The Importance of Being Earnest: Shedding Light on Johnny's (False) Sense of Privacy

Wirawan Agahari*, Alexandra Dirksen†, Martin Johns†, Mark de Reuver‡, Tobias Fiebig§
*TU Delft, Tilburg University w.agahari@tilburguniversity.edu
†Technische Universität Braunschweig, {a.dirksen, m.johns}@tu-braunschweig.de
‡TU Delft, g.a.dereuver@tudelft.nl
§ Max Planck Institut für Informatik, FG INET, tfiebig@mpi-inf.mpg.de

***Abstract*—As privacy concerns grow, organizations and policy makers promote the use of privacy-enhancing technologies (PETs) to improve user trust and data-sharing behaviors. However, privacy-enhancing technologies (PETs) are often technologically complex and opaque to lay users. It is challenging to understand and effectively communicate the functionality of complex PETs to the users, such as Secure Multi-Party Computation (MPC).**

Studies typically assess the impact of new PETs by presenting users with a high-level description of the technology before measuring how this treatment changed their attitude or behavior. These results influence business and regulatory decisions (see Gartner's Hype Cycle for Emerging Technology [123]). In the present study, we question this approach. We assess whether naming specific PETs and providing generic descriptions impact users' willingness to put trust in service providers and share their data. Our survey presented three randomized controlled trials with 1,457 participants in a data marketplace scenario. The first group was treated with a PET (MPC), the second group with a fictional PET, and the third with a non-PET, serving as a control group.

Our findings reveal that user trust and data-sharing willingness increased with MPC and the fictional PET, indicating that the high-level description, rather than the technology name, shapes user perception. We conclude that *claiming* the use of a PET is not an effective method to measure the impact of *actually* using this technology. However, given their mental model, lay users cannot verify the privacy claims of such descriptions presented in studies or by service providers. This increases the risks of users being deceived into a false sense of privacy, leading them to expose more private data than they otherwise would.

1. Introduction

Consumers are increasingly reluctant to share data with businesses due to increasing concerns over privacy and control [72, 133, 143, 169]. This reluctance is plausible given the prevalence of documented mishandling of users' private data [7, 14, 83]. In turn, companies are constantly developing better methods to mislead users into disclosing as much personal data as possible.

Economics has long examined the balance between digitalization and data economy goals [17, 42]. As proposed, this data economy poses enormous potential for enabling automation, personalization, and knowledge creation [41, 162]. To contribute to this discussion, researchers extensively studied what influences users' willingness to share their data, especially in the more economics-oriented Information Systems field. In these studies, factors such as perceived control [112], general privacy concerns [129], perceived risks [50], and trust [145] are found to influence users data sharing decisions.

Yet, with the aforementioned reluctance of users to actually share their data, organizations are turning to technical remedies in the form of PETs to find ways to leverage data while being able to preserve privacy [17].

Meanwhile, the image of PETs has shifted from unnecessary to essential, offering competitive advantages [131, 155]. This is demonstrated by the emerging uses of, e.g., End-to-End Encryption for messaging [182], Fully Homomorphic Encryption, and Zero-Knowledge protocols for cloud storage [107] or Differential Privacy [51, 58, 71] by major companies. 'The Blockchain' was seen to hold similarly disruptive potential to overcome users' privacy concerns and lead the way into a new age of data-driven economic growth [32, 128, 187]. Here, Multi-party computation (MPC) has recently been found to be a promising technology to fulfill these conflicting requirements of preserving privacy and leveraging data [17].

Such technologies typically also provide privacy protection for the user in addition to their security benefits. If accepted, they can potentially increase the user's trust in the product and, therefore, the company. Consequently, besides the expectable hype [72], researchers also investigated how such new, disruptive technologies would influence users' willingness to and perception of sharing data. Methodologically, quantitative studies in this field usually work with mock-up and prototype setups, relying on explaining what a new PET is doing while then collecting stated preferences from study participants to infer the impact of a given PET, see, e.g., Smith et al. [166] for an overview of the field. Beyond the issue of self-reporting bias [35, 54], there *must* be some truth to the privacy assertions claimed, considering the

2025 IEEE Symposium on Security and Privacy (SP) | 979-8-3315-2236-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/SP61157.2025.00150

DOI 10.1109/SP61157.2025.00150

wide-spread adoption of new PETs in the industry, starting with the long-since gone 'SSL badges' on websites [113].

In this paper, we present the results of a large-scale ($N = 1457$) randomized controlled treatment study that was conducted in November 2021 to assess the impact of MPC on users' trust and willingness to share data in a data marketplace (DMP). We designed this study following best practices, comparing a DMP using MPC with one default case of the DMP acting as a trusted third party. A common practice for such studies is to utilize high-level descriptions with the explicit naming of the PET and mock-ups to make statements about specific technologies [87, 160]. Out of an abundance of caution, we included a control condition to ensure that we were not just testing for the *name* of a PET. In this control condition, we introduce the PET by a different name, again accompanied by a high-level description. However, this technology is entirely fictitious.

Running our study with a representative end-user sample from the United Kingdom, we find that both — MPC and our made-up technology — similarly impact users' data-sharing behavior compared to a baseline of a trusted third party. We did, however, not find significant differences among these two; see Table 5 and 6.

While this result may initially seem obvious, it contradicts common practice regarding the use of mock-ups and high-level descriptions for end-user studies on the impact of PETs. This boils down to the underlying issue that users usually lack the ability to *verify* whether it actually *does* what it promises [117, 144]. At the same time, providing more in-depth and technical explanations would necessarily exclude participants who are less familiar with the technology. The core findings of our study are:

- Based on our finding that the name of technology makes *no* significant difference regarding users' trust and willingness to share data, we argue that only the high-level communicable privacy guarantees influence how well a PET is perceived in end-user studies.
- Given the difficulty of communicating PETs reliably to participants, we argue for studies assessing the impact of PETs to shift their focus instead on the effects of particular privacy properties of PETs.
- Development and investment decisions rooted in studies assessing end-users trust in specific PETs should be treated with caution and scrutiny, especially by regulators. This also applies to advertisements that explicitly practice name-dropping of PETs.

Structure: The remainder of this paper is structured as follows. We first provide additional background on prior studies on PETs' impact on users' privacy perceptions and a brief background on MPC in Section 2. Subsequently, we introduce our study methodology and instrument in Section 3, where we also discuss our work's ethical implications and necessary precautions. We present our results and statistical evaluation in Section 4 before analyzing and contextualizing them in Section 5. Finally, we conclude in Section 6. In addition, we make our complete supplemental material available for download [1].

2. Background and Related Work

In this section, we introduce relevant background and related work. Here, we also emphasize concepts that may differ between computer science-focused privacy studies and more economics-related fields investigating privacy.

2.1. Privacy Enhancing Technology (PET)

According to Goldberg et al. *'Privacy refers to the ability of the individual to protect information about [her-] himself'* [79]. Consequently, the field of creating PETs, which includes or even focuses on protecting a user's privacy, emerged [19, 39] either. Furthermore, over the past decades, policymakers (GDPR, CCPA, etc.) have established requirements for a systems' privacy properties to protect users' privacy.

Despite most PETs using similar underlying technical concepts depending on their purpose, e.g., encryption, to protect privacy properties, there is no common *universal* definition of what properties make a PET a PET. For example, the European Agency *ENISA* claims PETs to be "a fuzzy concept in practice" [157]. Nevertheless, they roughly describe PETs as software to protect against risks to the privacy of an individual [157].

As such, policymakers tend to focus on those underlying technologies or the protected properties in the context of PETs: For example, in 2023, the UK Information Commissioner's Office considered the following PET concepts as state-of-the-art: Differential privacy, Homomorphic Encryption, Zero-Knowledge-Proofs, Secure Multiparty Computation, and Private Set Intersection[2] [95]. In contrast, Canada's Privacy Commissioner names goals for PETs to achieve, e.g., anonymity, confidentiality, data minimization, and transparency, among others[2] [152].

Regarding privacy engineering in the industrial context, one must consider additional aspects. For example, Iwaya et al. emphasize the importance of corporate management communicating its commitment to privacy values to its software developers [98]. This creates a tension between the (legal and individual) right to privacy and the industry's interests. On the one hand, individuals have the right to privacy and, therefore, not to have their data processed without their consent. On the other side, the data industries' business model is usually based on the processing and resale of data - which consequently is unwilling to put their interests at risk [21, 165]. Greaney discussed this conflict in *Data Privacy In The Age of Surveillance Capitalism* [82][3].

Considering these diverse perspectives, the variety of use cases, and the rapid involvement of technology, we conclude

1. https://anonymous.4open.science/r/mpc_supplemental_material-D8CF/

2. These lists do not claim to be complete and serve only as an example.

3. This title refers to "Surveillance Capitalism", coined by Zuboff [194].

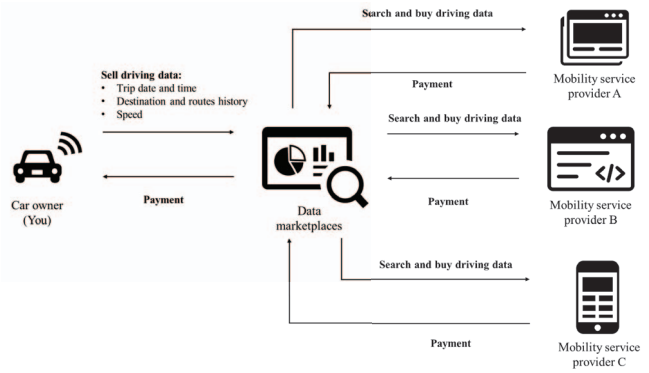

Figure 1. Overview of a Data Marketplace for driving related data.

that there is no comprehensive list of properties or concepts that a technology must comply with to be considered a PET.

2.2. Data Marketplaces (DMP)

Generally, data marketplaces are defined as multi-sided platforms that facilitate data sharing and trading between data providers and data buyers, which can be individuals or businesses [92, 110, 169, 172]. Data marketplaces allow participants to store, maintain, access, and trade data from various sources based on a wide range of standardized or negotiated licensing models [163, 171]. Their role between data providers is regularly seen as a method to allow data-creating parties to gain equitable access to monetize their data [61, 92, 110]. This is especially crucial for data-heavy scenarios, like the "Internet-of-Things" [137] and 'Smart Cities' [156].

Naturally, due to the central role of DMPs, critical voices also highlight the risks, along with traditional discourse on the productization of users [60]. As such, efforts to decentralize DMPs [177], or to enhance their acceptance by introducing novel technology [111, 142, 178] are common.

The practical implementation of DMPs these days raises doubt whether the use of technology, especially PETs, can improve equitable participation in data exploitation [18], analogous to work in the broader context of PETs and fairness [33, 84]: Data marketplaces tend to show involvement by established players in the cloud economy [15]. As such, DMPs may accelerate centralization and surveillance capitalism by re-enforcing existing power imbalances in data sovereignty [37].

Data Marketplaces for Driving Data are a specific sector implementation of a DMP to make driving data accessible to various interested parties. For example, insurance companies [16], societal stakeholders [127] or city planers [52], represent a variety of use-cases. Figure 1 provides a high-level overview of their workflow.

2.3. Trusted-Third-Party (TTP)

When we refer to a TTP in this work, we do not imply that the TTP has any specific features that *qualify* it to act as a TTP between two entities. Furthermore, we do not imply that this party is necessarily impartial to all aspects of a transaction. However, we presuppose that both interacting parties leveraging a TTP place trust in this party concerning a specific property.

Put into an example: While a DMP shares an interest in facilitating transactions via its platform, it may hold its interest in pulling as much data as possible from a data provider onto the platform. However, the data provider trusts the DMP to not unnecessarily reveal information to data consumers because doing so would counter its interests. Similarly, data consumers trust that the DMP will provide them with truthful, e.g., data aggregations after paying the DMP for their services. Thus, we choose TPP as a counterpart to MPC and DCP as it relies more on the semantic framing of the term "trust" instead of the (supposedly) utilisation of a specific technology.

2.4. Multi-party computation (MPC)

MPC, or often also *Secure* Multi-Party Computation, is a summary term for a set of cryptographic techniques where several parties jointly compute a function to generate a meaningful output without disclosing the input provided by either party [40, 188]. As such, this is applicable in various use cases that require joint computation but also necessitate not sharing individual plain-text data [12]. Therefore, it is helpful for cases where two or more parties, e.g., individuals or organizations, would like to collaborate using sensitive data that requires strict privacy protection. Modern practical use-cases include auction-based pricing [27], gender wage gap analysis [119], and health-care data processing [59].

MPC is closely related to and partially overlapping with other PETs [5, 13], e.g., homomorphic encryption [74, 138], differential privacy [56, 57], and federated learning [120, 135]. While these technologies share similar characteristics in protecting input data while computing meaningful output, they differ in specifics. For instance, homomorphic encryption protects data at rest, held by one data owner. Similarly, differential privacy strives to preserve privacy while generating generally publishable datasets. Furthermore, federated learning expands on MPC, keeping the inputs decentralized by focusing on training machine learning models. Nevertheless, these technologies can complement each other to meet robust privacy and security requirements when necessary [9, 148, 190].

