Agahari, Wirawan; Petronia, Masud; de Reuver, Mark

Conference Paper

Cutting out the trusted third party in business-to-business data exchange: A quantitative study on the impact of multi-party computation on firms' willingness to share sensitive data in supply chains

23rd Biennial Conference of the International Telecommunications Society (ITS): "Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world", Online Conference / Gothenburg, Sweden, 21st-23rd June, 2021

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Agahari, Wirawan; Petronia, Masud; de Reuver, Mark (2021) : Cutting out the trusted third party in business-to-business data exchange: A quantitative study on the impact of multi-party computation on firms' willingness to share sensitive data in supply chains, 23rd Biennial Conference of the International Telecommunications Society (ITS): "Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world", Online Conference / Gothenburg, Sweden, 21st-23rd June, 2021, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/238001

Cutting out the trusted third party in business-to-business data exchange: A quantitative study on the impact of multi-party computation on firms' willingness to share sensitive data in supply chains

Research Paper

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

Masud Petronia
Delft University of Technology
Delft, the Netherlands
mnpetronia@hotmail.com

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

Abstract

Many firms hesitate to share data via a Trusted Third Party (TTP) due to the risk of exposing sensitive information to competitors. Multi-party computation (MPC) is a cryptographic technology that removes the need for TTPs in data sharing, as it allows conducting computations without having to disclose the underlying datasets. While MPC could resolve certain data-sharing barriers, it is uncertain under what conditions business actors prefer MPC over TTP-based data sharing. This paper explores how MPC affects organizational willingness to share sensitive data for collective purposes, focusing on Internet-of-Things (IoT) data within supply chains. We conduct an online experiment on 106 participants representing decision-makers in logistics organizations. We find that participants are more willing to share sensitive data via MPC-based applications than conventional TTP applications. Also, MPC significantly increases participants' perception of trustworthiness and security while sharing sensitive data. However, we find no difference in relative advantage between the two applications. Our study implies that technologies like MPC could allow companies to directly share data without trusted third parties, thus leveling the playing field of the data economy. Hence, regulators and policymakers may consider MPC and related privacy-preserving technologies as a way to break the dominance of big tech corporations in the data economy.

Keywords: multi-party computation, data sharing, willingness to share sensitive data, data economy

Introduction

Sharing data between companies brings many benefits: data can be shared and monetized (Koutroumpis, Leiponen, & Thomas, 2020), or it can be shared with other parties to enhance business operations (Huang, Hung, & Ho, 2017; Lotfi, Mukhtar, Sahran, & Zadeh, 2013; Sendhil Kumar & Pugazhendhi, 2012). When data from different entities and domains are combined, new information and knowledge are created and discovered (Guan, Zhang, Zhou, & Dan, 2020), unlocking possibilities for economic growth (Zafrir, 2020). For instance, sharing data within supply chains allow benchmarking for process improvement. However, most firms still refrain from data sharing (European Commission, 2020). Moreover, data sharing currently always requires a Trusted Third Party (TTP), creating a fear of losing sensitive information to competitors by, for instance, using the data to reversely engineer sensitive business processes. With the lack of a functioning market for data, most companies will struggle to compete, especially against the big tech companies, which control substantial masses of data.

Multi-Party Computation (MPC) could become a tool to overcome trust concerns (Zare-Garizy et al., 2018), create new business opportunities (Arnaut, Pont, Scaria, Berghmans, & Leconte, 2018; Koutroumpis et al., 2020), and foster the data economy (European Commission, 2020; Zafrir, 2020). MPC is a cryptographic technique that involves sharing information while not disclosing submitted data between any involved parties (Yao, 1986). In this regard, MPC allows organizations to share data while preserving confidentiality, enabling them to obtain more valuable information (Zhao et al., 2019). Nevertheless, MPC implementation has long remained limited, and only recently, computing resources are sufficient to execute demanding MPC algorithms. Moreover, how MPC affects the business domain regarding data sharing capabilities and value creation remains unclear (Agahari, Dolci, & de Reuver, 2021; Damgård, Damgård, Nielsen, Nordholt, & Toft, 2017; Kerschbaum et al., 2011). Furthermore, from a technology perspective, it is expected that MPC resolves several data-sharing barriers. Still, it is uncertain how business decision-makers perceive this technology.

This paper explores how MPC affects organizational willingness to share sensitive data for collective purposes. To fulfill this objective, we opt for an experimental research design by comparing MPC and TTP as a conventional, non-MPC-based solution. We focus on sharing Internet-of-Things (IoT) data within the supply chain domain, given its highly competitive nature, as barriers like data sensitivity hinder data sharing opportunities (e.g., de Prieëlle, de Reuver, & Rezaei, 2020; Khurana, Mishra, & Singh, 2011).

In section 2, we provide a background on MPC and the supply chain domain. We also develop our conceptual model as a basis to measure MPC's impact on firms' willingness to contribute protected data in this section. Subsequently, we present the demonstration platform in section 3. After that, we elaborate on our experimental design and outline our findings in section 4 and section 5, respectively. Finally, we discuss our results and conclude the deliverable in section 6.

Background

Multi-Party Computation (MPC)

MPC is a powerful instrument because it provides a possible solution to Computation on Encrypted Data (CoED) (Archer et al., 2018). MPC comprises two or more input parties, each with a concealed dataset, whereby they jointly compute an objective functionality (e.g., an application-oriented task such as electronic voting) based on their inputs (Zhao et al., 2019). MPC can be deployed in different frames of reference: between companies within the same domain (e.g., assessing common customers between organizations for marketing purposes), across other units within the same company (e.g., cross-selling), and across supply chain tiers (e.g., streamlining manufacturer-supplier in supply chains).

