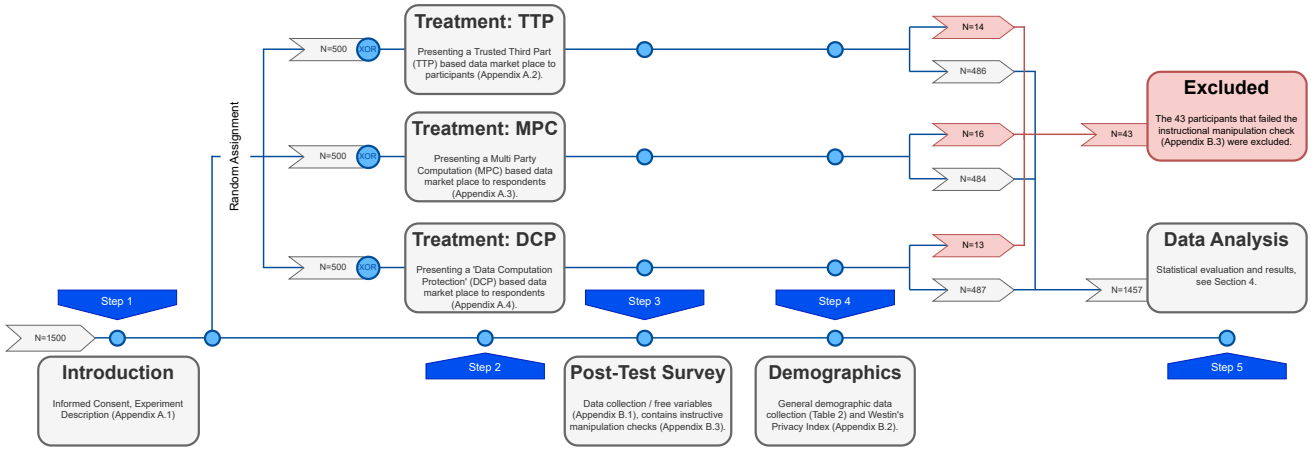
Appendix

1. Experimental Setup

In this appendix, we list our full experimental setup, and utilized instrument, i.e., questionnaire and treatments presented to participants.
The questionnaire contains two main parts:

- An introductionary part that is the same for all three treatments, and,
- The individual treatment conditions.



2. Questionnaire Introduction

Introduction

Dear participants,

Thank you for making time to take part in this survey. Your contribution is greatly appreciated!

You are being invited to participate in a research study titled **"Does multi-party computation (MPC) enhance control in data sharing through data marketplaces? An experimental study"** This study is conducted by <blinded for review>. The Human Research Ethics Committee of <blinded for review> approved this study.
The purpose of this research study is **to investigate the impact of <a Trusted Third Party (TTP)—a privacy-enhancing technology called Multi-Party Computation (MPC)—a privacy-enhancing technology called Data-Computation-Protection> on individuals' control over data and willingness to share data in data marketplaces.** This study will take you **approximately 20 minutes** to complete. Your answer will remain anonymous, cannot be traced back to you, and will only be used for research purposes. **Your participation in this study is entirely voluntary and you can withdraw at any time.**

We believe there are no known risks associated with this research study; however, as with any online-related activity, the risk of a breach is always possible. To the best of our ability, your answers in this study will remain confidential. We will minimize any risks by **only storing data at remote, protected storage at <blinded for review>, only accessible by project members, as well as abstaining from both distributing data to others or retrieving it on personal devices.**

An anonymized, non-reducible version of this dataset will be publicly available through <blinded for review>. Before publication, we will drop any personal data.

For any further inquiries, please refer to: <blinded for review>

Please check the first box to give permission to process your data for this research:

☐ I acknowledge that I have read and understood this introduction, and ***I hereby give consent*** that my survey data will be processed for this research.

☐ ***I do not consent***, and I do not wish to participate in this study.