In 2020, the European Data Protection Board (EDPB) recommended MPC as a key PET supplementary measure to the GDPR. It proposed its application for fields like financial and healthcare services, machine learning, or privacy-preserving data storage, among others [43]. EDPBs recommendation and the rapid development of MPC protocols in research and industry [81, 100, 150, 191] leads to the choice of MPC being a representative for PETs in this study.

2.5. Data-Computation-Protection (DCP) (fictional technology)

This background section introduces the concept of a technology called Data Computation Protection. However, since DCP is a *fictional technology* we made up for this survey, there is no definition of functions or any related work to refer to.

Previous work regularly assumes that naming a technology along with a high-level description is sufficient to make statements on the user's position towards it [87, 160]. As DCP serves as our control condition to assess this assumption, we opted for this approach. We constructed the description for both DCP and MPC by applying the general concepts of PETs, as proposed in Sec.2.1 for the description. Concretely, we applied wording and structure repeatedly used in well-known fully-fledged PETs (which applies to MPC, as this technology is not fictitious), i.e., encryption, decryption, data access, and computation.

3. Methodology

In this section, we present our survey methodology. As our research question requires high internal validity [179], we use a controlled, survey-based online experiment. More specifically, we used a between-subject post-test-only design, meaning that each participant was randomly assigned to a different treatment with different conditions and got an identical post-test [38]. This design allows us to explore the effect of a treatment (e.g., TTP vs. MPC vs. DCP) on a given situation (e.g., consumers' data-sharing decisions).

3.1. Experiment Overview

To test the impact of PETs on participants' data-sharing willingness, we set up a multi-step procedure, see Figure 2. We selected this scenario as providing a monetary incentive in exchange for data is a common mechanic to motivate users to share data [28, 149]. This also applies to users who have concerns regarding their privacy, a phenomenon called the privacy paradox [45]. The scenario of sharing driving data is also already being implemented by car insurance companies in exchange for reduced premiums [48, 168].

In the first step, users are introduced to a data-sharing scenario via a 'data marketplace', i.e., a dedicated entity that facilitates data trading. After presenting the scenario, users are randomly assigned to a treatment. Finally, after applying the treatment, users are asked to fill out a survey, followed by a final step in which we solicit general demographic data on the participant.

3.1.1. Scenario Description. In our scenario, users are asked to imagine that they can sell their driving-related data (trip date/time, destination, route history, speed, etc.) to interested third parties via a data marketplace. In return for sharing their data, they would receive payments from the data marketplace, which, in turn, charges the entities using this data. This overall setting has been selected as it illustrates a widely relatable case for end-users[4], while also having clear incentives for data consumers, e.g., when it comes to more effective traffic steering.

3.1.2. Treatments. In the second step, we present participants with a randomly selected treatment. Besides the scenario description itself, treatments included mock-ups of the expectable data marketplace. Our mock-ups were developed over two years and iteratively refined in multiple independent usability-focused qualitative pre-studies. We explored multiple ways of explaining and visualizing PETs suggested in prior work. For an example mock-up (MPC case), please see Figure 3. Our supplemental material contains higher-resolution screenshots of the mock-ups and makes it available for download[5].

For the treatments, we asked users to consider the overall scenario in which the data market implements the PET presented in the treatment for the following questionnaire. Our treatment conditions are:

a) TTP: In this treatment, we ask users to imagine that the data market serves as a TTP. This means that data buyers are not able to access the data directly. Instead, they request the data marketplace to run specific analyses on the user-supplied data and only receive aggregate statistics. Still, as the TTP, the data market has access to all data.

b) MPC: In this treatment, users are informed that MPC is being used. The functionality of MPC is described in a high-level manner, focusing on key properties (e.g., data encryption and only storage in the participants' car). While one might argue that this description insufficiently represents MPC and does not allow participants to grasp underlying concepts thoroughly, we did so to be consistent with the approaches taken in prior studies and the language commonly found in, e.g., privacy policies [94, 125, 126]. Furthermore, it is unlikely that average users from the general (our target) population would find a more detailed description sufficiently accessible.

c) DCP (fictional): To run our study on a sample from the general public, the description of MPC in the mock-up is rather high-level (Sec. 2). This carries the risk that an experiment may only test the impact of *something* related to PETs being mentioned and *not* the impact of the actual PET. Contrary to prior work, we decided to control for this bias by including an additional test case that uses an entirely fictional name while generally following the same phrasing as treatment b). If this treatment has a comparable effect to the MPC treatment compared to the baseline, we know that the effect is *not* caused by the named technology. Instead, the effect is more likely caused by the high-level description of the PET and/or the general notion of adding *some* technology to improve privacy. While such a finding would be negative for our specific study, it carries significant implications for the whole field, as our general approach

4. In 2021, approx. 25.6 million people in Great Britain lived in a household that owned at least one car [173].

5. https://anonymous.4open.science/r/mpc_supplemental_material-D8CF/

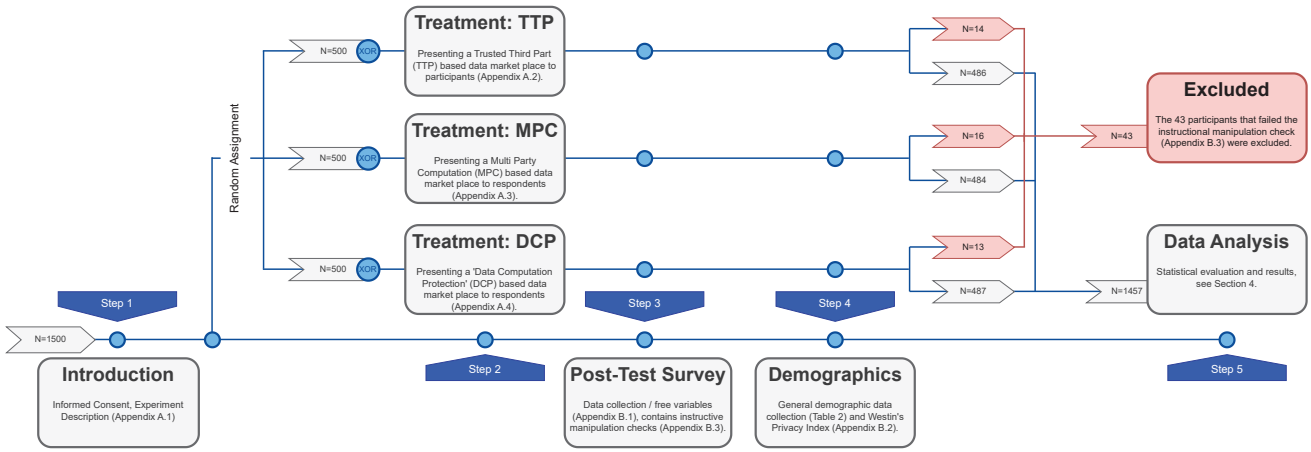

Figure 2. Overview of the experimental flow with the three treatment conditions.

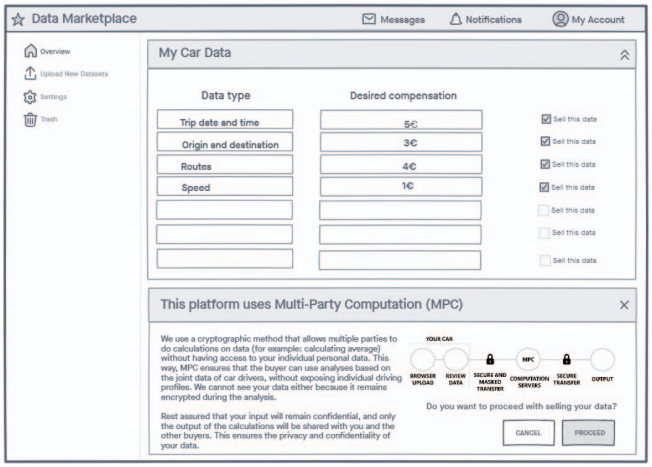

Figure 3. Design of the mock-up for the MPC scenario.

aligns with common practices when studying the impact of (new) PETs on users' trust.

3.1.3. Survey. After applying the treatment, users are asked to fill out a survey, see Appendix A, to solicit self-reported data on how the treatment affected the users' disposition toward data sharing in the given scenario. We root our survey in prior work on antecedents of consumers' willingness to share data derived from the information systems' privacy literature: Perceived control, privacy concerns, trust (in data buyers and data marketplaces operators), and perceived risks, see Table 1.

Hence, in this survey, we test six different measures on a five-point Likert scale [22, 122], utilizing instruments from prior work adjusted to the context of data marketplaces, adding a meta instrument on the general willingness to share data via data marketplaces by Pavlou [145]:

1) Perceived control (3 questions, from Xu et al. [166])
2) Perceived risk (2 questions, from Xu et al. [166])
3) Privacy concerns (2 questions, from Dinev & Hart [50])
4) Trust in data marketplaces operator (3 questions, from Kehr et al. [104])
5) Trust in data buyers (3 questions, from Kehr et al. [104])
6) Willingness to share data via data marketplaces (3 questions, from Pavlou [145])

Furthermore, we follow survey design best practices as summarized by Redmiles et al. [158]: To ensure participants are attentive and consciously filling out the survey, we added an instructional manipulation check [141]. For that test, participants are requested always to answer a specific Likert item, regardless of their disposition toward the question These two questions are:

- *There is nothing wrong with companies that collect personal information without consent. Regardless of what you think, please select "somewhat agree."*
- *Do you agree that data is the new oil? Regardless of what you think, please select "strongly disagree."*

Furthermore, to prevent order-effects [34, 115], the order of questions presented to participants in the questionnaire is fully randomized. Finally, we also extensively piloted and refined our questionnaire; see Section 3.2.

3.1.4. Demographic Data. As the last step in the survey, we collect demographic information on the participants. Specifically, we collect: i) Age, ii) Gender, iii) Education level, iv) Employment status, v) Industry type, vi) Role at work, vii) Car ownership, viii) Awareness of data marketplaces, ix) Awareness of PETs, x) Westin's Privacy Segmentation Index.

The final item, Westin's Privacy Segmentation Index [116], is an established measure in information systems' literature to segment participants into one of three categories concerning their privacy behavior: Privacy fundamentalists (most protective of their privacy), privacy unconcerned (least protective of their privacy), and, privacy pragmatists (weighing the pros and cons of sharing information). The index uses three questions on a 4-point Likert scale from 1

TABLE 1. ANTECEDENTS OF CONSUMERS' WILLINGNESS TO SHARE DATA DERIVED FROM THE INFORMATION SYSTEMS' PRIVACY LITERATURE.

Antecedents	Description	Related Work
Perceived control	The extent to which an individual believes that they can manage the release and dissemination of personal information [186].	Dinev et al. [49], Farrelly and Chew [64], Kim and Choi [108], Krasnova et al. [112], Markos et al. [132], S. Spiekermann [170], Schomakers et al. [162], Xu et al. [186]
Privacy concerns	The degree of an individual's concern about who has access to the data that is being shared and how other parties use it [167].	Cichy et al. [41], Kato et al. [101], Kehr et al. [104], Keith et al. [105], Malhotra et al. [129], Mangiò et al. [130], Naous et al. [139], Pal et al. [143], Smith et al. [166], L. Zhao et al. [189]
Trust (in data buyers & data marketplace operators)	An individual's belief that another party (data buyers and/or data marketplaces operator) will act as expected and not do harmful things, such as misusing personal data [104].	Buck and Reith [31], Dinev and Hart [50], Kehr et al. [104], Krasnova et al. [112], Liu et al. [124], Malhotra et al. [129], Pavlou [145], Wessels et al. [181]
Perceived risks	The expectation of losses if someone engages in data sharing [186].	Alashoor et al. [8], Cichy et al. [41], Dinev and Hart [50], Kehr et al. [104], Kim and Choi [108], Krasnova et al. [112], Malhotra et al. [129], Pal et al. [143], Pavlou [145], Zhou [192]

(strongly disagree) to 4 (strongly agree), and is widely used within the field [44, 55, 161, 185]:

- Consumers have lost control over how companies collect and use personal information.
- Most businesses handle the personal information they collect about consumers in a proper and confidential way.
- Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

3.2. Pilot Studies

We validated the instruments and measurements used in two pilot studies not included in the final result set. The first pilot was conducted with six local participants to validate the content validity of the constructs. Based on their feedback, we refined the questions, case descriptions, and experiment flow. The second pilot study was conducted with 300 participants recruited from the online crowd-sourcing platform Prolific, which was also used to recruit the main study participants; see Sec. 4.1.

3.3. Population Overview & Recruitment

Our population of interest comprises citizens of the United Kingdom (i.e., those with UK nationality or currently living in the UK) aged 18 years and older. We recruited participants using the online crowd-sourcing platform Prolific, which is commonly used in academic research nowadays [146, 153, 158].