A popular illustration of MPC is the millionaire's problem (Yao, 1986, a secure comparison function to determine which one of two millionaires is richest, without revealing the net worth to each other. Some real-life examples also exist, like auction-based pricing (Bogetoft et al., 2009), tax fraud detection (Bogdanov, Jõemets, Siim, & Vaht, 2015), and satellite collision prevention (Hemenway, Lu, Ostrovsky, & Welser Iv, 2016). Nevertheless, massive implementations of MPC are yet to happen due to barriers like *usability issues* (i.e., too complex to understand by non-experts, suspicion in the computation results),

technical issues (i.e., performance limitations and scalability), and *legal aspects* (i.e., current regulations discourage cooperation) (Choi & Butler, 2019).

MPC needs to have various security requirements, namely *privacy* (i.e., no party should be able to get information apart from their own), *correctness* (i.e., the output obtained by each party must be correct), *independence of input* (i.e., the input of a corrupted party must be independent of the inputs of the honest parties), *the guarantee of output* (i.e., corrupted parties should not be able to stop honest parties from receiving their own outputs), and *fairness* (i.e., corrupted parties should obtain their outputs if and only if the honest parties obtain their own outputs).

In essence, MPC is deployed in a distributed computing environment (see Figure 1). MPC comprises three actors: (1) *input parties* (IP) who deliver concealed data (i.e., sensitive, confidential, private) to the confidential computation; (2) *the result parties* (RP) who receive results (or partial results) from the confidential computation; and (3) *the independent computing parties* (CP) who jointly computing the confidential computation (Archer et al., 2018).

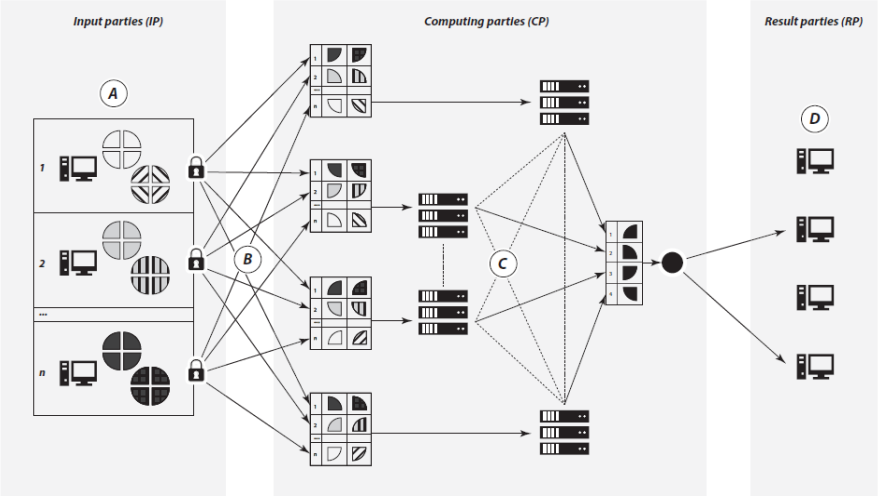

Figure 1. Example MPC application architecture with data flow (adapted from Bestavros et al., 2017; Bogetoft et al., 2009; and Bogdanov et al., 2012)

The data exchange process comprises two phases. The first phase includes submitting and distributing the input (indicators A and B in Figure 1). Data can be, for instance, collected through interfaces such as web-based forms, applets, or other plug-ins. From a practical view, each input interface has different requirements. Nevertheless, IP input data have to be secret-shared at the source. For instance, in Bogetoft et al. (2009), each share is encrypted with a different public key and sent to a storage server. In the case of Bogdanov et al. (2012) (web-based), each share is sent directly to a different proxy server over a secure HTTPS channel. Each interface has other perceived benefits; for example, a web-based form allows application users to authenticate themselves to the application and benefit from the public internet.

The second phase (indicators C and D in Figure 1) comprises the multi-computation part and the distribution results. Typically, MPC participants perform identical instructions dictated by an MPC protocol on the shares they possess. Finally, the output is distributed to the RPs, which does not need to be the same as IPs. The CP environment's architecture needs to protect against the reconstruction of shares to the original input value at the proxy server (e.g., through private and public keys). A requirement is that both IPs and CPs must be independent and incentivized not to collude.

MPC and data sharing in supply chains

Scholars defined a supply chain as an organized system that represents a series of interrelated entities, members, or partners, with different functions directly involved in flows of products, services, information, and finances from and to end-customers (Atallah et al., 2004; Curkovic, Scannell, & Wagner, 2015; Min & Zhou, 2002). Within SC networks, Cooper, Lambert, and Pagh (1997) define Supply Chain Management

(SCM) as "the integration of key business processes from end-users through original suppliers that provide products, services, and information and add value for customers and other stakeholders." Per this definition, SCM encompasses activities at many levels: strategic, operational, and tactical. SCM has become increasingly important due to competitiveness introduced by market globalization, which resulted in a growing interest in dealing with inefficiencies and the uncertainties faced by supply chains' dynamic complexity (Milch & Laumann, 2016). The increasing body of research on supply chain models also confirms this (Min & Zhou, 2002). Supply chain model research aims to advance the frontiers of knowledge to integrate the entire supply chain process successfully. Herein, information serves as a means for Supply Chain Integration (SCI) in decentralized supply chains. More concisely, Lotfi et al. (2013) provide a synthesis of data-sharing benefits in supply chains.

Different theoretical incentives for data-sharing exist. For instance, successful integration can reduce supply chain inefficiencies, such as the well-known 'bullwhip' effect. The bullwhip effect is a phantom market demand, which is amplified due to a lack of information synchronization between supply chain members, which leads to higher operating costs (Li, Shaw, Sikora, Tan, & Yang, 2001). Such issues entail "prices, customer profiles, sales forecasts, and order history" (Min & Zhou, 2002), accounting for strategic, operational, and tactical information.