Case description: sharing driving data from the connected cars via data marketplaces

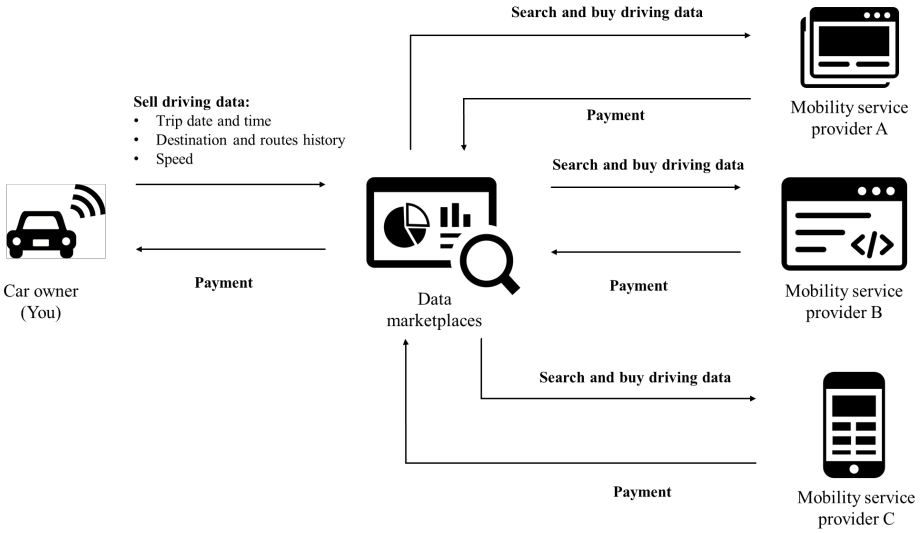
Imagine that you own a car that you regularly use to travel to work or other places. The car is connected to the Internet. Then, suppose that several mobility start-up companies want to offer various applications to improve driving behaviour and ultimately become better and safer drivers. **You do not know those companies, and you have not used their applications before.**

To achieve their goals, those companies would like to buy the data from your car. You can sell your car data to them via a **data marketplace**: a website where you can sell your car data to those mobility start-up companies. Please assume that it takes you very little effort to share your data on the data marketplace; all you need to do is register and click "upload."

To offer their services, those companies would like to buy the following data from you on the data marketplace:

- **Trip date and time:** when are you driving to a particular destination
- **Destination and routes history:** GPS information on where you are driving
- **Speed:** how fast are you driving

A simplified illustration is provided in the figure below (you can zoom the image if you are using a smartphone/tablet).



In the following questions, we will present a drawing of the data marketplace. Then, we will ask your perception on whether you would offer your data to those mobility start-up companies through the data marketplace based on the design presented. You may assume that when you make your data available, those companies would be able to **describe your driving behaviour** and **suggest better and safer driving advice to you (if you use their apps in the future).** Furthermore, by selling your data, **you will get financial compensation.**

3. Treatment 1: Trusted Third Party (TTP)

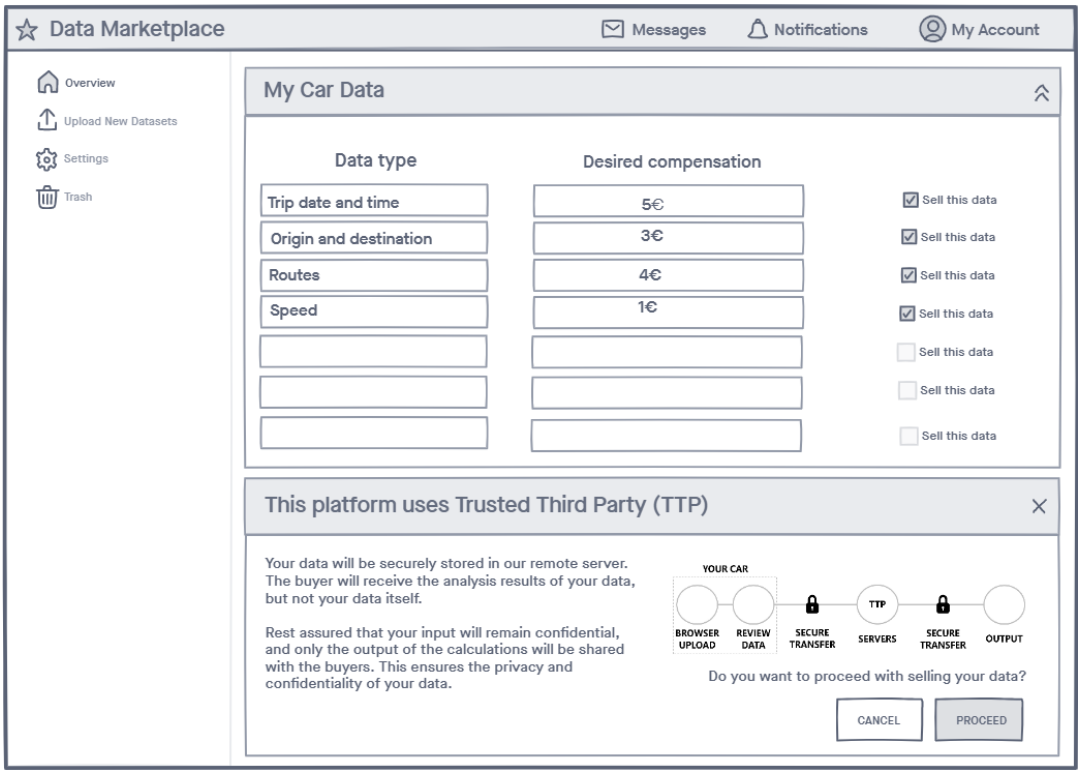
A technology to share your confidential information in a data marketplace is a **Trusted Third Party (TTP)**. The TTP stores, processes, and analyses your data on a central system.