Participants recruited via Prolific are more diverse, naïve, and honest than similar crowdsourcing platforms like Amazon Mechanical Turk (MTurk) [3, 146]. Please note that Prolific uses a pool of volunteer participants to receive survey requests. This panel's diversity is ensured by, e.g., additional recruitment efforts, i.e., it is not biased by, for example, self-selection bias. Furthermore, Prolific ensures the requested number of participants, explaining the *seemingly* 100% response rate. Also, Prolific claims to be able to offer representative samples based on age, gender, and ethnicity. [154]

Nevertheless, using Prolific for academic research also has limitations like participant selection bias and monetary incentives, which should be considered when interpreting the results [102, 158]. Overall, our sample roughly conforms to the demographic parameters of the underlying population; see Section 4.1.

3.4. Ethical Considerations

In our study, we collected informed consent from our participants and informed them that their participation was voluntary. See our supplemental material at https://anonymous.4open.science/r/mpc_supplemental_material-D8CF/ for the full text. Participants were awarded 2.5 GBP for participating in the survey, following the rate recommended by Prolific (7.5 GBP/hour) concerning the rounded-up average completion time for the survey in the pre-study (average 15.6 minutes, SD = 9.3).

Before engaging with participants, our research design was audited and cleared by our institution's Human Research Ethics Committee (HREC) under No. <REDACTED>. The clearing process involved an evaluation of our research ethics, as well as our data management plan. Furthermore, the HREC also audited our informed consent form.

4. Results

Here, we first describe the general parameters of our dataset and the demographic parameters of the respondents in our sample compared to the demographics of the underlying population. Next, we perform a thorough statistical analysis, auditing the dataset for noise and unreliable measures we may have introduced. Finally, based on the responses received, we compare the effects of the selected treatments.

4.1. Demographic Overview

According to Prolific, we collected the data in November 2021 and recruited 1500 participants who are representative of the UK population. We excluded 43 because they failed to answer two instructional manipulation checks correctly, suggesting that these participants did not participate in the experiment seriously [141]. The final sample of 1457 participants is representative in terms of gender (47.9% male compared to 49.4% in the target population), ethnicity (85.5%

white compared to 84.8% in the target population), and car ownership (64.9% own/have access to the car compared to 76% in the target population). However, the sample is biased toward the younger generation (58% between 18 and 37 compared to 32.6% in the target population) and highly educated people (60.7% higher education compared to 47% in the target population), although the median age was representative (35 years compared to 39 years in the target population).

Looking at other demographics, more than half of the participants currently work full-time (55.7%) or part-time (18.7%) and primarily work in the education (12.4%), IT (8.9%), or retail industry (7.9%). About a quarter of our participants hold a managerial position, either at a junior (8.9%), middle (14.1%), or upper management level (3.4%). Moreover, 45.4% of participants claimed they were aware of data marketplaces and provided examples such as Snowflake, Facebook, Prolific, Compare the Market, and YouGov. Meanwhile, 20.8% of participants were aware of PETs before participating in the survey, with many different encryption protocols named, such as end-to-end encryption, homomorphic encryption, zero-knowledge proofs, and Virtual Private Network (VPN). Further, the majority of our participants are privacy pragmatists (53.6%), followed by privacy fundamentalists (26.5%) and privacy unconcerned (19.9%), which is broadly similar to the distribution of privacy perspectives in comparison to other studies [93, 99, 116]. See Table 2 for the demographic characteristics of our sample.

TABLE 2. SAMPLE DEMOGRAPHICS FOR $N = 1457$.

Variable	Characteristics	N	%
Age	18-27	395	27.1%
	28-37	450	30.9%
	38-47	257	17.6%
	48-57	202	13.9%
	58+	153	10.5%
Gender	Male	698	47.9%
	Female	745	51.1%
	None of the above	11	0.8%
	Prefer not to say	3	0.2%
Education level	Doctorate degree (Ph.D./other)	39	2.7%
	Graduate degree (MA/MSc/MPhil/other)	276	18.9%
	Undergraduate degree (BA/BSc/other)	569	39.1%
	Technical/community college	135	9.3%
	High school diploma/A-levels	265	18.2%
	Secondary education (e.g., GED/GCSE)	158	10.8%
	No formal qualifications	12	0.8%
	I do not know/not applicable	1	0.1%
	Prefer not to say	2	0.1%
Employment status	Full-time	812	55.7%
	Part-time	273	18.7%
	Self-employed/freelance	18	1.2%
	Not in paid work (e.g., homemaker, retired, etc.)	184	12.6%
	Not employed (students)	65	4.5%
	Starting a new job within the next month	12	0.8%
	Unemployed (and job-seeking)	74	5.1%
	Prefer not to say	19	1.3%
Industry type	Education & Training	180	12.4%
	Information Technology	129	8.9%
	Retail	115	7.9%
	Medicine	104	7.1%
	Finance	96	6.6%
	Other	833	57.1%
Role at work	Upper Management	50	3.4%
	Middle Management	205	14.1%
	Junior Management	129	8.9%
	Others	1000	68.6%
	Prefer not to say	73	5%
Car ownership	Yes	946	64.9%
	Have access via parents/family	214	14.7%
	Have access via leasing/rental	50	3.4%
	No	247	17.0%
Awareness of DMPs	Shared data through DMPs multiple times	77	5.3%
	Shared data through DMPs once	67	4.6%
	Know but never shared data through a DMP	518	35.6%
	Never heard of data marketplaces	795	54.6%
Awareness of PETs	Already know before the survey	303	20.8%
	Have some ideas because of the survey	876	60.1%
	Still have no idea after the survey	278	19.1%
Westin's Priv. Seg. Index	Privacy fundamentalists	386	26.5%
	Privacy unconcerned	290	19.9%
	Privacy pragmatists	781	53.6%

4.2. Statistical Validity & Reliability

Before comparing our treatment conditions, we perform due diligence by assessing our measurement instrument's statistical validity and reliability, given the collected responses. Our instrument has sufficient internal validity and reliability for the entire dataset and each individual treatment. Please see Tables 3 for an overview.

Confirmatory Factor Analysis (CFA): First, to validate our constructs and measurement model (see Section 3), we perform a Confirmatory Factor Analysis (CFA), as introduced by Brown & Moore [29], using JASP version 0.16.1[6]. Using the three established criteria by Hu and Bentler [91], i.e., a Comparative Fit Index (CFI) ≥ 0.95, Tucker-Lewis Index (TLI) ≥ 0.95, and Root Mean Square Error of Approximation (RMSEA) ≥ 0.06, we find our model to have a good fit index, with $CFI = 0.988$, $TLI = 0.984$, and $RMSEA = 0.043$. This means that, from a high-level statistical perspective, our questionnaire is well suited to measure the effects we aim to measure.

Factor Loading: Next, to further assess the validity of our constructs, we also investigate the factor loadings of each survey item. For this, we use a threshold of 0.70, following a recommendation made by Fornell & Larcker that has been established in the literature since 1981 [68]. Here, the analysis revealed that one item (CTRL_3, see Section A.1 in Appendix A) does not meet this criterion, i.e., does not sufficiently measure what it is supposed to measure. Hence, we excluded this item to ensure it does not introduce noise in our evaluation. The remaining items, see Table 3, have a factor loading of 0.79 or greater, higher than the recommended threshold.

Assessing Internal Reliability: We then assess the internal reliability of our model by looking at the Composite Reliability (CR) and Cronbach's alpha of each construct, which should have a value of 0.7 or higher [85, 86]. Here, we

6. https://jasp-stats.org/previous-versions/

TABLE 3. DESCRIPTIVE STATISTICS, CONVERGENT VALIDITY, INTERNAL CONSISTENCY, AND RELIABILITY OVER OUR CONSTRUCTS.

Construct	Item	Factor Loadings	Mean	SD	R^2	α	CR	AVE
Perceived control (CTRL)	CTRL_1	0.79	3.25	1.14	0.63	0.74	0.80	0.67
	CTRL_2	0.84	3.45	1.12	0.71			
Perceived risk (RISK)	RISK_1	0.93	3.07	1.07	0.86	0.90	0.94	0.88
	RISK_2	0.95	3.07	1.09	0.89			
Privacy concerns (PRIV)	PRIV_1	0.91	3.20	1.17	0.83	0.89	0.93	0.87
	PRIV_2	0.96	3.36	1.13	0.92			
Trust in data marketplaces operator (TRSD)	TRSD_1	0.90	3.43	0.89	0.81	0.90	0.93	0.82
	TRSD_2	0.90	3.35	0.87	0.80			
	TRSD_3	0.92	3.50	0.90	0.84			
Trust in data buyers (TRSB)	TRSB_1	0.94	3.06	1.01	0.89	0.95	0.97	0.93
	TRSB_2	0.98	3.09	1.02	0.95			
	TRSB_3	0.97	3.09	1.03	0.94			
Willingness to share data via data marketplaces (WTSD)	WTSD_1	0.97	3.06	1.15	0.94	0.94	0.96	0.90
	WTSD_2	0.95	2.99	1.12	0.91			
	WTSD_3	0.92	2.88	1.17	0.85			

Notes: SD = Standard Deviation; α = Cronbach's Alpha; CR = composite reliability; AVE = average variance extracted; We removed CTRL_3 due to low factor loadings, see Section 4.2

TABLE 4. DISCRIMINANT VALIDITY: CORRELATION AMONG CONSTRUCTS AND THE SQUARE ROOT OF THE AVE. DIAGONALS REPRESENT THE SQUARE ROOT OF THE AVERAGE VARIANCE EXTRACTED, AND OTHER VALUES REPRESENT THE CORRELATIONS.

	CTRL	RISK	PRIV	TRSD	TRSB	WTSD
CTRL	**0.82**					
RISK	-0.43	**0.94**				
PRIV	-0.34	0.75	**0.93**			
TRSD	0.45	-0.58	-0.52	**0.90**		
TRSB	0.37	-0.48	-0.45	0.68	**0.96**	
WTSD	0.43	-0.70	-0.61	0.61	0.57	**0.95**

find we establish convergent validity as all constructs have CR and Cronbach's alpha values greater than 0.8 and 0.74, respectively, see also Table 3.

Convergent Validity: Subsequently, we examine convergent validity through the Average Variance Extracted (*AVE*), which should be greater than 0.5, according to Fornell and Larcker [68]. We find all our constructs to satisfy this requirement, with the lowest *AVE* being 0.67 for perceived control and the highest value of 0.93 for trust in data buyers, again, see Table 3.

Discriminant Validity: We also examine the discriminant validity of the constructs by checking whether the correlation among constructs is lower than the square root of *AVE* [68].All inter-construct correlation coefficients are well below the square root of *AVE*, i.e., we also establish discriminant validity, see Table 4.

Multi-Group Confirmatory Factor Analysis: Finally, we run a Multi-Group Confirmatory Factor Analysis (MGCFA) to check whether all criteria are also met in the three treatment conditions we applied, i.e., across *all* responses and for each subset individually. We estimate the model using configural invariance testing and find a good level of the fit index, with $CFI = 0.980$, $TLI = 0.975$, and $RMSEA = 0.053$. All treatment conditions also show convergent and discriminant validity, with all factor loadings, CR, and Cronbach's alpha higher than 0.7 and AVE higher than 0.5. Furthermore, comparing the square root of AVE and all inter-construct correlation coefficients in all treatment conditions suggests discriminant validity.

TABLE 5. THE RESULTS OF ONE-WAY ANOVA FOR ALL CONSTRUCTS COMPARING THE TTP, MPC, AND DCP TREATMENT. NOTE THAT FROM $N = 1457$, THREE DATA LINES WERE NOT COMPLETE FOR ALL RELEVANT COMBINATIONS OF CONSTRUCTS RELEVANT HERE, LEADING TO A FINAL $N = 1454$ FOR THE ONE-WAY ANOVA, AS WE FILTERED THESE.

Construct		TTP (N=486)	MPC (N=484)	DCP (N=487)	F-Value	ω^2	p
CTRL	**M**	2.99	3.51	3.55	F(2, 1454) = 50.35	0.063	$<.001^{\ddagger}$
	SD	1.02	0.94	0.96			
RISK	**M**	3.45	3.17	3.22	F(2, 1454) = 9.49	0.012	$<.001^{\ddagger}$
	SD	1.06	1.09	1.10			
PRIV	**M**	3.28	2.95	2.98	F(2, 1454) = 15.38	0.019	$<.001^{\ddagger}$
	SD	1.00	1.05	1.01			
TRSD	**M**	3.37	3.46	3.46	F(2, 1454) = 2.21	0.002	0.11
	SD	0.83	0.80	0.79			
TRSB	**M**	2.96	3.16	3.12	F(2, 1454) = 5.65	0.006	$0.004^{\dagger}$
	SD	0.99	0.93	0.99			
WTSD	**M**	2.83	3.08	3.02	F(2, 1454) = 7.17	0.008	$<.001^{\ddagger}$
	SD	1.08	1.09	1.07			

Note: * p<.05, † p<.01, ‡ p<.001

4.3. Comparison Between TTP, MPC, and DCP

We first perform a MANOVA on the collected data to check whether antecedents of consumers' willingness to share data differ across our treatments (TTP, MPC, and DCP, see Section 3.1.2). We do this since we used a between-subject design with several antecedents of consumers' willingness to share data as multiple dependent variables. Subsequently, we conduct one-way ANOVAs to compare the effect of our treatments on each of the antecedents of consumers' data-sharing decisions (see Table 5). For the analysis, we use composite scores for each construct, derived from aggregating the scores of items belonging to each construct divided by the number of items. Further, we conduct Levene's test [73] to test for equal variances and find that the variances for each construct are equal across our treatment.