Evidence for the net outcome in supply chains remains limited with regards to data-sharing efforts within business-enhancing activities. The reason is that the data-sharing landscape faces many barriers. For instance, there are shareable and non-shareable data, and firms can be unwilling or unable to share certain types of data (e.g., Ojha, Sahin, Shockley, and Sridharan, 2019). Concerns may initially arise regarding the purpose of sharing data, and fear of sensitive information leakage may also exist. With such uncertainty, firms may choose to refrain from data sharing. This uncertainty can reflect security concerns, liability concerns, accountability concerns, legislative concerns, and strategic concerns (Khurana et al., 2011). Also, when there is a legitimate purpose for sharing data, there can be a fear of information leakage. When there is uncertainty over outcomes, wrong incentives, and non-aligned goals, firms may also refrain from sharing data (e.g., when both firms have profit-maximizing goals). Finally, because of the complexity of SC/SCN, incentives to share data may be overwhelmed by the unknown risks.

Several general supply chain scenarios are suitable for MPC implementations, according to existing studies. For instance, MPC can facilitate *freight bidding* between carriers and shippers. In this scenario, both parties can match the bid, ask prices, and release information only when there is a match without the need for a trusted third party (cf. Bogetoft et al., 2009). Another scenario involves *performance benchmarking* between organizations that require them to share sensitive data. While the typical scenario includes building trusted networks or using a trusted third party, MPC is also relevant in this case (e.g., Damgård et al., 2017). With MPC in place, benchmarking metrics can be calculated without each party seeing the underlying data. Furthermore, another use case is *risk analysis of SCNs*, which is even more relevant given the increasing complexity of SCNs due to globalization and new business models (e.g., Zare-Garizy et al., 2018). MPC can serve as a means to calculate risks in the network without giving away protected data (e.g., Adhikari, Bisi, and Avittathur, 2020).

Theoretical framework and hypotheses development

We draw upon Inter-Organizational Systems (IOS) literature and conceptualize those factors into the MPC context. The model comprises three factors: (1) perceived trustworthiness, (2) perceived security, and (3) perceived relative advantage. These factors will serve as a basis to develop the conceptual model and hypotheses in the next section.

Perceived trustworthiness

In terms of MPC, trustworthiness refers to the extent to which the MPC is perceived as suitable for providing its stated functionalities according to agreed-upon norms. Trustworthiness is an essential concept within the context of MPC because its presence is not apparent to the Input Party (IP), thus requiring the IP to rely on its perceptions of the system as a whole. Therefore, trustworthiness should be a verifiable property of the system (Feller, 2014). For instance, active security with abort is an MPC property that could result in unexpected opportunistic behavior (Archer et al., 2018). While this behavior can be dealt with through the MPC environment's protocol or infrastructure, this condition is not (clearly) visible to IPs, which act based

on their beliefs of the information provided at the front-end. These aspects relate to the application's perceived trustworthiness. It requires one first to understand the meaning of active security with abort and then understand how this is dealt with by the application and finally deciding if this satisfies their requirements.

Trustworthiness is associated with risk (Hart & Saunders, 1997). In the MPC context, we consider the risks perceived by potential adopters with trying "something new," which is associated with uncertainties due to the application's complexity, divisibility, and observability. As a result, it is assumed that when one agrees to use MPC, it is likely the result of a positive view of these factors.

For this paper, we argued that the system's trustworthiness is imperative for understanding the willingness to use the MPC application. We base this argument on the extreme case of using an MPC in an environment with unknown participants, requiring input parties to rely on their perceptions of the system itself. Besides, the system's trustworthiness is expected to increase the level of trust one lays in other (unknown) contributors' behavior. For instance, system integrity prevents inconsistencies, positively affecting others' predictability (Raj et al., 2014).

Perceived security

Security refers to the degree to which the mechanisms of the technology are perceived to protect against harm despite risks posed by outside threats (Abomhara & Køien, 2014). At a fundamental level, usually, security concerns protecting assets of value to an organization. In the context of MPC, security is defined from the view of possible attacks, which may aim to discover others' sensitive information or disrupt computation tasks (based on protocols). Researchers have proposed several security definitions to prove that a protocol is secure, which mainly attempts to guarantee several security requirements, including (but not limited) to privacy, correctness, independence of input, a guarantee of output, and fairness. The standard definition of security in the MPC literature is based on these requirements.

However, unlike real or technical security, perceived security is a psychological concept. From a physiological perspective, perceived security plays a vital role in users' behaviors related to technology. According to Zhang, Reithel, and Li (2009): "Perceived security protection mechanism refers to one's perception of the existence and effectiveness of hardware, software, and physical security protection." In the context of MPC, perceived security relates to the degree to which contributors believe that their submitted data is kept confidential in the knowledge-sharing process. To examine perceived security in the context of MPC, we assume that we can apply the general (cognitive) determinants of perceived security in information systems.

Past research showed perceived control as an effective measure to increase perceived security (Huang et al., 2011). Perceived control is the extent to which one feels in control of a situation. It is the difference between 'real' security and the belief about security. Although perceived control falsely indicates one's actual control, perceptual control influences behavior significantly (Chang, 2010; Wu, Wang, & Huang, 2010). Besides, with MPC, it is assumed that (non-technical) users do not fully understand security control's technical mechanisms.

Thus, perceived control is determined by the interface's information or functions (or information control (Skinner, 1996). These include: "explicit information, choice, warning signals, regulated administration, help, feedback, and instructions and, depending on how they are provided, may or may not achieve the intended effect of changing the actual amount of control present (objective control conditions) or the individual's perceptions of control" (Skinner, 1996, p. 558). In de Reuver, Fiebig, Agahari & Faujdar (2019), we found the effect of information presentation and the perception towards the application. Therefore, perceived control has a positive effect on the perceived security of MPC-enabled applications.

Perceived risk is another phenomenon that affects perceived security, particularly in protecting organizational assets (i.e., the sensitive data) from loss or disclosure. Following Pavlou & Gefen (2004), perceived risk in data sharing is described as the perception of an organization that there is a likelihood of suffering a loss when sharing data with other organizations. In the context of adopting information security technology, managerial perception of risk is highly dependent on the degree of uncertainty in data sharing, including possible negative consequences (Chang, 2010). Ultimately, managers have high expectations when considering security solutions due to high perceived risk.