Example:

Four colleagues go out to dinner, and they have agreed that the person with the highest salary should pay the bill. However, for privacy reasons, they do not want to disclose their salary to each other. So, they decided to ask the waiter to be the Trusted Third Party (TTP). They individually tell their salary to the waiter. Then, the waiter gives the bill to the colleague who has the highest salary, without the colleagues knowing what their salary is from each other. As a TTP, the waiter will know all of their salaries and compare them before giving the bill.
In short: TTP has access to the data of all data providers. But it will tell data buyers only the answers to the questions that data buyers have.

In this design, you can share your driving data via a **TTP-based data marketplace.** The data marketplace is managed by a platform operator that is also responsible for processing all data.

After you agree to sell your driving data, **it will be stored in the remote server of data marketplaces.** Then, when the mobility service providers buy your driving data, they have to tell the platform operator which analyses they want to perform. After that, the platform operator performs the analysis and sends the results to those companies (as data buyers). This way, those companies only see the analysis results based on your driving data and not your driving data itself. **Only the platform operator can view your data because it performs the analyses.**
A screenshot preview of the TTP-based data marketplace is presented below (you can zoom the image if you are using a smartphone/tablet).
To convince you that the analysis of your data is confidential, a disclaimer has been added that explains how TTP works.



☐ Please tick here if you have **read the description** and **understand the scenario** of sharing driving data through TTP-based data marketplaces

You have read the scenario of sharing driving data through **TTP-based data marketplaces**. The code for this scenario is **A1**.
Please enter the code here: _____

4. Treatment 2: Multi-Party Computation (MPC)

A technology to share your confidential information in a data marketplace is a **Multi-Party Computation (MPC)**. With MPC, your data is encrypted, meaning that **your data is being changed so that it cannot be read without knowledge of the secret key that has been used to change your data.** Your encrypted data is then shared and can be used to perform meaningful calculations. Think of MPC as a black box that calculates a specific function. Parties discretely share their input with MPC, then the output follows from the function without revealing the input.

Example:

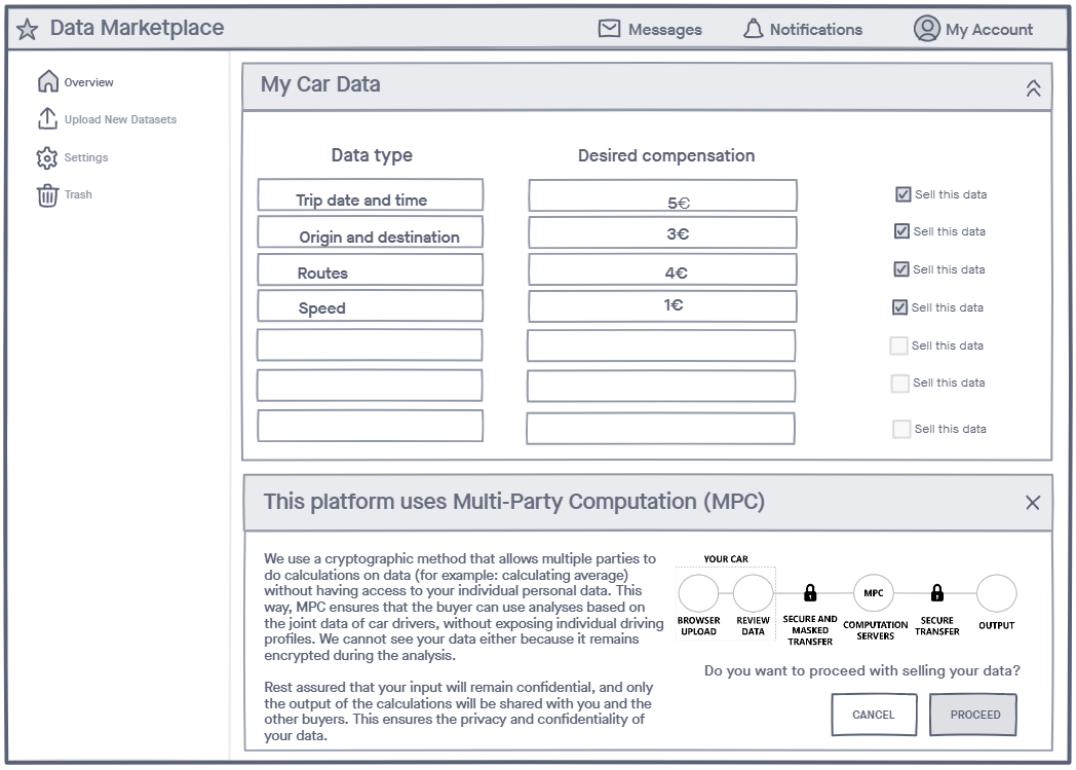
> Four colleagues go out to dinner, and they have agreed that the person with the highest salary should pay the bill. However, for privacy reasons, they do not want to disclose their salary. That's why they decide to use MPC. They individually enter their salary into the MPC application. This application indicates which colleague has the highest salary, without the colleagues knowing what their salary is from each other. The application itself does not see this data either because the salaries are first encrypted before the analysis is performed.
>
> **In short: MPC is a protocol that creates knowledge for all parties via a function without releasing the underlying data.**

In this design, you can share your driving data via an **MPC-based data marketplace.** The data marketplace is managed by a platform operator, but **they do not have access to your data.** They only connect buyers (in this case, mobility service providers) and sellers (in this case, you).

After you agree to sell your driving data, it will be encrypted and stored in your car. Then, when mobility service providers buy your driving data, they have to tell the platform operator which analyses they want to perform. **You can choose to exclude your driving data if you wish.** Then, using MPC, the platform operator performs the analysis and sends the results to those companies (as data buyers). This way, those companies only see the analysis results based on your driving data and not driving car data itself. **The platform operator does not have access to your driving data because it is encrypted and stored in your car.**

A screenshot preview of the MPC-based data marketplace is presented below (you can zoom the image if you are using a smartphone/tablet).

To convince you that the analysis of your data is confidential, a disclaimer has been added that explains how MPC works.



☐ Please tick here if you have **read the description** and **understand the scenario** of sharing driving data through MPC-based data marketplaces

You have read the scenario of sharing driving data through **MPC-based data marketplaces**. The code for this scenario is **B2**.

Please enter the code here: _____

5. Treatment 3: Data-Computation-Protection (DCP/fictional technology)

A technology to share your confidential information in a data marketplace is a **Data-Computation-Protection (DCP)**. With DCP, your data is encrypted, meaning that **your data is being changed so that it cannot be read without knowledge of the secret key that has been used to change your data.** Your encrypted data is then shared and can be used to perform meaningful calculations. Think of DCP as a black box that calculates a specific function. Parties discretely share their input with DCP, and the output follows from the function without revealing the input.