4.3.1. Comparison Overview. The MANOVA shows that there is a significant effect for *both* of our treatments on antecedents of consumers' data-sharing decisions (Pillai's trace$= 0.08$, $F(12, 2900) = 9.96, p < 0.001$) in comparison to the TTP case. The subsequent one-way ANOVAs (see Table 5) reveal a significant effect of our treatments on perceived control $[F(2, 1454) = 50.35, p < 0.001, \omega^2 = 0.06]$, perceived risk $[F(2, 1454) = 15.38, p <$

TABLE 6. THE RESULTS OF OUR POST-HOC COMPARISONS BETWEEN TTP, MPC, AND DCP. THE SAME FILTERING AS IN TABLE 5 APPLIES.

Construct	Comparison	Mean Δ	SE	df	t	p
CTRL	TTP - MPC	0.52	0.06	1454	-8.31	$< .001^{\ddagger}$
	TTP - DCP	-0.56	0.06	1454	-9.03	$< .001^{\ddagger}$
	MPC - DCP	-0.04	0.06	1454	-0.71	0.76
RISK	TTP - MPC	0.38	0.07	1454	5.00	$< .001^{\ddagger}$
	TTP - DCP	0.30	0.07	1454	4.58	$< .001^{\ddagger}$
	MPC - DCP	-0.03	0.07	1454	-0.43	0.904
PRIV	TTP - MPC	0.29	0.07	1454	4.11	$< .001^{\ddagger}$
	TTP - DCP	0.23	0.07	1454	3.32	$0.003^{\dagger}$
	MPC - DCP	-0.06	0.07	1454	-0.80	0.706
TRSB	TTP - MPC	-0.2	0.06	1454	-3.21	$0.004^{\dagger}$
	TTP - DCP	-0.15	0.06	1454	-2.47	0.036^{*}
	MPC - DCP	0.05	0.06	1454	0.74	0.737
WTSD	TTP - MPC	-0.25	0.07	1454	-3.61	$< .001^{\ddagger}$
	TTP - DCP	-0.19	0.07	1454	-2.80	0.014^{*}
	MPC - DCP	0.06	0.07	1454	0.81	0.696

Note: * p<.05, † p<.01, ‡ p<.001

$0.001, \omega^2 = 0.02]$, privacy concerns $[F(2, 1454) = 9.49, p < 0.001, \omega^2 = 0.01]$, trust in data buyers $[F(2, 1454) = 5.65, p = 0.004, \omega^2 = 0.01]$, and willingness to share data $[F(2, 1454) = 7.17, p < 0.001, \omega^2 = 0.01]$ at the $p < .05$ level. Reassuringly, we find no significant differences for our treatments concerning trust in the data marketplaces operator $[F(2, 1454) = 2.21, p = 0.11]$.

4.3.2. MPC vs. DCP. Next, we dive into the difference between MPC and the control treatment DCP by conducting a series of post hoc tests using Tukey's correction [47] to better account for outliers and address potential multiplicity issues, see also Table 6.

Control: Participants who received the MPC treatment perceive higher control over data (mean difference to TPP$= 0.52$, $p < 0.001$). In comparison, participants in the control DCP group also perceive a higher control over their data control (mean difference to TPP$= 0.56$, $p < 0.001$). Comparing both treatment groups with each other, i.e., MPC with DCP, we find no significant difference (mean difference $= 0.04$, $p \sim= 0.76$).

Trust in buyer: For participants in the MPC group, trust in data buyers increased (mean difference to TPP:$= 0.2$, $p < 0.05$). Participants in the DCP group saw a similar, even though slightly lower, increase in trust (mean difference to TTP $= 0.15$, $p < 0.036$). Here, changes to trust are also not influenced by either treatment (mean difference $= 0.05$, $p = 0.737$).

Willingness to share: Again, both groups (MPC and DCP) saw a higher willingness to share data when treated, with participants treated with MPC having a slightly higher mean difference and higher statistical significance (mean difference to TPP $= 0.25$, $p < 0.001$) than participants treated with DCP (mean difference to TPP $= 0.19$, $p < 0.01$). For a comparison between MPC and DCP, however, we again find no significant difference (mean difference $= 0.06$, $p = 0.696$).

Perceived risk: Similar to the other measures, perceived risk was reduced for MPC (mean difference to TPP $= 0.38$, $p < 0.001$) and DCP (mean difference to TPP $= 0.3$, $p < 0.001$) alike. As before, there is also no difference between the treatments (mean difference $= 0.03$, $p = 0.904$).

Privacy concerns: Finally, in both treatment conditions, also the level of privacy concerns was reduced, with MPC (mean difference to TPP $= 0.29$, $p < 0.001$) again showing a slightly higher impact than DCP (mean difference to TPP $= 0.23, p < 0.003$). Unsurprisingly, for the last measure, there again is no significant difference between MPC and the fictional control DCP mean difference $= 0.06$, $p = 0.706$).

4.3.3. Summary. To phrase our results more colloquially, both of our treatments (MPC and DCP) increase respondents' perceived control, lower their perceived risk, lessen their privacy concerns, increase their trust in data buyers, and ultimately increase their willingness to share data. However, comparing MPC with DCP, we did not find a significant difference. Furthermore, neither group (TTP, MPC, DCP) impacts respondents' trust in the data marketplace, so it is unlikely that a change in respondents' trust in the data marketplace influenced the results.

4.4. Effects of Control Variables

In addition to the core questions related to our study, our questionnaire included control variables to allow us to test whether our instrument may have missed additional main or interaction effects, i.e., to gauge its external validity. We perform two-way ANOVAs on these to test whether our control variables (i.e., Westin's Privacy Segmentation Index, industry type, car ownership, awareness of data marketplaces, and stated awareness of PETs) result in significant differences.

Before the analyses, we organized our sample depending on the control variables. We use the current classification for Westin's Privacy Segmentation Index without making any changes. For industry type, we assigned participants of non-IT industries to one group (non-IT), while the rest were assigned to another (IT). For car ownership, we assigned participants who do not own a car or only have access via rental or family members to one group (do not own a car), while the rest were assigned to the "own a car" group. Regarding awareness of data marketplaces, we assigned participants that (1) know data marketplaces but never share data, (2) share data once, or (3) share data multiple times as one group (aware of data marketplaces), while those who never heard of data marketplaces were classified as "not aware of data marketplaces" group. Finally, concerning awareness of PETs, those who were either aware of PETs before the survey or became aware because of the survey were assigned as one group (aware of PETs). The remaining participants were assigned to the "Unaware of PETs" group.

We find a significant main effect of Westin's Privacy Segmentation Index ($p < .001$ in all cases) and awareness of PETs ($p < .001$ in all cases except for "Trust in Data Buyers", where $p = 0.009$) on all constructs, e.g., those considered privacy fundamentalists are less likely to be willing to share personal data than privacy pragmatists. Industry

type also has a statistically significant main effect on trust in data buyers ($p = 0.006$ for "Trust in Data Buyers").

The remaining control variables have no significant main effects on any constructs. Furthermore, we find no interaction effects between control variables and our treatments. Please see Table 7 for the results of two-way ANOVA for the main, and Table 8 for the results of two-way ANOVA for the interaction effects of control variables.

5. Discussion

In this section, we interpret our core findings and discuss the implications of our results for researchers, industry, and policymakers alike.

5.1. Expectable Results

Following our methodology, the limited delta between the MPC and DCP treatments, and straight-forward intuition aligning with our findings, one might argue that the effect we quantitatively tested is one of the things *everyone knows*; Although our outcomes may initially appear obvious, our empirical data confirms the urgent need for greater awareness and attention to this problem.

Additionally, our methodology closely follows researchers' standard practices in applied privacy, usable security and privacy, and economics. However, we included our extra DCP condition as a placebo to enhance the rigor of our approach. Results of such studies are regularly the scientific foundation of projected adoption [123], investment decisions, and policy efforts. However, if our study had not included DCP as a control treatment, our results would indicate the significant promise of MPC for resolving common obstacles to realizing a privacy-friendly data economy and improving users' willingness to share personal data, i.e., our conclusion would have been similar to the results of related theoretical and empirical work, see also Section 2.

5.2. The 'Explanatory Gap' of PETs

Our study found comparable effects for an established PET (MPC) and a made-up PET (DCP) being claimed to be used. This suggests that our study technically produces a null-result regarding the difference between MPC and DCP. Despite the statistical significance of individual comparisons, we cannot make any qualitative statement on the impact of MPC on the metrics in our study, as the same effect is observed with a placebo (DCP); see Sec. 4. However, given that the pretense of using any PET remains the same, we conclude that in a study involving end-users, the main effects can be attributed to the pretense of a PET being used, regardless of its actual efficacy or even existence. We attribute this to the high-level explanation necessary to describe a PET in an end-user-accessible manner. However, such explanations are necessary, as expecting the user to become an expert and assess the technology behind PETs is not feasible. Consequently, users must give the companies a leap of faith and *trust* their PET's description of how it works and whether it accomplishes its promises. Lakkaraju and Bastani [117] already explored in 2020 how users' trust can be misled by providing malicious explanations, in which they included features/wording that users believe are relevant and omitted those that users believe could be problematic. Hence, connecting to tangential work from other domains [88], we call the underlying issue the *Explanatory Gap of PETs*[7].

5.3. A False Sense of Privacy

The *Explanatory Gap of PETs* regularly appears implicitly in related work [24, 75, 77, 103] and is a core issue of usable security and privacy, going back to its roots [175, 184]. However, there does not seem to be a fundamental solution. An even more worrying fact is that as technology becomes increasingly pervasive in our lives, the quantity of data that can be extracted from us is concomitantly growing. This, in turn, increases its value on data markets [96], which leads to user data often being referred to as 'The New Gold' [11][8].

The consequence for the users is that, due to the higher number of data violation incidents [36], they become increasingly aware of the value of their privacy [147], and their demand for deployment of PETs increase accordingly [9]. The consequence for the industry is that it becomes increasingly difficult to protect this data, i.e., especially with progressing cloudification, it is challenging to know *which* data they store *where* and share with *whom* [67]. This leads to increased costs due to data breaches [97], a growing number of regulations [62, 140] and, luckily, a growing adoption of PETs [159], trying to meet the perceived demand of users. However, in our study, participants who were treated with the *claim* of a PET being used showed a significantly higher willingness to share data than participants in the control group; see Sec. 4.3.3). Considering the treatment DCP to be a fictitious PET, we conclude that just the *claim* of it being used created a *false sense of privacy* (FSP) in the participants. As the everyday user generally lacks the mental models of specific PETs, FSP risks users disclosing more data to such a service, assuming that it is adequately protected. This renders the integration of PETs harmful, as it conflicts with the concept of data minimization (Sec. 2.1) [174]. Ultimately, from a service provider's perspective, when trying to convince users to share personal data, it is not about a technology being a *working* solution for privacy but about making users *believe* that it is.

Examples of this issue materializing in practice are equally prevalent. Companies claiming to protect the user's

7. The term 'Explanatory Gap' is used in the domain of Philosophy [88] to describe the gap between experienced cognitive processes and the available physical explanations.

8. The authors rather agree with the alternative notion 'Data is the New Oil': Similar to oil, once it spills, the beaches will be soiled and it is close to impossible to get all of it back into the barrel.

9. The increased demand is reflected in the growing market value of PETs [96].

TABLE 7. THE RESULTS OF TWO-WAY ANOVA FOR MAIN EFFECTS. AS IN TABLE 5, WE FILTERED LINES NOT HOLDING DATA FOR ALL COMPARED CONSTRUCTS, LEADING TO A REDUCTION BY NINE TO $N = 1448$ FOR WESTIN, AND BY SIX TO $N = 1451$ FOR THE REMAINING EFFECTS.

Construct	WESTIN		INDUSTRY		CAR		DMP		PETS	
	F-value	p	F-value	p	F-value	p	F-value	p	F-value	p
CTRL	F(2, 1448) = 49.03	<.001‡	F(1, 1451) = 0.07	0.786	F(1, 1451) = 0.73	0.393	F(1, 1451) = 0.5	0.481	F(1, 1451) = 19.76	<.001‡
RISK	F(2, 1448) = 116.52	<.001‡	F(1, 1451) = 0.31	0.58	F(1, 1451) = 0.9	0.343	F(1, 1451) = 0.21	0.644	F(1, 1451) = 18.69	<.001‡
PRIV	F(2, 1448) = 108.29	<.001‡	F(1, 1451) = 0.34	0.559	F(1, 1451) = 0.01	0.935	F(1, 1451) = 0.13	0.716	F(1, 1451) = 18.3	<.001‡
TRSD	F(2, 1448) = 162.75	<.001‡	F(1, 1451) = 2.39	0.122	F(1, 1451) = 0.54	0.463	F(1, 1451) = 3.18	0.075	F(1, 1451) = 15.12	<.001‡
TRSB	F(2, 1448) = 163.23	<.001‡	F(1, 1451) = 7.69	0.006*	F(1, 1451) = 0.09	0.77	F(1, 1451) = 0.43	0.513	F(1, 1451) = 6.77	0.009†
WTSD	F(2, 1448) = 128.15	<.001‡	F(1, 1451) = 0.01	0.906	F(1, 1451) = 0.01	0.907	F(1, 1451) = 3.34	0.068	F(1, 1451) = 16.04	<.001‡

Notes: WESTIN = Westin's Privacy Segmentation Index; INDUSTRY = Industry type; CAR = Car ownership; DMP = awareness of data marketplaces; PETS = awareness of Privacy-Enhancing Technologies (PETs);
* p<.05, † p<.01, ‡ p<.001

TABLE 8. THE RESULTS OF TWO-WAY ANOVA FOR THE INTERACTION EFFECT BETWEEN DATA SHARING APPROACHES AND CONTROL VARIABLES. WE APPLIED THE SAME FILTERS AS IN TABLE 7 FOR DATA LINES THAT WERE INCOMPLETE FOR SPECIFIC EFFECT COMBINATIONS.