Perceived relative advantage

In the context of MPC, the relative advantage is viewed from the perspective of data sharing advantage, consistent with Kanger and Pruulmann-Vengerfeldt (2015). Consequently, relative advantage refers to the extent to which MPC can be used to solve data-sharing cases relative to non-MPC solutions. To give an illustration, when assuming a secure platform for data exchange, strictly speaking, this platform may not be used since the advantage it provides to alternatives is not defined (not known to users). This argument aligns with Kanger and Pruulmann-Vengerfeldt (2015), which points out that organizations might perceive other solutions as better alternatives. In other words, when MPC is perceived to provide a low level of advantage (e.g., low security and/or no viable solution to the matter at hand) compared to other alternatives, it may not be considered a solution for the given activity.

Hypotheses development

Willingness to share sensitive data

We develop a theoretical model on the antecedents of data sharing through MPC. In this paper, we discuss MPC as an enabler to share sensitive data. Given the primary aim of MPC and its several successful deployments, we expect that, compared to conventional Trusted Third Party (TTP), MPC increases firms' willingness to share sensitive data–when properly presented. Thus, we propose the following hypothesis:

> **H1: Firms are more willing to share sensitive data through an MPC-based application than through a TTP-based application.**

Perceived trustworthiness

No party is expected to share sensitive data through an MPC application, which is perceived as untrustworthy. Although we have argued that trust between the different parties becomes less relevant, the application owner (or "the MPC application service provider") is still essential. A form of partnership is established where the trustor (contributor) becomes dependent on the trustee (the application owner). In the context of partnership, Zaheer and Venkatraman (1995) characterize trust-based dependability, predictability, and faith. Even though this construct of trust is based on strategic partnerships, it can be conceptualized in terms of an MPC application: dependability refers to one's beliefs that the application is designed to function in the best interest of the contributors; predictability refers to the belief that the application functions according to claims made, and; faith refers to the belief that the trustee does not behave opportunistically. Thus, a positive perception of trustworthiness as a construct comprised of these three components is required for contributing data over an MPC application. However, we should note that faith relates to the service provider. Our key takeaway from the above is that an application's perceived trustworthiness is an essential item of consideration. Therefore, we propose the following hypothesis:

> **H2: Perceived trustworthiness of an MPC-enabled application is greater than the perceived trustworthiness of a TTP-based application.**

Perceived security

MPC is, in broad terms, a security technology. However, there is no international or widely accepted security criteria or standard at this point. Therefore, when managers are faced with this emerging technology, it is expected that they are more likely to base their judgment on their perception. Given that the value of MPC in terms of security is not apparent to companies, emphasis on perception is further enhanced. As a result, whether one will contribute protected data via MPC is, to a great extent, determined by the perceived security of MPC. In fact, security is perceived as the main goal of MPC. Therefore, the direct primary utility provided by MPC is its ability to enable confidential data sharing. Thereby, it is unlikely that an organization contributes protected data in case of negative perceptions of security. As a result, the conjecture is that perceived security, to a great extent, determines the willingness to contribute data via MPC.

In de Reuver et al. (2019), we found that the effect that MPC has on perceived security–to a great extent–is determined by the presentation of the technology. We can explain this relationship through the lens of the Communication Privacy Management Theory (CPMT), which is rule-based and posits costs (e.g., risk) and benefits (e.g., usefulness) that individuals develop to aid in decisions about whether to disclose private

information. Although CPMT is limited to the individual level (e.g., see Petronio (1991)), the concept of boundary rule formation (boundary management) (Petronio, 2013) is borrowed. Conceptualized in terms of MPC, MPC can provide a means for boundary management and lower perceived risk and increase perceived control. Altogether, we hypothesize that:

> **H3 : Perceived security of an MPC-enabled application is greater than the perceived security of a TTP-based application.**

Perceived relative advantage

The importance of relative advantage on willingness to contribute data via MPC depends on the degree of familiarity with conventional data transactions or interoperability issues. What can also affect the willingness to share sensitive data via MPC is the degree to which a party needs to share but is faced with technological barriers. As Kanger and Pruulmann-Vengerfeldt (2015) point out, if the perceived relative advantage of MPC does not seem pressing to the organization, they might not consider MPC for the given task. To some extent, this is similar to "perceived benefits" in the boundary rule formation (Petronio, 2013), in which it affects willingness to disclose personal information.

A person (or organization) may be willing to contribute data through MPC, depending on the type of shared data. Whether this person/organization views MPC as a solution depends on whether he/she perceived the advantage provided by MPC concerning alternatives (i.e., the relative advantage of MPC). However, if one is not familiar with conventional data transactions or interoperability issues, they may not perceive an advantage from the use of MPC. The reason is that they are not aware of the implications of conventional data-sharing solutions. In such a case, the perceived relative advantage is opaque and might not significantly affect the willingness to contribute through MPC. Since there is no clear direction on the effect of MPC on relative advantage, we propose the following hypothesis:

> **H4 : There is no difference in terms of perceived relative advantage between an MPC-enabled application and a TTP-based application.**

Research approach

To examine the effect of MPC on the willingness to share sensitive data, we conducted a controlled experiment to compare participant groups and measure the degree of change stemming from the treatment. To do this, we develop mock-ups of two identical applications that reflect two experimental conditions: the Trusted Third Party (TTP) and the MPC-based application. The differences between the two mock-ups are that the MPC group provides (1) a generic high-level introductory video to MPC (available at http://bit.ly/IntroMPC) and (2) an animated MPC illustration (see Figure 2), which are necessary as we expect participants to have little to no knowledge of MPC.