Example:

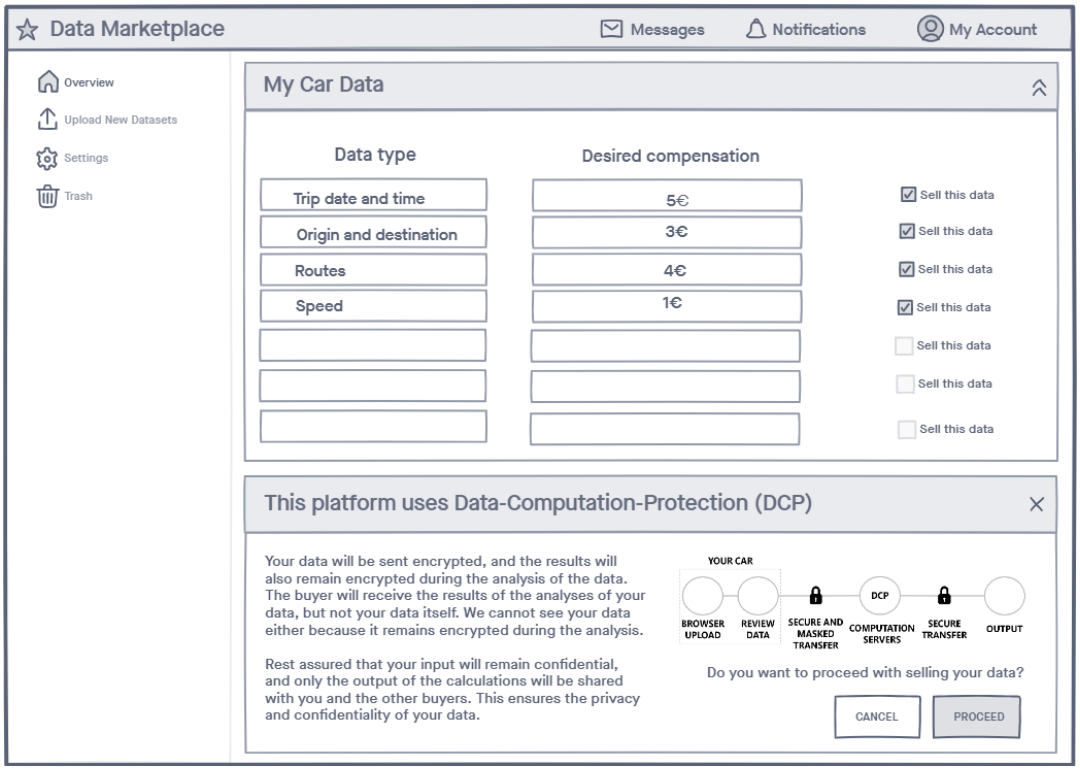
> Four colleagues go out to dinner, and they have agreed that the person with the highest salary should pay the bill. However, for privacy reasons, they do not want to disclose their salary. That's why they decide to use DCP. They individually enter their salary into the DCP application. This application indicates which colleague has the highest salary, without the colleagues knowing what their salary is from each other. The application itself does not see this data either because the salaries are first encrypted before the analysis is performed.
>
> **In short: DCP is a protocol that creates knowledge for all parties via a function without releasing the underlying data.**

In this design, you can share your driving data via an **DCP-based data marketplace.** The data marketplace is managed by a platform operator, but **they do not have access to your data.** They only connect buyers (in this case, mobility service providers) and sellers (in this case, you).

After you agree to sell your driving data, it will be encrypted and stored in your car. Then, when mobility service providers buy your driving data, they have to tell the platform operator which analyses they want to perform. **You can choose to exclude your driving data if you wish.** Then, using DCP, the platform operator performs the analysis and sends the results to those companies (as data buyers). This way, those companies only see the analysis results based on your driving data and not driving car data itself. **The platform operator does not have access to your driving data because it is encrypted and stored in your car.**

A screenshot preview of the DCP-based data marketplace is presented below (you can zoom the image if you are using a smartphone/tablet).

To convince you that the analysis of your data is confidential, a disclaimer has been added that explains how DCP works.



☐ Please tick here if you have **read the description** and **understand the scenario** of sharing driving data through DCP-based data marketplaces

You have read the scenario of sharing driving data through **DCP-based data marketplaces**. The code for this scenario is **C3**.

Please enter the code here: _____