Construct	SCENARIOxWESTIN		SCENARIOxINDUSTRY		SCENARIOxCAR		SCENARIOxDMP		SCENARIOxPETS	
	F-value	p	F-value	p	F-value	p	F-value	p	F-value	p
CTRL	F(4, 1448) = 0.41	0.805	F(2, 1451) = 2.32	0.099	F(2, 1451) = 0.44	0.643	F(2, 1451) = 5.58	0.004†	F(2, 1451) = 1.21	0.299
RISK	F(4, 1448) = 0.15	0.962	F(2, 1451) = 0.51	0.603	F(2, 1451) = 2.61	0.432	F(2, 1451) = 2.61	0.074	F(2, 1451) = 0.65	0.523
PRIV	F(4, 1448) = 0.28	0.89	F(2, 1451) = 0.23	0.793	F(2, 1451) = 0.85	0.743	F(2, 1451) = 0.85	0.43	F(2, 1451) = 1.13	0.323
TRSD	F(4, 1448) = 0.3	0.88	F(2, 1451) = 1.04	0.354	F(2, 1451) = 2.49	0.519	F(2, 1451) = 2.49	0.083	F(2, 1451) = 1.24	0.29
TRSB	F(4, 1448) = 1.77	0.132	F(2, 1451) = 0.21	0.814	F(2, 1451) = 1.32	0.342	F(2, 1451) = 1.32	0.266	F(2, 1451) = 0.37	0.694
WTSD	F(4, 1448) = 1.05	0.38	F(2, 1451) = 0.02	0.983	F(2, 1451) = 2.1	0.199	F(2, 1451) = 2.1	0.122	F(2, 1451) = 0.49	0.612

Notes: SCENARIO = Data sharing approaches(TTP/MPC/DCP); WESTIN = Westin's Privacy Segmentation Index; INDUSTRY = Industry type; CAR = Car ownership; DMP = awareness of data marketplaces; PETS = awareness of Privacy-Enhancing Technologies (PETs)
* p<.05, † p<.01, ‡ p<.001

privacy by, e.g., using suitable PR campaigns [4, 183], were later identified by research to neglect their promise [109, 121] or fined by the authorities for violating data protection regulations [89]. Utilizing dark patterns is another state-of-the-art method to lure users into disclosing more data [23, 180].

5.4. A Matter of Trust and Verifiability

At their core, the 'Explanatory Gap' and 'False Sense of Privacy' are not *technical* problems. Instead, they are the culmination of the complexity of PETs and the resulting lack of mental models of users, and not to be neglected, the market dynamics and monetary incentives *encouraging* companies to leverage the 'Explanatory Gap' and 'False Sense of Privacy' to increase users' willingness to share data.

In his lecture "Reflections on Trusting Trust", Ken Thompson advised users on how to trust the systems they are using: "Don't." [175]. However, as this extreme advice is not practicable, we need to find a way to improve the status quo at least. We argue that there needs to be a fundamental shift in how the community and companies handle PETs: From pushing individual technologies to focusing on the tangible *privacy properties*, they aim to provide [78].

To put this into an example, instead of claiming the use of *asymmetric end-to-end encryption*, the claim should be instead *ensuring that exclusively sender and recipient can read a message exchanged between the two*. This might sound like simply using more accessible language, a frequently recommended approach [103]. However, technically, the wording *asymmetric end-to-end encryption* already simplifies the corresponding encryption protocol, along with its diverse variants and configurations.

What actually changes in such wording is the claim to be tested becomes independent of the technology used to realize it. For users, this more clearly communicates the role of *them having to trust*. At the same time, for auditors and oversight bodies, it provides a clear set of properties to, e.g., formally, during audits, or in certification processes, *test* for. Also, users (and other relevant stakeholders) are not required to adapt their mental models as soon as a technology surpasses its hype cycle, and a *new* PET would technically take place in the description.[10] Consequently, it is not relevant *which* technology is used as long as it provides the promised privacy properties.

While 'Open Source' could be a fundamental component of this approach, it stretches beyond, ultimately to an extension of Kerckhoffs's principle [106]: Opening systems in terms of their source code, but also *documentation*, opens both to public and regulatory scrutiny. This approach increases the chance that incorrectly claimed security and privacy properties, whether through human error [103] or malicious intent, can be detected. Additionally, open standards enable *choice* for users by encouraging interoperability and, therefore, the potential for data portability. This would make it easier for users to vote with their feet if an operator or company loses their trust.

10. This naturally does not imply that services should not *also* publish an in-depth technical description/whitepaper *in addition*, explaining *how* they accomplish the specific privacy properties for domain experts.

In summary, the proposed shift in the community's approach is comparatively subtle and does not eliminate the user's need to trust someone. However, it shifts the trust from an individual service provider's commercial incentives to the engagement of a whole privacy-aware community and regulatory oversight while more clearly communicating the *trust* required by users.

5.5. Implications for Policy-Makers

Verifiable privacy properties are useless if no independent party verifies them. Current commercial approaches such as Pentest Certificates or IT-Security Labels [30], offered by Germany's Authorities, aim to demonstrate the *absence* of vulnerabilities in a given scenario or context. Instead, we call for an approach towards demonstrating the *presence* of privacy properties. Instead of testing the unscoped question of "Is this secure?", it has to be tested whether made claims regarding privacy properties are sufficiently realized.

At this point, we see policy makers as the only party to counterbalance the incentive structure of the industry. They could seize their role of 'keeping the industry honest' by, e.g., establishing certification processes for software vendors, well-established processes from the sectors of medical [136], automotive [53, 176] or food industry [66]. After verifying the privacy property claims in their software products, vendors could obtain an attestation that users can rely on. Furthermore, authorities should proactively investigate privacy issues, i.e., not rely on users reporting concerns before coming into action. Given that users' behavior seems to be perception-focused, this way, regulators would not work reactively, i.e., reacting to users' complaints, but instead proactively.

However, this approach requires policymakers to alter applicable legislation to enable the proactive investigations necessary to ensure organizations adhere to their promises and the rules that apply.

5.6. Implications for Industry

Cynically, the main implication of our results on industry players could be that it does not matter if they implement PETs as long as they can convince their customers to do so. Nevertheless, we argue that the industry's motivation to implement PETs should not be rooted in its positive impact on users' willingness to buy their products and/or share their data when utilizing a service. Instead, they should focus on implementing verifiable privacy properties in their products and proving this to their customers via official certification processes. Certificates can be a competitive advantage, as they can improve the credibility and recognition among customers by demonstrating the trustworthiness of a product or service [10, 63, 118]. However, we acknowledge that this would require a change in market dynamics, e.g., through the aforementioned policy actions.

Another beneficial side effect for the industry is that they do not need to rely on the hype cycle of new technologies [123]. According to Funk, "[technological] hype wastes resources and time and distracts from more plausible pathways for improving productivity or solving social problems." [69]. Since the domains of Formal Verification and Privacy and Security properties are fundamental aspects of Computer Science, they can be assumed less susceptible to named hype cycles and, therefore, more reliable selling points in the long run. [11]

5.7. Recommendations for Future Research

The domain of formal verification is well-established in Computer Science, with Verifiable Cryptography being a well-established subdomain [20]. To the best of our knowledge, there are no practically applicable formal specification and verification methods for privacy properties. However, theoretical prior work exists that can be built upon [1, 25, 65, 90, 151, 193]. Therefore, we encourage the research community to investigate further the feasibility of formal specification and verification of privacy properties, and to develop appropriate methods that can be implemented by policy makers and industry alike.

Our results demonstrate that the impact of new PETs on users' decision-making is difficult to observe in a lab environment. Technically, to make a qualified statement about the impact of a specific technology, a study design must ensure that participants understand what a given PET *does* and what guarantees it can provide. However, if a survey would provide more detailed information about the technology, real-world circumstances would not necessarily be reflected, where users are usually confronted with product-positive marketing campaigns [4, 183], and not with detailed technical specifications or privacy policies [134]. Furthermore, such more in-depth descriptions would likely introduce additional side effects, e.g., based on individual respondents' familiarity or even expertise in the topic.

Furthermore, past research demonstrated that it is notoriously difficult to accurately communicate how a given PET works without oversimplifying or being too complex. For example, experts and non-experts showing surprisingly similar mental models for, e.g., VPNs [24], operators having limited mental models of, e.g., HTTPS [114], or programmers being challenged by implementing basics of secure development [2, 80]. Self-reported efficacy of participants is notoriously unreliable due to a variety of effects; First and foremost, but certainly not only, social desirability effects [70]. Similarly, *testing* whether a participant *understands* how a technology works is even more difficult, as seen in the related field of assessing learning outcomes [6, 26]. Hence, it would be hardly feasible to attain a census-representative population of participants who are sure to be sufficiently versed in a PET's inner workings to adequately understand a study's stated technical premises regarding a PET.

11. We note that, technically, this more somber perspective on privacy attestation may be able to become a hype term by itself. However, if the hype concerns a more honest description of privacy properties, we argue that the effect differs from the hype around a specific technology.

Hence, we suggest following related work on learning [6, 26], which recommends to not focus on assessing 'understanding', but instead test capabilities, e.g., e.g., can explain/analyze/etc., possibly enhanced with drawings or similar expressive aids. This, as done by, e.g., Binkhorst et al. [24] and Krombholz et al. [114], allows assessing a participant's mental model of a PET and subsequently comparing it to an expert assessment. Still, given that this approach is qualitative, it will be challenging to execute for quantitative work.

5.8. Limitations

As with all empirical research, our study has limitations to consider when assessing its conclusions. First, we excluded perceived benefits in our model of data sharing willingness, despite this having been identified as a dominant factor in explaining an individual's data sharing decisions [46]. However, as we focus on the impact of MPC and DCP, respectively, compared to each other and a baseline, we instead decided not to include this variable to keep the model simple. We accomplish this by instructing participants, regardless of the treatment condition, that they *would*, as the scenario is hypothetical, be paid for data sharing, again equal for all treatments. However, this also means that our results are not directly generalizable to circumstances where the perceived benefits may differ along with claimed PETs.

Similarly, our scenario did not include additional information that may positively influence participant's disposition toward the data marketplace or data buyers, e.g., claiming that a certification process or regular audits are in place. However, for the same simplicity reasons stated above, we decided not to include this variable in the models. Consequently, the same considerations also apply.

Furthermore, our study is built on hypothetical scenarios and mock-ups that are not working prototypes. However, this is a common practice in the field, and the exact approach/scenario we aimed to investigate is shown in Sec. 2. Nevertheless, it means that effects may differ for cases where, e.g., a design science research (DSR) approach is used to develop an artifact or at least a seemingly working mock-up of a PET to demonstrate the evaluated scenario.

Another point to consider is the timing of our survey. The data collection was conducted in 2021 during the waning phase of the COVID-19 pandemic. Public restrictions during this time accelerated digitalization in many public and private sectors. This led to extensive use of tools for pandemic tracking, remote communication, payment, and others. According to a study in 2023, people perceive a possible routinization of [...] using apps and the need to choose a trade-off between their personal privacy and public health: "Participants routinely expected that data collected through apps related to public health would be shared with unknown third parties" (Seberger and Patil, 2023 [164]). It is difficult to determine whether and how much this change in users' perception impacted the outcome of our study. However, this emphasizes the need to repeat our study later to identify possible impacts.

Finally, we work with a census representative sample from the U.K.'s population. Hence, our findings are limited in their generalizability beyond the U.K. — or at least generally western — populations. Such a survey requires a more extensive study, considering additional factors such as culture, demographics, and prior experiences with privacy infringement's [76].