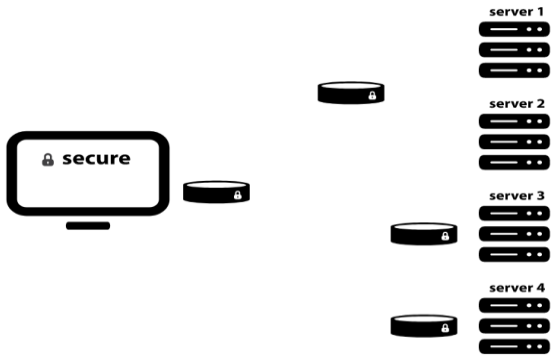

Figure 2. The animated MPC illustration presented in the MPC-based application

The participants are decision-makers within organizations with roles like technology managers, business strategists, improvement managers, IT advisors, program managers, project managers, and project engineers. We collect responses in July and August 2020 via an online crowdsourcing platform (N=98) using education level (undergraduate, graduate, and doctorate) and industry role (upper management,

trained professional, middle management, and junior management) as a custom prescreening to filter out our participants. We also distribute the experiment through our networks (N=8). The final sample consists of 106 respondents, ranging from 21 to 54 years old, with an average age of 33 years and a standard deviation of 7.05. The majority of participants are skilled professionals (73.5%), while more than 90 percent possess an undergraduate degree or higher. As expected, out of 53 participants assigned to the MPC group, more than 60% are unfamiliar with it.

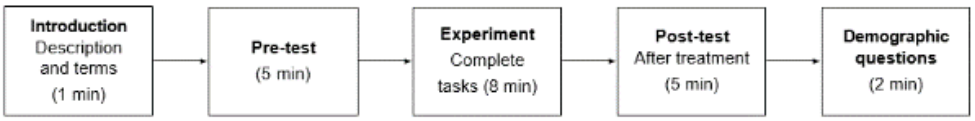

Figure 3. The experiment process flow

The complete experiment process flow has five parts (see Figure 3). First, participants are provided with an introduction to the study and provided with terms for conducting the experiment. Then, we presented all participants with the pre-test to measure participants' expectations for a data-sharing application. The pre-test is perfectly identical for both groups. Next, we presented participants with the experimental treatment by randomly assigning them to one group (MPC or TTP group). In both groups, we introduced participants to a persona where they became a manager of an e-commerce distribution center that needs to improve delivery times. We asked participants to performed several tasks that resemble the usage of the data sharing application, in which they need to share sensitive IoT data. We then asked participants to upload the input data and describe what happens to the data after submission. After completing the tasks, we presented participants with a post-test to rate their perceptions of the application. The experiment finished with the demographic questions, which are the same for the two groups.

As for the measurement items, since there are no similar quantitative studies on the impact of MPC on willingness to share data, scales are not yet available. Hence, we developed the measurement items based on existing literature on perceived trustworthiness, perceived security, and perceived relative advantage (see the theoretical background section). We list our survey items in the appendix. Several questions (marked by an asterisk) can only be asked during the post-test. In each survey item, respondents will rate their score using a 5-point Likert scale.

Results

We performed an independent T-test to test our hypotheses by comparing perceived trustworthiness, perceived security, perceived relative advantage, and willingness to share sensitive data while using MPC and TTP (See Table 1). Upon running the independent t-test, in some cases, Levene's test indicates that the two groups' variances are not equal. Put differently; the significance suggests that the assumption of homogeneity of variance is violated. Given that we acquired the data from the same population and that the sample sizes are the same size, there is a good reason to ignore Levene's test results (Stevens, 2016, ch. 6). Therefore, we ran the t-tests using bootstrap (robust test) (Field, 2017, ch. 10).

Variables		MPC	TTP	t-value	p	Results
Perceived trustworthiness	M	3.85	3.59	t(104) = 1.74	0.04 (one-tailed)	Significant
	SD	0.10	0.11			
Perceived security	M	4.15	3.34	t(104) = 5.76	<0.001 (two-tailed)	Significant
	SD	0.11	0.09			
Perceived relative advantage	M	3.94	3.92	t(93.6) = 0.15	0.88 (two-tailed)	Not Significant
	SD	0.07	0.10			
Willingness to share sensitive data	M	3.92	3.60	t(95.5) = 2.37	0.02 (two-tailed)	Significant
	SD	0.08	0.11			

Table 1. Comparison between MPC and TTP

In testing H1 (*willingness to share sensitive data*), we first performed a Bayesian comparison of means for testing the effect sizes for the two independent means (two experimental groups). On average, participants

given an MPC application (N=53) are more willing to share sensitive data (M=3.92, SE=0.08) than those given a TTP application (N=53) (M=3.60, SE=0.11). We set the prior distributions for the group means to a mean of 3 and a standard deviation of 0.35 for the TTP group, and a mean of 4 and a standard deviation of 0.35 for the MPC group. The Bayes factor was estimated using Gönen's method with a prior difference between means of 1 with a variance of 0.25. The Bayesian estimate of the true difference between means was 0.31, 95% confidence interval [0.08, 0.59]. The associated Bayes factor, BF01=3.14, suggested that the data were moderately more probable under the alternative hypothesis than the null.

Then, we performed an independent T-test using bootstrap. The result suggests that the homogeneity of variance assumption was not met (p= 0.001). On average, participants given an MPC application (N=53) are more willing to share sensitive data (M=3.92, SE=.080) than those given a TTP application (N=53) (M=3.60, SE=0.11). This difference, 0.32, bias-corrected and accelerated (BCa) 95% confidence interval (CI) [0.05, 0.59], was significant (t(95.5)=2.37, p=0.02), and a Cohen's d effect of d=0.46 represents a 'medium' effect size. Thereby we find evidence to *support hypothesis H1*.

Like the willingness to share sensitive data, we measure the overall perception of trustworthiness, relative advantage, and security in the post-test. Thus, measuring the effect of MPC over TTP is done similarly to the above. We did not perform the Bayesian comparison of means here since we have no prior estimates.

