Taylor, C. & Wagman, L. (2016). The economics of privacy. *Journal of economic Literature,* 54 (2)**,** pp. 442-92.
Acquisti, A. & Varian, H. R. (2005). Conditioning prices on purchase history. *Marketing Science,* 24 (3)**,** pp. 367-381.
Bansal, G. & Zahedi, F. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *ICIS 2008 Proceedings***,** pp. 7.
Beaver, D., Micali, S. & Rogaway, P. The round complexity of secure protocols. Proceedings of the twenty-second annual ACM symposium on theory of computing, 1990. 503-513.
Benlian, A. & Hess, T. (2011). The signaling role of IT features in influencing trust and participation in online communities. *International Journal of Electronic Commerce,* 15 (4)**,** pp. 7-56.
Bennett, A. & Chakravarti, A. (2009). The self and social signaling explanations for consumption of CSR-associated products. *ACR North American Advances*.
Blattberg, R. C. & Deighton, J. (1991). Interactive marketing: Exploiting the age of addressability. *Sloan management review,* 33 (1)**,** pp. 5-15.
Borking, J. J. (2011). Why adopting privacy enhancing technologies (pets) takes so much time. *Computers, privacy and data protection: an element of choice.* Springer.
Calzolari, G. & Pavan, A. (2006). On the optimality of privacy in sequential contracting. *Journal of Economic theory,* 130 (1)**,** pp. 168-204.
Chan, E. Y. & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior,* 119**,** pp. 106718.
Chen, H., Laine, K. & Rindal, P. Fast private set intersection from homomorphic encryption. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017. 1243-1255.

Chen, J. V., Ross, W. & Huang, S. F. (2008). Privacy, trust, and justice considerations for location-based mobile telecommunication services. *info*.

Chod, J., Trichakis, N., Tsoukalas, G., Aspegren, H. & Weber, M. (2020). On the financing benefits of supply chain transparency and blockchain adoption. *Management Science,* 66 (10), pp. 4378-4396.

Connelly, B. L., Certo, S. T., Ireland, R. D. & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of management,* 37 (1), pp. 39-67.

Culnan, M. J. (1993). "How did they get my name?": an exploratory investigation of consumer attitudes toward secondary information use. *MIS quarterly*, pp. 341-363.

Danezis, G. & Gürses, S. (2010). A critical review of 10 years of privacy technology. *Proceedings of surveillance cultures: a global surveillance society*, pp. 1-16.

Diaz, C. & Gürses, S. (2012). Understanding the landscape of privacy technologies. *Proceedings of the information security summit,* 12, pp. 58-63.

Dolci, R. (2020). Realising platform control in data marketplaces through Secure Multi-Party Computation: A qualitative study exploring the use of Secure Multi-Party Computation (MPC) as an instrument for realising platform control in data marketplaces.

European Commission 2020. The European Data Strategy, (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN) accessed on 5 Nov. 2021 at 22:28.

Evans, D., Kolesnikov, V. & Rosulek, M. (2017). A pragmatic introduction to secure multi-party computation. *Foundations and Trends® in Privacy and Security,* 2 (2-3).

Fogel, J. & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior,* 25 (1), pp. 153-160.

Ghanem, S. M. & Moursy, I. A. Secure Multiparty Computation via Homomorphic Encryption Library. 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS), 2019. IEEE, 227-232.

Goldberg, I. (2007). *Privacy-enhancing technologies for the internet III: ten years later*, Auerbach Publications.

Goldreich, O. Towards a theory of software protection and simulation by oblivious RAMs. Proceedings of the nineteenth annual ACM symposium on theory of computing, 1987. 182-194.

Goldreich, O., Micali, S. & Wigderson, A. (2019). How to play any mental game, or a completeness theorem for protocols with honest majority. *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali.*

Grover, V., Chiang, R. H., Liang, T.-P. & Zhang, D. (2018). Creating strategic business value from big data analytics: A research framework. *Journal of Management Information Systems,* 35 (2), pp. 388-423.

Hartmann, P. & Apaolaza-Ibáñez, V. (2012). Consumer attitude and purchase intention toward green energy brands: The roles of psychological benefits and environmental concern. *Journal of business Research,* 65 (9), pp. 1254-1263.

Jozani, M., Ayaburi, E., Ko, M. & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior,* 107, pp. 106260.

Klitou, D. (2014). New Privacy Threats, Old Legal Approaches: Conclusions of Part II. *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century.* The Hague: T.M.C. Asser Press.