6. Conclusion

In this paper, we build upon information privacy theory from the fields of economics and human factors in security and privacy to investigate the impact of using secure Multi-Party-Computation on consumers' data-sharing decisions. We use a double-blind, randomized control trial with a between-subject design conducted via an online survey with three mock-ups of personal data marketplaces. We find, statistically robust, that the sole claim of implementing a PET, not the specifically named PET, is sufficient to increase consumers' trust in data buyers, reduce perceptions of risks, and lower privacy concerns, ultimately increasing willingness to share. Our key takeaways are:

- The specific name of a PET does not necessarily influence how users' trust and willingness to share data are influenced in a study. Instead, the high-level description and presentation of a PET are the significant factors. This must be considered when interpreting studies that claim to find a significant impact of a (new) PET on users' trust.
- Beyond academic studies, the implied–effectively–black-box nature of PETs means that especially users with a lack of understanding of how a PET works and whether it is effective must *trust* descriptions and claims. The resulting issue, which we name 'The Explanatory Gap of PETs,' allows monetary-motivated actors to mislead users into sharing more data.
- This 'Explanatory Gap of PETs' leaves the user with no choice but to either trust a vendor's privacy protection claims or not. If the user decides to trust, it potentially fosters a "False Sense of Privacy", i.e., the risk of passing on more data than he would have done if he had fully understood the circumstances.
- Hence, development and investment decisions rooted in studies on how users' trust changes by (claiming to be) using a PET need to be critically assessed, especially by regulators.

Finally, our work highlights an intrinsic dilemma of privacy-enhancing technologies, which follows directly from Ken Thompson's 'Reflections on Trusting Trust' [175]: "Ultimately everyone must trust that what the screen shows is actually what is really happening."

References

[1] A. Abe and A. Simpson. "Formal Models for Privacy." In: *EDBT/ICDT Workshops*. 2016.

[2] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. L. Mazurek, and C. Stransky. "Comparing the usability of cryptographic APIs". In: *2017 IEEE Symposium on Security and Privacy (SP)*. 2017.

[3] T. L. Adams, Y. Li, and H. Liu. "A replication of beyond the turk: Alternative platforms for crowdsourcing behavioral research–sometimes preferable to student groups". In: *AIS Transactions on Replication Research* 1 (2020).

[4] M. A. L. Agency TBWA. *Apple.Privacy. That's iPhone.* 2023. URL: https://www.youtube.com/watch?v=ZL95c-ojWdk.

[5] N. Agrawal, R. Binns, M. Van Kleek, K. Laine, and N. Shadbolt. "Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021.

[6] G. S. Alaghbary. "Integrating technology with Bloom's revised taxonomy: Web 2.0-enabled learning designs for online learning". In: *Asian EFL Journal* 1 (2021).

[7] Alasdiar Ferguson. *Angus: Ukrainian refugee's personal details released after data breach*. https://www.thenational.scot/news/24524487.angus-ukrainian-refugees-personal-details-released-data-breach/. accessed: Aug. 2024. 2024.

[8] T. Alashoor, S. Han, and R. C. Joseph. "Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model". In: *Communications of the Association for Information Systems* 1 (2017).

[9] G. Alter, B. H. Falk, S. Lu, and R. Ostrovsky. "Computing Statistics from Private Data". In: *Data Science Journal* (2018).

[10] S. W. Anderson, J. D. Daly, and M. F. Johnson. "Why firms seek ISO 9000 certification: regulatory compliance or competitive advantage?" In: *Production and operations management* 1 (1999).

[11] J. Angwin. "The web's new gold mine: Your secrets". In: *Wall Street Journal* 07 (2010).

[12] D. W. Archer, D. Bogdanov, Y. Lindell, L. Kamm, K. Nielsen, J. I. Pagter, N. P. Smart, and R. N. Wright. "From Keys to Databases—Real-World Applications of Secure Multi-Party Computation". In: *The Computer Journal* 12 (2018).

[13] A. Aslan, M. Greve, T. Diesterhöft, and L. Kolbe. *Can Our Health Data Stay Private? A Review and Future Directions for IS Research on Privacy-Preserving AI in Healthcare*. Wirtschaftsinformatik 2022 Proceedings. 2022. URL: https://aisel.aisnet.org/wi2022/digital_health/digital_health/8.

[14] AT&T. *AT&T Addresses Illegal Download of Customer Data*. https://about.att.com/story/2024/addressing-illegal-download.html. accessed: Aug. 2024. 2024.

[15] S. A. Azcoitia and N. Laoutaris. "A survey of data marketplaces and their business models". In: *ACM SIGMOD Record* 3 (2022).

[16] P. Baecke and L. Bocca. "The value of vehicle telematics data in insurance risk selection processes". In: *Decision Support Systems* (2017).

[17] D. Balson and W. Dixon. *Cyber Information Sharing: Building Collective Security*. World Economic Forum, 2020. URL: https://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf.

[18] R. Bandara, M. Fernando, and S. Akter. "Addressing privacy predicaments in the digital marketplace: A power-relations perspective". In: *International Journal of Consumer Studies* 5 (2020).

[19] P. Baran. "On Distributed Communications:: IX. Security, Secrecy, and Tamper-Free Considerations". In: (1964).

[20] M. Barbosa, G. Barthe, K. Bhargavan, B. Blanchet, C. Cremers, K. Liao, and B. Parno. "SoK: Computer-Aided Cryptography". In: *2021 IEEE Symposium on Security and Privacy (SP)*. 2021.

[21] J. Bareis. *BigTech's Efforts to Derail the AI Act*. https://verfassungsblog.de/bigtechs-efforts-to-derail-the-ai-act/. 2023. (Visited on 11/11/2024).

[22] K. A. Batterton and K. N. Hale. "The Likert scale what it is and how to use it". In: *Phalanx* 2 (2017).

[23] B. M. Berens, M. Bohlender, H. Dietmann, C. Krisam, O. Kulyk, and M. Volkamer. "Cookie disclaimers: Dark patterns and lack of transparency". In: *Computers & Security* (2024).

[24] V. Binkhorst, T. Fiebig, K. Krombholz, W. Pieters, and K. Labunets. "Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context". In: *31st USENIX Security Symposium (USENIX Security 22)*. 2022.

[25] F. Biondi and A. Legay. "Security and privacy of protocols and software with formal methods". In: *International Symposium on Leveraging Applications of Formal Methods*. 2016.

[26] B. S. Bloom, M. D. Engelhart, E. J. Furst, W. H. Hill, D. R. Krathwohl, et al. *Taxonomy of educational objectives: The classification of educational goals. Handbook 1: Cognitive domain*. Longman New York, 1956.

[27] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft. "Secure Multiparty Computation Goes Live". In: *Financial Cryptography and Data Security*. 2009.

[28] E. M. Boucher, H. E. Ward, A. C. Mounts, and A. C. Parks. "Engagement in Digital Mental Health Interventions: Can Monetary Incentives Help?" In: *Frontiers in Psychology* (2021). (Visited on 11/08/2024).

[29] T. A. Brown and M. T. Moore. "Confirmatory factor analysis". In: *Handbook of Structural Equation Modeling* (2012).

[30] BSI. *The IT Security Label for manufacturers*. 2024. URL: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/fuer-Hersteller/IT-SiK-fuer-hersteller_node.html.

[31] C. Buck and R. Reith. "Privacy on the road? Evaluating German consumers' intention to use connected cars". In: *International Journal of Automotive Technology and Management* 3 (2020).

[32] V. Buterin, J. Illum, M. Nadler, F. Schär, and A. Soleimani. "Blockchain privacy and regulatory compliance: Towards a practical equilibrium". In: *Blockchain: Research and Applications* 1 (2024).

[33] A. Calvi, G. Malgieri, and D. Kotzinos. "The unfair side of Privacy Enhancing Technologies: addressing the trade-offs between PETs and fairness". In: *The 2024 ACM Conference on Fairness, Accountability, and Transparency*. 2024.

[34] D. T. Campbell and J. C. Stanley. *Experimental and quasi-experimental designs for research*. Ravenio books, 2015.

[35] D. T. Campbell and D. W. Fiske. "Convergent and discriminant validation by the multitrait-multimethod matrix." In: *Psychological bulletin* 2 (1959).

[36] I. T. R. Center. *Number of data violation incidents and individuals impacted in the United States from 1st quarter 2021 to 1st quarter 2024*. https://www.statista.com/statistics/1418469/us-number-of-data-compromises-individuals-affected/ last accessed Aug. 2024. 2024.

[37] V. Charitsis, D. Zwick, and A. Bradshaw. "Creating worlds that create audiences: theorising personal data markets in the age of communicative capitalism". In: (2018).

[38] G. Charness, U. Gneezy, and M. A. Kuhn. "Experimental methods: Between-subject and within-subject design". In: *Journal of Economic Behavior & Organization* 1 (2012).

[39] D. L. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms". In: *Communications of the ACM* 2 (1981). (Visited on 11/11/2024).

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

[41] P. Cichy, T.-O. Salge, and R. Kohli. *Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars*. MIS Quarterly, 2021.

[42] E. Commission. "A European strategy for data". 2020. URL: https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf.

[43] E. D. P. B. P. Consultation. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. Jan. 2020. URL: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/inpher-_edpb_supplementary_measures_comment.pdf (visited on 03/11/2025).

[44] K. P. Coopamootoo and T. Groß. "Why privacy is all but forgotten". In: *Proceedings on Privacy Enhancing Technologies* (2017).

[45] R. E. Crossler and F. Bélanger. "The mobile privacy-security knowledge gap model: Understanding behaviors". In: (2017).

[46] M. J. Culnan and P. K. Armstrong. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation". In: *Organization Science* 1 (1999).

[47] F. David and J. Tukey. "Exploratory data analysis". In: *Biometrics* 4 (1977).

[48] S. Derikx, M. De Reuver, and M. Kroesen. "Can privacy concerns for insurance of connected cars be compensated?" In: *Electronic markets* (2016).

[49] T. Dinev, V. Albano, H. Xu, A. D'Atri, and P. Hart. "Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective". In: *Advances in Healthcare Informatics and Analytics*. 2016.

[50] T. Dinev and P. Hart. "An extended privacy calculus model for e-commerce transactions". In: *Information Systems Research* 1 (2006).

[51] B. Ding, J. Kulkarni, and S. Yekhanin. "Collecting telemetry data privately". In: *Advances in Neural Information Processing Systems* (2017).

[52] Y. Ding, C. Chen, S. Zhang, B. Guo, Z. Yu, and Y. Wang. "Greenplanner: Planning personalized fuel-efficient driving routes using multi-sourced urban data". In: *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. 2017.

[53] E. Directorate General for Internal Market Industry and SMEs. *CE marking*. 2022. URL: https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm.

[54] S. I. Donaldson and E. J. Grant-Vallone. "Understanding self-report bias in organizational behavior research". In: *Journal of business and Psychology* (2002).

[55] J. L. Dupree, R. Devries, D. M. Berry, and E. Lank. "Privacy personas: Clustering users via attitudes and behaviors toward security practices". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 2016.

[56] C. Dwork. "Differential Privacy". In: *Automata, Languages and Programming*. 2006.

[57] C. Dwork and A. Roth. "The Algorithmic Foundations of Differential Privacy". In: *Foundations and Trends® in Theoretical Computer Science* 3-4 (2014).

[58] T. J. Edison. *Learning new words*. https://patents.google.com/patent/US9594741B1/en. 2017.

[59] M. B. van Egmond. *Identifying heart failure patients at high risk using MPC*. The Sugar Beet: Applied MPC, 2020. URL: https://medium.com/applied-mpc/identifying-heart-failure-patients-at-high-risk-using-mpc-ab8900e75295.

[60] R. Eichler, C. Gröger, E. Hoos, H. Schwarz, and B. Mitschang. "From data asset to data product–the role of the data provider in the enterprise data marketplace". In: *Symposium and Summer School on Service-Oriented Computing*. 2022.

[61] R. Eichler, C. Gröger, E. Hoos, C. Stach, H. Schwarz, and B. Mitschang. "Introducing the enterprise data marketplace: a platform for democratizing company data". In: *Journal of Big Data* 1 (2023).

[62] European Commission. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[63] J. M. T. Farinha, D. Galar, I. A. Fonseca, and U. Kumar. "Certification of maintenance providers: A competitive advantage". In: *Journal of Quality in Maintenance Engineering* 2 (2013).

[64] R. Farrelly and E. Chew. "Who's in to win?: Participation rate in a primary personal information market". 2016.

[65] M. Fazouane, H. Kopp, R. W. van der Heijden, D. Le Métayer, and F. Kargl. "Formal verification of privacy properties in electric vehicle charging". In: *Engineering Secure Software and Systems: 7th International Symposium, ESSoS 2015, Milan, Italy, March 4-6, 2015. Proceedings 7*. 2015.

[66] FDA. *Hazard Analysis Critical Control Point (HACCP)*. 2024. URL: https://www.fda.gov/food/guidance-regulation-food-and-dietary-supplements/hazard-analysis-critical-control-point-haccp.

[67] T. Fiebig, M. Lindorfer, and S. Gürses. "Position Paper: Escaping Academic Cloudification to Preserve Academic Freedom". In: *Privacy Studies Journal* 1 (2022).

[68] C. Fornell and D. F. Larcker. "Evaluating structural equation models with unobservable variables and measurement error". In: *Journal of Marketing Research* 1 (1981).

[69] J. Funk. "What's behind technological hype?" In: *Issues in Science and Technology* 1 (2019).

[70] D. C. Ganster, H. W. Hennessey, and F. Luthans. "Social desirability response effects: Three alternative models". In: *Academy of Management Journal* 2 (1983).

[71] G. M. Garrido, X. Liu, F. Matthes, and D. Song. "Lessons learned: Surveying the practicality of differential privacy in the industry". In: *arXiv preprint arXiv:2211.03898* (2022).