In testing H2 (*perceived trustworthiness*), the robust test result indicates that the homogeneity of variance assumption was not met (p=0.06). On average, participants given an MPC application (N=53) perceive a higher level of trustworthiness (M=3.85, SE=0.10) than those given a TTP application (N=53) (M=3.59, SE=0.11). This difference, (0.26, 95% confidence interval (CI) [-0.04, 0.57]), was not significant (t(104)=1.74, p=.09). Based on the two-tailed results, we cannot accept the alternate hypothesis.

However, to avoid making a type two error and increase power, a one-tailed approach is used. The critical values are t(104)[one-tailed]=1.66, and t(104)[two-tailed]=1.98. In SPSS, an independent t-test is used with a 90% confidence interval (one end of the distribution). The results of the one-tailed test indicate that, on average, participants given an MPC application (N=53) perceive a higher level of trustworthiness (M=3.85, SE=0.10) than those given a TTP application (N=53) (M=3.59, SE=0.11). This difference (0.264, 90% confidence interval (CI) [0.02, 0.52]) was significant (t(104)=1.74, p=0.04). Thereby we find evidence to *support hypothesis H2*. A Cohen's d effect of d=0.41 represents a 'medium' effect size.

In testing H3 (*perceived security*), the homogeneity of variance assumption was met (p=0.55). On average, participants given an MPC application perceive a higher degree of security (M=4.15, SE=0.11) than those given a TTP application (M=3.34, SE=0.09). This difference (0.88, bias-corrected and accelerated (BCa) 95% confidence interval (CI) [0.53, 1.09]) was significant (t(104)=5.76, p<.001). Thereby we find evidence to *support hypothesis H3* with a 'very large' effect size (a Cohen's d effect of d=1.2).

As for H4 (*perceived relative advantage*), the homogeneity of variance assumption was not met (p=0.01). On average, participants given an MPC application (N=53) perceive a higher level of relative advantage (M=3.94, SE=0.07) than those given a TTP application (N=53) (M=3.92, SE=0.10). This difference (0.02, bias-corrected and accelerated (BCa) 95% confidence interval (CI) [-0.23, 0.27]) was not significant (t(93.6)=0.15, p=0.88 (two-tailed). Thereby we find evidence to *support hypothesis H4*. It represented a Cohen's d effect of d=0.03 (negligible effect size).

The quantitative analysis shows that MPC contributes to perceptions of willingness to share sensitive data (see Table 1). We hypothesized that MPC contributes to perceived trustworthiness, perceived relative advantage, and perceived security. However, while participants are more willing to share sensitive data over an MPC application than a TTP application, the difference lies primarily in perceived trustworthiness and perceived security due to MPC.

Discussions and conclusions

In this paper, we explored how MPC affects organizational willingness to share sensitive data for collective purposes. To do so, we conducted experimental research within the context of IoT data sharing in supply chains by comparing the perception using MPC and TTP-based solutions. We found support for all of our hypotheses (see Table 2). MPC significantly increases firms' perceptions of trustworthiness and security while sharing sensitive data. Ultimately, firms' are more willing to share sensitive data using MPC-based applications than TTP. This positive attitude towards MPC is probably due to firms becoming independent

from intermediaries compared to the conventional data sharing process, as those intermediaries typically have access to raw data.

#	Hypotheses	Results
H1	Firms are more willing to share sensitive data through MPC than over Trusted Third Party (TTP).	Supported
H2	Perceived trustworthiness of an MPC-enabled application is greater than the perceived trustworthiness of a TTP-based application.	Supported
H3	Perceived security of an MPC-enabled application is greater than the perceived security of a TTP-based application.	Supported
H4	There is no difference in terms of perceived relative advantage between an MPC-enabled application and a TTP-based application.	Supported

Table 2. Results of the hypotheses testing

Our findings also imply that organizations are less willing to share sensitive data when trustworthiness or security is perceived as lacking. Hence, MPC developers should carefully assess the perception of trustworthiness and security when developing MPC-enabled applications. Also, a clear description of how MPC protects the sensitive data owned by firms in the data sharing process should be present. This is because an MPC application is not likely to be used if (1) the application is not perceived as trustworthy; (2) the organization behind the application is credible and traceable; and (3) the data providers can ensure that the protocols that are claimed to be used are in fact the protocols being used. By clearly describing the use of MPC in the data sharing process, firms could thoroughly assess the trustworthiness and security of the application and fully understand the data sharing process before considering using it.

We also found no difference between the perception of relative advantage provided by MPC-based applications and TTP. Given the novelty of MPC and its limited real-life implementations, it is understandable that firms do not see the real benefit of using MPC compared to the existing solution. Also, while MPC does provide a viable solution in protecting confidentiality, the use of TTP as an existing data-sharing solution is backed by business cases and thorough assessments, suggesting the importance of the purpose of data sharing on top of security aspects. Despite this fuzzy view of priority, when viewing MPC as a solution to foster sharing of sensitive data initiated due to cooperation and collaboration endeavors, MPC was found to carry potential in this regard. However, the MPC-based application must provide firms with levers to fully understand the whole process.

This research has two main limitations. The first one concerns the data collection phase, where we used a crowdsourcing platform as our primary source. Our unit of analysis here is at the organizational level, while most responses were collected at an individual level. Although we performed several checks to ensure participants met the proxy requirement for organizational decision-makers and shared their perceptions in the context of their organization, participants' answers might not entirely reflect the view of their organizations. In the organization, the decision-making process might occur in groups, such as project teams, rather than individuals. Hence, we suggest researchers perform case studies to enrich our general understanding of MPC adoption in organizational settings.

The second limitation is regarding the designed instrument. The mock-up was developed following scholars' recommendations and suggestions. It was also based on the successful deployment of an MPC web application. However, it is apparent that the application's development involved a lengthy discussion with many parties. As a result, these parties are more likely to be aware of the back-end before giving consent to their participation. We included more information than the reference application to address this issue—however, potentially at the cost of increased cognitive load. On the other hand, this provides a complete way of demonstrating the application, assuming that participants are unfamiliar with it. When there is a higher degree of familiarity with MPC, and when prospects are educated on the items and aspects that warrant attention, such an application can be "cleaned"-—while adhering to transparency requirements.