Kohli, R. & Grover, V. (2008). Business value of IT: An essay on expanding research directions to keep up with the times. *Journal of the association for information systems,* 9 (1), pp. 1.

Lam, J. (2020). Scenario Analysis of Secure Multi-party Computation implementation in EU-based multinational banks.

Lee, D.-J., Ahn, J.-H. & Bang, Y. (2011). Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. *Mis Quarterly*, pp. 423-444.

Li, H., Chen, Q., Zhu, H., Ma, D., Wen, H. & Shen, X. S. (2017). Privacy leakage via de-anonymization and aggregation in heterogeneous social networks. *IEEE Transactions on Dependable and Secure Computing,* 17 (2), pp. 350-362.

Li, X.-B. & Sarkar, S. (2014). Digression and value concatenation to enable privacy-preserving regression. *MIS quarterly: management information systems,* 38 (3), pp. 679.

Lindell, Y. & Pinkas, B. (2009). A proof of security of Yao's protocol for two-party computation. *Journal of cryptology,* 22 (2), pp. 161-188.

Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research,* 15 (4), pp. 336-355.

Mata, F. J., Fuerst, W. L. & Barney, J. B. (1995). Information technology and sustained competitive advantage: A resource-based analysis. *MIS quarterly*, pp. 487-505.

Melville, N., Kraemer, K. & Gurbaxani, V. (2004). Information technology and organizational performance: An integrative model of IT business value. *MIS quarterly*, pp. 283-322.

Muris, T. J. (2004). The Federal Trade Commission and the future development of US consumer protection policy. *George Mason Law & Economics Research Paper,* (04-19).

Paine, C., Reips, U.-D., Stieger, S., Joinson, A. & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies,* 65 (6), pp. 526-536.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS quarterly*, pp. 977-988.

Posner, R. A. (1977). The right of privacy. *Ga. L. Rev.,* 12, pp. 393.

Posner, R. A. (1981). The economics of privacy. *The American economic review,* 71 (2), pp. 405-409.

Rossnagel, H. The market failure of anonymity services. IFIP International Workshop on Information Security Theory and Practices, 2010. Springer, 340-354.

Schiffner, S., Berendt, B., Siil, T., Degeling, M., Riemann, R., Schaub, F., Wuyts, K., Attoresi, M., Gürses, S. & Klabunde, A. Towards a roadmap for privacy technologies and the General Data Protection Regulation: A transatlantic initiative. Annual Privacy Forum, 2018. Springer, 24-42.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, pp. 989-1015.

Smith, H. J., Milberg, S. J. & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, pp. 167-196.

Soh, C. & Markus, M. L. (1995). How IT creates business value: a process theory synthesis. *ICIS 1995 Proceedings*, pp. 4.

Spence, M. (1978). Job market signaling. *Uncertainty in economics.* Elsevier.

Stone, E. F., Gueutal, H. G., Gardner, D. G. & Mcclure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology,* 68 (3), pp. 459.

Taddicken, M. (2014). The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on

different forms of self-disclosure. *Journal of Computer-Mediated Communication,* 19 (2), pp. 248-273.
Tsai, J. Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information systems research,* 22 (2), pp. 254-268.
Tucker, C. E. (2012). The economics of advertising and privacy. *International journal of Industrial organization,* 30 (3), pp. 326-329.
Van Der Vlist, F. N. & Helmond, A. (2021). How partners mediate platform power: Mapping business and data partnerships in the social media ecosystem. *Big Data & Society,* 8 (1), pp. 20539517211025061.
Van Dyke, T. P., Midha, V. & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets,* 17 (1), pp. 68-81.
Wang, H., Lee, M. K. & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM,* 41 (3), pp. 63-70.
Wimelius, H. 2011. *Duplicate systems: investigating unintended consequences of information technology in organizations.* Institutionen för informatik, Umeå universitet.
Wirtz, J., Lwin, M. O. & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of service industry management*.
Yao, A. C. Protocols for secure computations. 23rd annual symposium on foundations of computer science (sfcs 1982), 1982. IEEE, 160-164.
Zöll, A., Olt, C. M. & Buxmann, P. 2021. Privacy-sensitive Business Models: Barriers of Organizational Adoption of Privacy-Enhancing Technologies. *European Conference on Information Systems(ECIS).* Marrakech-Morocco.
Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology,* 30 (1), pp. 75-89.