[72] Gartner. *Gartner Says Digital Ethics is at the Peak of Inflated Expectations in the 2021 Gartner Hype Cycle for Privacy*. 2021. URL: https://www.gartner.com/en/newsroom/press-releases/2021-09-30-gartner-says-digital-ethics-is-at-the-peak-of-inflate.

[73] J. L. Gastwirth, Y. R. Gel, and W. Miao. "The impact of Levene's test of equality of variances on statistical theory and practice". In: *Statistical Science* 3 (2009).

[74] C. Gentry. "Fully homomorphic encryption using ideal lattices". In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. 2009.

[75] N. Gerber, V. Zimmermann, B. Henhapl, S. Emeröz, and M. Volkamer. "Finally johnny can encrypt: But does this make him feel more secure?" In: *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 2018.

[76] N. Gerber, P. Gerber, and M. Volkamer. "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior". In: *Computers & security* (2018).

[77] N. Gerber, V. Zimmermann, B. Henhapl, S. Emeröz, and M. Volkamer. "Finally johnny can encrypt: But does this make him feel more secure?" In: *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 2018.

[78] G. Gilboa-Freedman and R. Smorodinsky. "On the properties that characterize privacy". In: *Mathematical Social Sciences* (2020).

[79] I. Goldberg, D. Wagner, and E. Brewer. "Privacy-Enhancing Technologies for the Internet". In: *Proceedings IEEE COMPCON 97. Digest of Papers*. 1997. (Visited on 11/08/2024).

[80] P. L. Gorski, Y. Acar, L. Lo Iacono, and S. Fahl. "Listen to developers! a participatory design study on security warnings for cryptographic apis". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 2020.

[81] S. D. Gowda. "Secure Multiparty Computation: Protocols, Collaborative Data Processing, and Real-World Applications in Industry". In: *Cloud Security*. 2024.

[82] C. Greaney. "Data Privacy in the Age of Surveillance Capitalism". In: *EDITORIAL–From the Senior Editor* (2020).

[83] J. Guffey and Y. Li. "Cloud Service Misconfigurations: Emerging Threats, Enterprise Data Breaches and Solutions". In: *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. 2023.

[84] S. Gürses and B. Berendt. "PETs in the surveillance society: a critical review of the potentials and limitations of the privacy as confidentiality paradigm". In: *Data Protection in a Profiled World* (2010).

[85] J. F. Hair, C. M. Ringle, and M. Sarstedt. "PLS-SEM: Indeed a silver bullet". In: *Journal of Marketing Theory and Practice* 2 (2011).

[86] J. F. Hair, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser. *Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research*. European Business Review, 2014.

[87] Y. Hanif and H. S. Lallie. "Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with

perceived cyber security, risk, and trust". In: *Technology in Society* (2021).
[88] G. Harman. "Explaining an explanatory gap". In: *APA Newsletter on Philosophy and Computers* 02 (2007).
[89] Helen Dixon. *Data Protection Commission announces conclusion of two inquiries into Meta Ireland*. 2023. URL: https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.
[90] L. Hirschi, D. Baelde, and S. Delaune. "A method for verifying privacy-type properties: the unbounded case". In: *2016 IEEE Symposium on Security and Privacy (SP)*. 2016.
[91] L. Hu and P. M. Bentler. "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives". In: *Structural Equation Modeling: A Multidisciplinary Journal* 1 (1999).
[92] L. Huang, Y. Dou, Y. Liu, J. Wang, G. Chen, X. Zhang, and R. Wang. "Toward a research framework to conceptualize data as a factor of production: The data marketplace perspective". In: *Fundamental Research* 5 (2021).
[93] T. Hughes-Roberts. "Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behaviour?" In: *2013 International Conference on Social Computing*. 2013.
[94] Z. V. C. Inc. *Zoom Privacy Statement*. https://explore.zoom.us/en/privacy/ last accessed Aug. 2024. 2024.
[95] U. Information Commissioner's Office. *Chapter 5: privacy-enhancing technologies (PETs)*. https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf. 2023. (Visited on 11/11/2024).
[96] C. Institute. *Customer data platform industry revenue worldwide from 2020 to 2023*. https://www.statista.com/statistics/1293577/customer-data-platform-industry-revenue/ last accessed Aug. 2024. 2024.
[97] P. Institute. *Average cost of a data breach in the United States from 2006 to 2023*. https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/ last accessed Aug. 2024. 2024.
[98] L. H. Iwaya, M. A. Babar, and A. Rashid. "Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices". In: *IEEE Transactions on Software Engineering* 9 (2023). (Visited on 11/08/2024).
[99] C. Jensen, C. Potts, and C. Jensen. "Privacy practices of Internet users: Self-reports versus observed behavior". In: *International Journal of Human-Computer Studies* 1 (2005).
[100] J. Jentsch, A. B. Ünal, Ş. S. Mağara, and M. Akgün. *Privacy Preserving Data Imputation via Multi-party Computation for Medical Applications*. May 2024. arXiv: 2405.18878 [cs]. (Visited on 03/11/2025).
[101] N. Kato, Y. Murakami, T. Endo, and K. Nawa. "Study on privacy setting acceptance of the drivers for the data utilization on the car". In: *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. 2016.
[102] N. Kaufmann, T. Schulze, and D. Veit. "More than fun and money: Worker motivation in crowdsourcing-a study on Mechanical Turk". 2011.
[103] M. Kaur, M. van Eeten, M. Janssen, K. Borgolte, and T. Fiebig. "Human factors in security research: Lessons learned from 2008-2018". In: *arXiv preprint arXiv:2103.13287* (2021).
[104] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch. "Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus". In: *Information Systems Journal* 6 (2015).
[105] M. J. Keith, S. C. Thompson, J. Hale, P. B. Lowry, and C. Greer. "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior". In: *International Journal of Human-Computer Studies* 12 (2013).
[106] A. Kerckhoffs. *La cryptographie militaire, ou, Des chiffres usités en temps de guerre: avec un nouveau procédé de déchiffrement applicable aux systèmes à double clef*. Librairie militaire de L. Baudoin, 1883.
[107] M. Kesarwani, A. Kaul, S. Braghin, N. Holohan, and S. Antonatos. "Secure k-Anonymization over Encrypted Databases". In: *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*. 2021.
[108] M. Kim and B. R. Choi. "The Impact of Privacy Control on Users' Intention to Use Smart Home Internet of Things (IoT) Services". In: *Asia Marketing Journal* 1 (2022).
[109] K. Kollnig, A. Shuba, R. Binns, M. Van Kleek, and N. Shadbolt. "Are iPhones Really Better for Privacy? A Comparative Study of iOS and Android Apps". In: *Proceedings on Privacy Enhancing Technologies* 2 (2022).
[110] P. Koutroumpis, A. Leiponen, and L. D. Thomas. "Markets for data". In: *Industrial and Corporate Change* 3 (2020).
[111] V. Koutsos, D. Papadopoulos, D. Chatzopoulos, S. Tarkoma, and P. Hui. "Agora: A privacy-aware data marketplace". In: *IEEE Transactions on Dependable and Secure Computing* 6 (2021).
[112] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand. "Online social networks: Why we disclose". In: *Journal of Information Technology* 2 (2010).
[113] L. Kraus, M. Ukrop, V. Matyas, and T. Fiebig. "Evolution of SSL/TLS indicators and warnings in web browsers". In: *Security Protocols XXVII: 27th International Workshop, Cambridge, UK, April 10–12, 2019, Revised Selected Papers 27*. 2020.
[114] K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. von Zezschwitz. ""If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS". In: *2019 IEEE Symposium on Security and Privacy (SP)*. 2019.
[115] Krosnick, Jon A and Alwin, Duane F. "An evaluation of a cognitive theory of response-order effects in survey measurement". In: *Public opinion quarterly* 2 (1987).
[116] P. Kumaraguru and L. F. Cranor. "Privacy indexes: A survey of Westin's studies. Carnegie Mellon University". 2005.
[117] H. Lakkaraju and O. Bastani. ""How do I fool you?" Manipulating User Trust via Misleading Black Box Explanations". In: *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*. 2020.
[118] R. Lambert and M. Frenz. "The economic impact for manufacturing sites operating to BRCGS certification". In: (2021).
[119] A. Lapets, F. Jansen, K. D. Albab, R. Issa, L. Qin, M. Varia, and A. Bestavros. "Accessible Privacy-Preserving Web-Based Data Analysis for Assessing and Addressing Economic Inequalities". In: *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. 2018.
[120] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith. "Federated Learning: Challenges, Methods, and Future Directions". In: *IEEE Signal Processing Magazine* 3 (2020).
[121] K. Liang, J. K. Liu, R. Lu, and D. S. Wong. "Privacy concerns for photo sharing in online social networks". In: *IEEE Internet Computing* 2 (2014).
[122] R. Likert. "A technique for the measurement of attitudes." In: *Archives of psychology* (1932).
[123] A. Linden, J. Fenn, et al. "Understanding Gartner's hype cycles". In: *Strategic Analysis Report R-20-1971. Gartner, Inc* (2003).
[124] C. Liu, J. T. Marchewka, J. Lu, and C.-S. Yu. "Beyond concern—A privacy-trust-behavioral intention model of electronic commerce". In: *Information & Management* 2 (2005).
[125] P. S. M. LLC. *Signal Terms & Privacy Policy*. https://signal.org/legal/ last accessed Aug. 2024. 2024.
[126] W. LLC. *WhatsApp Privacy Policy*. https://www.whatsapp.com/legal/privacy-policy last accessed Aug. 2024. 2024.
[127] L. Longhi and M. Nanni. "Car telematics big data analytics for insurance and innovative mobility services". In: *Journal of Ambient Intelligence and Humanized Computing* 10 (2020).
[128] Y. Maleh, M. Shojafar, M. Alazab, and I. Romdhani. "Blockchain for cybersecurity and privacy: architectures, challenges, and applications". In: (2020).
[129] N. K. Malhotra, S. S. Kim, and J. Agarwal. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model". In: *Information Systems Research* 4 (2004).
[130] F. Mangiò, D. Andreini, and G. Pedeliento. "Hands off my data: Users' security concerns and intention to adopt privacy enhancing technologies". In: *Italian Journal of Marketing* 4 (2020).

[131] N. Manohar. "FHE: IDEAs (Interesting Directions and Emerging Applications)". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. 2024.

[132] E. Markos, G. R. Milne, and J. W. Peltier. "Information sensitivity and willingness to provide continua: A comparative privacy study of the United States and Brazil". In: *Journal of Public Policy & Marketing* 1 (2017).

[133] C. McClain, M. Faverio, M. Anderson, and E. Park. "How Americans view data privacy". In: *Pew Research Center* (2023).

[134] A. M. McDonald and L. F. Cranor. "The cost of reading privacy policies". In: *Isjlp* (2008).

[135] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas. "y". In: *Communication-Efficient Learning of Deep Networks from Decentralized Data*. 2017.

[136] *Medical Software and Medical Apps: Qualification, Classification and Approval as a Medical Device*. https://www.vde.com/topics-en/health/consulting/medical-software-and-medical-apps. (Visited on 11/13/2024).

[137] K. Mišura and M. Žagar. "Data marketplace for Internet of Things". In: *2016 International Conference on Smart Systems and Technologies (SST)*. 2016.

[138] M. Naehrig, K. Lauter, and V. Vaikuntanathan. "Can homomorphic encryption be practical?" In: *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*. 2011.

[139] D. Naous, V. Kulkarni, C. Legner, and B. Garbinato. *Information Disclosure in Location-based Services: An Extended Privacy Calculus Model*. ICIS, 2019.

[140] Office of the Attorney General. *California Consumer Privacy Act*. 2018. URL: https://oag.ca.gov/privacy/ccpa.

[141] D. M. Oppenheimer, T. Meyvis, and N. Davidenko. "Instructional manipulation checks: Detecting satisficing to increase statistical power". In: *Journal of Experimental Social Psychology* 4 (2009).

[142] K. R. Özyilmaz, M. Doğan, and A. Yurdakul. "IDMoB: IoT data marketplace on blockchain". In: *2018 crypto valley conference on blockchain technology (CVCBT)*. 2018.

[143] D. Pal, S. Funilkul, and X. Zhang. "Should I Disclose My Personal Data? Perspectives From Internet of Things Services". In: *IEEE Access* (2021).

[144] F. Pasquale. *The black box society: The secret algorithms that control money and information*. Harvard University Press, 2015.

[145] P. A. Pavlou. "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model". In: *International Journal of Electronic Commerce* 3 (2003).

[146] E. Peer, L. Brandimarte, S. Samat, and A. Acquisti. "Beyond the Turk: Alternative platforms for crowdsourcing behavioral research". In: *Journal of Experimental Social Psychology* (2017).

[147] A. Petrosyan. *UK: personal data gathering awareness change among users 2023*. https://www.statista.com/statistics/1384379/uk-personal-data-collection-awareness-change/ last accessed Aug. 2024. 2023.

[148] M. Pettai and P. Laud. "Combining Differential Privacy and Secure Multiparty Computation". In: *Proceedings of the 31st Annual Computer Security Applications Conference*. 2015.