As a takeaway, our findings are also crucial as recent technological advancement allows the possibility to bring MPC in a real-life setting. We contributed to setting up a basis to understand how MPC can potentially resolve confidentiality concerns in data sharing. Moreover, according to our results, technologies like MPC potentially eliminate the need for trusted third parties for sharing data. In this way, such technologies significantly impact the relevance of trusted parties in the data economy, such as telecom operators or other intermediaries. The technologies also give a means for companies to directly share data, thus leveling the

playing field of the data economy. Hence, regulators and policymakers may consider MPC and related privacy-preserving technologies as a way to break the dominance of big tech corporations in the data economy.

Appendix

Survey questions

Construct	Dimension	Item wording
Perceived trustworthiness	Observability of the data transaction process	The intent of the application is clear to me.
		The application clearly describes how my data is processed from data submission to output.
		The application provides a complete and detailed description of how METHOD is used to protect my data
	Perceived complexity of the application	Interaction with the application is clear and understandable.
		The descriptions of METHOD are complex.
		Understanding how the data is processed does not require a lot of my mental effort.
	Perceived trustworthiness of the application	Claims made by the application are clear and accurate.
		The application is open and transparent in how it protects my data.
		*I am satisfied with the trustworthiness of the METHOD application.
Perceived security	Perceived risk	It feels safe contributing sensitive company data over the application.
		The use of METHOD gives me a feeling of security assurance.
	Perceived control over input data	Only I am able to view my contributed data.
		The service provider cannot examine my data beyond my control.
		I feel capable of using the application.
		My data cannot be accessed by other contributors.
	Perceived security of the application	I am satisfied with the security the METHOD provides.
Perceived relative advantage	Perceived simplification of the data sharing process	The application provides a simple way to securely contribute data.
		The application does not require expertise from multiple organizational departments.
		The application provides an advantage over conventional data sharing practices.
		When contributing data, no other party knows about my participation.
		I feel less hesitant with contributing sensitive company data when using this METHOD application.
	Perceived relative advantage	*METHOD provides a simple solution to secure data contribution.
Firms' willingness to share sensitive data through MPC	Willingness to use the application	*I would be willing to use METHOD based on the solution it provides to secure data contribution.
		*I would be willing to use this application based on its trustworthiness.
		*I would be willing to use this application based on the security provided by METHOD.
		*Overall, if the output (the analytics) of the application provides sufficient value to my organization, then I would be willing to contribute sensitive company data over a METHOD application.

Note: The word METHOD (in uppercase) must be replaced with MPC or TTP for each respective solution.

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. We would like to thank Hadi Asghari for his suggestions during the execution of the study. We would also like to thank all the participants in the survey.

References

Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*. https://doi.org/10.1109/PRISMS.2014.6970594

Adhikari, A., Bisi, A., & Avittathur, B. (2020). Coordination mechanism, risk sharing, and risk aversion in a five-level textile supply chain under demand and supply uncertainty. *European Journal of Operational Research*, *282*(1), 93–107. https://doi.org/10.1016/j.ejor.2019.08.051

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

Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., Smart, N. P., & Wright, R. N. (2018). From Keys to Databases—Real-World Applications of Secure Multi-Party Computation. *The Computer Journal*, *61*(12), 1749–1771. https://doi.org/10.1093/comjnl/bxy090

Arnaut, C., Pont, M., Scaria, E., Berghmans, A., & Leconte, S. (2018). *Study on data sharing between companies in Europe*. https://data.europa.eu/doi/10.2759/354943

Atallah, M. J., Deshpande, V., & Schwarz, L. B. (2004). *Secure Supply-Chain Collaboration: A new technology for supply-chain management*. Unpublished.

Bestavros, A., Lapets, A., Jansen, F., Varia, M., Volgushev, N., & Schwarzkopf, M. (2017). Design and Deployment of Usable, Scalable MPC. *Theory and Practice of Multi-Party Computation Workshop*.

Bogdanov, D., Jõemets, M., Siim, S., & Vaht, M. (2015). How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation. In R. Böhme & T. Okamoto (Eds.), *Financial Cryptography and Data Security* (pp. 227–234). Springer. https://doi.org/10.1007/978-3-662-47854-7_14

Bogdanov, D., Talviste, R., & Willemson, J. (2012). Deploying Secure Multi-Party Computation for Financial Data Analysis. In A. D. Keromytis (Ed.), *Financial Cryptography and Data Security* (pp. 57–64). Springer. https://doi.org/10.1007/978-3-642-32946-3_5

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

Chang, A. J.-T. (2010). Roles of perceived risk and usefulness in information system security adoption. *2010 IEEE International Conference on Management of Innovation Technology*, 1264–1269. https://doi.org/10.1109/ICMIT.2010.5492818

Choi, J. I., & Butler, K. R. B. (2019). Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/1368905

Cooper, M. C., Lambert, D. M., & Pagh, J. D. (1997). Supply Chain Management: More Than a New Name for Logistics. *The International Journal of Logistics Management*, *8*(1), 1–14. https://doi.org/10.1108/09574099710805556

Curkovic, S., Scannell, T., & Wagner, B. (2015). *Managing Supply Chain Risk: Integrating with Risk Management*. CRC Press.

Damgård, I., Damgård, K., Nielsen, K., Nordholt, P. S., & Toft, T. (2017). Confidential Benchmarking Based on Multiparty Computation. In J. Grossklags & B. Preneel (Eds.), *Financial Cryptography and Data Security* (pp. 169–187). Springer. https://doi.org/10.1007/978-3-662-54970-4_10

De Prieëlle, F., De Reuver, M., & Rezaei, J. (2020). The Role of Ecosystem Data Governance in Adoption of Data Platforms by Internet-of-Things Data Providers: Case of Dutch Horticulture Industry. *IEEE Transactions on Engineering Management*, 1–11. https://doi.org/10.1109/TEM.2020.2966024

De Reuver, M., Fiebig, T., Agahari, W., & Faujdar, V. (2019). *User experiment report* (D2.4). Safe-DEED. https://safe-deed.eu/wp-content/uploads/2020/08/D2_4.pdf

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

Feller, T. (2014). Requirements for Trustworthiness. In *Trustworthy Reconfigurable Systems: Enhancing the Security Capabilities of Reconfigurable Hardware Architectures* (pp. 35–60). Springer Vieweg. https://doi.org/10.1007/978-3-658-07005-2_3

Field, A. (2017). *Discovering statistics using ibm spss statistics* (5th ed.). Sage Publications Ltd.

Guan, Z., Zhang, X., Zhou, M., & Dan, Y. (2020). Demand information sharing in competing supply chains with manufacturer-provided service. *International Journal of Production Economics*, *220*, 107450. https://doi.org/10.1016/j.ijpe.2019.07.023

Hart, P., & Saunders, C. (1997). Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange. *Organization Science*, *8*(1), 23–42. https://doi.org/10.1287/orsc.8.1.23

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

Huang, D.-L., Rau, P.-L. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870–883. https://doi.org/10.1016/j.ijhcs.2011.07.007

Huang, Y.-S., Hung, J.-S., & Ho, J.-W. (2017). A study on information sharing for supply chains with multiple suppliers. *Computers & Industrial Engineering*, *104*, 114–123. https://doi.org/10.1016/j.cie.2016.12.014

Kanger, L., & Pruulmann-Vengerfeldt, P. (2015). Social Need for Secure Multiparty Computation. *Cryptology and Information Security Series*, *13*, 43–57. https://doi.org/10.3233/978-1-61499-532-6-43

Kerschbaum, F., Schroepfer, A., Zilli, A., Pibernik, R., Catrina, O., de Hoogh, S., Schoenmakers, B., Cimato, S., & Damiani, E. (2011). Secure Collaborative Supply-Chain Management. *Computer*, *44*(9), 38–43. https://doi.org/10.1109/MC.2011.224

Kharuna, M. K., Mishra, P. K., & Singh, A. R. (2011). Barriers to Information Sharing in Supply Chain of Manufacturing Industries. *International Journal of Manufacturing Systems*, *1*(1), 9–29. https://doi.org/10.3923/ijmsaj.2011.9.29

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

Li, J., Shaw, M. J., Sikora, R. T., Tan, G. W., & Yang, R. (2001). *The Effects of Information Sharing Strategies on Supply Chain Performance*. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.136.9595&rep=rep1&type=pdf#:~:text=Information%20sharing%20among%20supply%20chain,accurately%20based%20on%20real%20demand.

Lotfi, Z., Mukhtar, M., Sahran, S., & Zadeh, A. T. (2013). Information Sharing in Supply Chain Management. *Procedia Technology*, *11*, 298–304. https://doi.org/10.1016/j.protcy.2013.12.194

Milch, V., & Laumann, K. (2016). Interorganizational complexity and organizational accident risk: A literature review. *Safety Science*, *82*, 9–17. https://doi.org/10.1016/j.ssci.2015.08.010

Min, H., & Zhou, G. (2002). Supply chain modeling: Past, present and future. *Computers & Industrial Engineering*, *43*(1–2), 231–249. https://doi.org/10.1016/S0360-8352(02)00066-9

Ojha, D., Sahin, F., Shockley, J., & Sridharan, S. V. (2019). Is there a performance tradeoff in managing order fulfillment and the bullwhip effect in supply chains? The role of information sharing and information type. *International Journal of Production Economics*, *208*, 529–543. https://doi.org/10.1016/j.ijpe.2018.12.021

Pavlou, P. A., & Gefen, D. (2004). Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research*, *15*(1), 37–59. https://doi.org/10.1287/isre.1040.0015

Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples. *Communication Theory*, *1*(4), 311–335. https://doi.org/10.1111/j.1468-2885.1991.tb00023.x

Petronio, S. (2013). Brief status report on Communication Privacy Management theory. *Journal of Family Communication*, *13*(1), 6–14. https://doi.org/10.1080/15267431.2013.743426

Raj, G., Sarfaraz, M., & Singh, D. (2014). Survey on trust establishment in cloud computing. *2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence)*, 215–220. https://doi.org/10.1109/CONFLUENCE.2014.6949375

Sendhil Kumar, R., & Pugazhendhi, S. (2012). Information Sharing in Supply Chains: An Overview. *Procedia Engineering*, *38*, 2147–2154. https://doi.org/10.1016/j.proeng.2012.06.258

Skinner, E. A. (1996). A guide to constructs of control. *Journal of Personality and Social Psychology*, *71*(3), 549–570. https://doi.org/10.1037/0022-3514.71.3.549

Stevens, J. P. (2016). *Applied Multivariate Statistics For The Social Sciences* (6th ed.). Routledge/Taylor & Francis Group.

Wu, J., Wang, Z., & Huang, L. (2010). The relationship among propensity to trust, institution-based trust, perceived control, and trust in platform. *2010 IEEE 2nd Symposium on Web Society*, 424–428. https://doi.org/10.1109/SWS.2010.5607414

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

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

Zaheer, A., & Venkatraman, N. (1995). Relational governance as an interorganizational strategy: An empirical test of the role of trust in economic exchange. *Strategic Management Journal*, *16*(5), 373–392. https://doi.org/10.1002/smj.4250160504

Zare-Garizy, T., Fridgen, G., & Wederhake, L. (2018). A Privacy Preserving Approach to Collaborative Systemic Risk Identification: The Use-Case of Supply Chain Networks. *Security and Communication Networks*, *2018*, 1–18. https://doi.org/10.1155/2018/3858592

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330–340. https://doi.org/10.1108/09685220910993980

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