[149] C. Phonthanukitithaworn and C. Sellitto. "A Willingness to Disclose Personal Information for Monetary Reward: A Study of Fitness Tracker Users in Thailand". In: *SAGE Open* 2 (2022).

[150] S. E. V. S. Pillai and K. Polimetla. "Enhancing Network Privacy through Secure Multi-Party Computation in Cloud Environments". In: *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*. 2024. (Visited on 03/11/2025).

[151] S. Preibusch. "Experiments and formal methods for privacy research". In: *Privacy and Usability Methods Pow-wow (PUMP)* (2010).

[152] O. of the Privacy Commissioner of Canada. *Privacy Enhancing Technologies – A Review of Tools and Techniques*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/. 2017. (Visited on 11/11/2024).

[153] Prolific. "The participants for this paper were recruited using Prolific". In: (2014). year accessed: 2024.

[154] Prolific. *Representative samples*. 2022. URL: https://researcher-help.prolific.co/hc/en-gb/articles/360019236753-Representative-samples.

[155] A. Rai, S. Natarajan, and T. Mehta. "Unpacking Social and Economic Gains from Encryption". In: (2021).

[156] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari. "Towards a decentralized data marketplace for smart cities". In: *2018 IEEE International Smart Cities Conference (ISC2)*. 2018.

[157] *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*. https://www.enisa.europa.eu/publications/pets. Report/Study. (Visited on 11/11/2024).

[158] E. M. Redmiles, Y. Acar, S. Fahl, and M. L. Mazurek. "A summary of survey methodology best practices for security and privacy researchers". In: (2017).

[159] P. Research. *Privacy-enhancing Computation Market Size, Share, and Trends 2024 to 2033*. https://www.precedenceresearch.com/privacy-enhancing-computation-market last accessed Aug. 2024. 2024.

[160] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy. "The mechanics of trust: A framework for research and design". In: *International journal of human-computer studies* 3 (2005).

[161] C. E. Schairer, C. Cheung, C. Kseniya Rubanovich, M. Cho, L. F. Cranor, and C. S. Bloss. "Disposition toward privacy and information disclosure in the context of emerging health technologies". In: *Journal of the American Medical Informatics Association* 7 (2019).

[162] E.-M. Schomakers, C. Lidynia, and M. Ziefle. "All of me? Users' preferences for privacy-preserving data markets and the importance of anonymity". In: *Electronic Markets* 3 (2020).

[163] F. Schomm, F. Stahl, and G. Vossen. "Marketplaces for data: An initial survey". In: *ACM SIGMOD Record* 1 (2013).

[164] J. S. Seberger and S. Patil. "Post-COVID Public Health Surveillance and Privacy Expectations in the United States: Scenario-Based Interview Study". In: *JMIR mHealth and uHealth* 10 (2021). (Visited on 03/11/2025).

[165] M. Silva. *DMA, One Year On: Taking Stock of the EU's Attempts to Rein In Big Tech*. https://botpopuli.net/dma-one-year-on-taking-stock-of-the-eus-attempts-to-rein-in-big-tech/. 2024. (Visited on 11/11/2024).

[166] H. J. Smith, T. Dinev, and H. Xu. "Information privacy research: An interdisciplinary review". In: *MIS Quarterly* (2011).

[167] H. J. Smith, S. J. Milberg, and S. J. Burke. "Information privacy: Measuring individuals' concerns about organizational practices". In: *MIS Quarterly* (1996).

[168] M. Soleymanian, C. B. Weinberg, and T. Zhu. "Sensor data and behavioral tracking: Does usage-based auto insurance benefit drivers?" In: *Marketing Science* 1 (2019).

[169] M. Spiekermann. "Data marketplaces: Trends and monetisation of data goods". In: *Intereconomics* 4 (2019).

[170] S. Spiekermann. *Perceived Control: Scales for Privacy in Ubiquitous Computing (SSRN Scholarly Paper ID 761109)*. Social Science Research Network, 2005.

[171] F. Stahl, F. Schomm, G. Vossen, and L. Vomfell. "A classification framework for data marketplaces". In: *Vietnam Journal of Computer Science* 3 (2016).

[172] F. Stahl, F. Schomm, and G. Vossen. *The data marketplace survey revisited*. Tech. rep. ERCIS Working Paper, 2014.

[173] Statista. *Number of cars owned by households in Great Britain from 2015 to 2021*. https://www.statista.com/statistics/304290/car-ownership-in-the-uk last accessed Aug. 2024. 2023.

[174] *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs) - Publications Office of the EU*. https://op.europa.eu/en/publication-detail/-/publication/a2b75ceb-ada3-4e53-866f-7193f7270a85. (Visited on 11/13/2024).

[175] K. Thompson. "Reflections on trusting trust". In: *Commun. ACM* 8 (1984).

[176] D. for Transport. *Improving road vehicle standards enforcement*. 2022. URL: https://www.gov.uk/government/consultations/improving-new-vehicle-safety-and-environmental-compliance-plus-passenger-vehicle-digital-radio-requirement/improving-road-vehicle-standards-enforcement.

[177] M. Travizano, C. Sarraute, G. Ajzenman, and M. Minnoni. "Wibson: A decentralized data marketplace". In: *arXiv preprint arXiv:1812.09966* (2018).
[178] M. Travizano, C. Sarraute, M. Dolata, A. M. French, and H. Treiblmaier. "Wibson: A case study of a decentralized, privacy-preserving data marketplace". In: *Blockchain and distributed ledger technology use cases: Applications and lessons learned* (2020).
[179] P. Verschuren and H. Doorewaard. *Designing a research project*. Vol. 2. Eleven International Publishing, 2010.
[180] A. E. Waldman. "Cognitive biases, dark patterns, and the 'privacy paradox'". In: *Current Opinion in Psychology* (2020). Privacy and Disclosure, Online and in Social Interactions.
[181] N. Wessels, J. Gerlach, and A. Wagner. *To Sell or not to Sell – Antecedents of Individuals' Willingness-to-Sell Personal Information on Data-Selling Platforms*. ICIS 2019 Proceedings. 2019. URL: https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/34.
[182] WhatsApp. *end-to-end encryption*. https://blog.whatsapp.com/end-to-end-encryption. accessed: Aug. 2024. 2016.
[183] I. WhatsApp. *Private Messaging showcase at Gateway of India in Mumbai — WhatsApp*. 2023. URL: https://www.youtube.com/watch?v=vprXR_OF2UI.
[184] A. Whitten and J. D. Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." In: *USENIX security symposium*. 1999.
[185] A. Woodruff, V. Pihur, S. Consolvo, L. Brandimarte, and A. Acquisti. "Would a Privacy Fundamentalist Sell Their DNA for $1000 If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences". In: *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. 2014.
[186] H. Xu, T. Dinev, J. Smith, and P. Hart. "Information privacy concerns: Linking individual perceptions with institutional privacy assurances". In: *Journal of the Association for Information Systems* 12 (2011).
[187] Y. Yu, Y. Li, J. Tian, and J. Liu. "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things". In: *IEEE Wireless Communications* 6 (2018).
[188] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, and Y. Tan. "Secure Multi-Party Computation: Theory, practice and applications". In: *Information Sciences* (2019).
[189] L. Zhao, Y. Lu, and S. Gupta. "Disclosure Intention of Location-Related Information in Location-Based Social Network Services". In: *International Journal of Electronic Commerce* 4 (2012).
[190] H. Zhong, Y. Sang, Y. Zhang, and Z. Xi. "Secure Multi-Party Computation on Blockchain: An Overview". In: *Parallel Architectures, Algorithms and Programming*. 2020.
[191] I. Zhou, F. Tofigh, M. Piccardi, M. Abolhasan, D. Franklin, and J. Lipman. "Secure Multi-Party Computation for Machine Learning: A Survey". In: *IEEE Access* (2024). (Visited on 03/11/2025).
[192] T. Zhou. "The impact of privacy concern on user adoption of location-based services". In: *Industrial Management & Data Systems* 2 (2011).
[193] A. Zigomitros, F. Casino, A. Solanas, and C. Patsakis. "A Survey on Privacy Properties for Data Publishing of Relational Data". In: *IEEE Access* (2020).
[194] S. Zuboff. "The Age of Surveillance Capitalism". In: *Social Theory Re-Wired*. 3rd ed. 2023.

Appendix A: Survey Items

Here, we list our survey questions. Note that the order of questions was randomized during the study to prevent order effects, see Section 3.1.3. References were *not* shown to participants. The full treatment conditions, consent information, and experimental flow are available online at: https://github.com/ichdasich/mpc_supplemental_material.

The results of our survey are available at: https://figshare.com/s/bedb755aea0f997450c9.

A.1. Main Survey Questions

Perceived control (Xu et al. [186])

CTRL_1 I believe I have control over who can access the sensitive data I provided to this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

CTRL_2 I think I have control over what kind of sensitive data is shared by this data marketplace to other companies.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

CTRL_3 I believe I have control over how other companies use the sensitive data I provided to this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

---

Perceived risk (Xu et al. [186])

RISK_1 I find it risky to provide my sensitive data via this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

RISK_2 There would be too much uncertainty associated with providing my sensitive data to this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

---

Privacy concerns(Dinev and Hart [50])

PRIV_1 I am concerned that other parties could find sensitive information about me on this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

PRIV_2 I am concerned about providing my sensitive data to this data marketplace because of what other parties might do with it.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

---

Trust in data marketplaces operator (Kehr et al. [104])

TRSD_1 I expect this data marketplace would be trustworthy regarding my sensitive data.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

TRSD_2 This data marketplace would tell the truth and fulfil promises related to my sensitive data.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

TRSD_3 I expect this data marketplace would be honest with me regarding the sensitive data I would provide.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

---

Trust in data buyers (Kehr et al. [104])

TRSB_1 I expect that data buyers would be trustworthy in handling the data they got from this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

TRSB_2 I expect that data buyers would tell the truth and fulfil promises in handling the data they got from this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

TRSB_3 I expect that data buyers would be honest when handling the data they got from this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

Willingness to share data via a DMP (Pavlou [145])

WTSD_1 Given the chance, I would share my data via this data marketplace.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

WTSD_2 Given the chance, I predict that I should share my data via this data marketplace in the future.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

WTSD_3 It is likely that I will share my data via this data marketplace in the near future.
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

A.2. Westin's Privacy Segmentation Index

Note: We use Westin's privacy index [116] to collect participant's disposition towards privacy as additional demographic information to be able to assess whether their privacy disposition influences treatment effects.

(1) Consumers have lost all control over how personal information is collected and used by companies.
Scale: Strongly Agree - Agree - Disagree - Strongly Disagree

(2) Most businesses handle the personal information they collect about consumers in a proper and confidential way.
Scale: Strongly Agree - Agree - Disagree - Strongly Disagree

(3) Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.
Scale: Strongly Agree - Agree - Disagree - Strongly Disagree

A.3. Instructional manipulation check

Note: To ensure that participants are attentive, we included an instructional manipulation check [141]. Below you can find the two checks we included in the survey:

(1) There is nothing wrong with companies that collect personal information without consent. Regardless of what you think, please select "somewhat agree."
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

(2) Do you agree that data is the new oil? Regardless of what you think, please select "strongly disagree."
Scale: Strongly Agree - Neutral - Agree - Disagree - Strongly Disagree

Appendix B: Meta-Review

B.1. Summary

This paper employs a large scale quantitative study to evaluate the impact on attitudes and intended actions of participants given a description of a privacy-enhancing technology (PET). The paper found that, when comparing their real treatment group (multiparty computation description) and a group of participants that received the fictional treatment, that there was no significant difference between the effects of the real PET and that of a fictional PET. The paper identifies this as a potential gap for PETs that could give users a false sense of privacy.

B.2. Scientific Contributions

Provides a Valuable Step Forward in an Established Field

B.2. Reasons for Acceptance

The work demonstrates a nuance between explaining PETs and the impact of explanations on perceptions and behaviors. This nuance has implications for future studies on communicating PETs as well as on the interpretation of past studies.

B.3. Noteworthy Concerns

1) The authors only compare the description of a real PET with its real name to a description of a fictional PET with a fictional name and do not compare other isolated factors, such as by comparing the same description with two different names assigned to it.
2) The paper is missing explanations critical for its interpretation such as what their fictional DCP description is, why TPP was chosen for the control group.
3) The contributions and motivation for this work are not presented with sufficient contextualization in regards to its limitations on relating to PETs other than MPC.

B.4. Response to the Meta-Review

1) The notable concerns state that our study does not evaluate a sufficiently large set of possible variables. We argue that our results highlight the general risk of studies misinterpreting the factors influencing users' perception when presenting PETs to lay users. We agree that isolating individual factors to gain deeper insight into this mechanism is interesting future work. However, for the study at hand, we limited the scope to the problem in general.
2) Our reasons for choosing TPP and MPC are explained in Sec.2.3 and Sec.2.4. The supplementary material contains the descriptions provided to participants.
3) The result of our study shows that intruducing PETs to users and measuring their perception should not rely on merely naming and explaining the technologies used. The risk of misinterpretation of its influence the risk of a false sence of privacy must be considered by the privacy advocating community, the research community as well as policy makers.