Lernende Systeme

GERMANY'S PLATFORM FOR ARTIFICIAL INTELLIGENCE

Secure and safe travel with AI

White Paper by
Tobias Hesse, Jörn Müller-Quade et al.
Working Group IT Security, Privacy, Legal and Ethical Framework;
Working Group Mobility and Intelligent Transport Systems

Executive Summary

Future mobility will be digitally networked and provide individual, customised mobility services. Artificial intelligence (AI) can make an important contribution here, on the one hand by relieving infrastructures, the environment and resources in a sustainable and resource-efficient way, and on the other hand by guiding travellers to their destination in a time-saving and flexible manner. This can be done conveniently with the intelligent travel assistant as an app on the smartphone or laptop. It bundles and analyses offers in the background and suggests individual travel routes that cover environmentally compatible and sustainable mobility.

Experts from the Working Group IT Security, Privacy, Legal and Ethical Framework and the Working Group Mobility and Intelligent Transport Systems of the Plattform Lernende Systeme show how the intelligent travel assistant can be used in the future and become a constant travel companion in everyday life. The paper focusses on how IT security and safety, in particular data security and data management, can be guaranteed for AI-based travel assistants. On the one hand, the success of such travel assistants depends on how the handling of the collected data along the mobility service chain is regulated and guaranteed with regard to IT safety and security and data protection, and on the other hand, whether it provides travel suggestions based on personal preferences. This area of conflict between usability, data protection and also IT safety and security must be covered.

How the AI-based travel assistant works

First the authors illustrate how an intelligent travel app can function by using the future environment scenario of a digital travel assistant from "Carla's Journey" (chapter 2), which was developed by the working group Mobility and Intelligent Transport Systems. The scenario illustrates how travellers, in this case Carla, will be able to reach their destination more easily, more quickly, more resource-efficient, and also more safely, more securely and more flexibly with the help of AI-based means of transport, infrastructures and applications (e.g. assistance systems). All this supported by an intelligent travel assistant that is constantly learning through AI methods.

Future environment scenario: The goal of the intelligent travel assistant is to determine the best possible journey regarding individual preferences, options and contextual factors. Finally, the travel assistant can be used at any time **before**, **during** and **after** a **journey**: for planning and booking, but also for changing the journey in the event of unforeseen restrictions in the traffic flow. And as a further advantage: it is also constantly evolving through feedback from users (chapter 2.3).

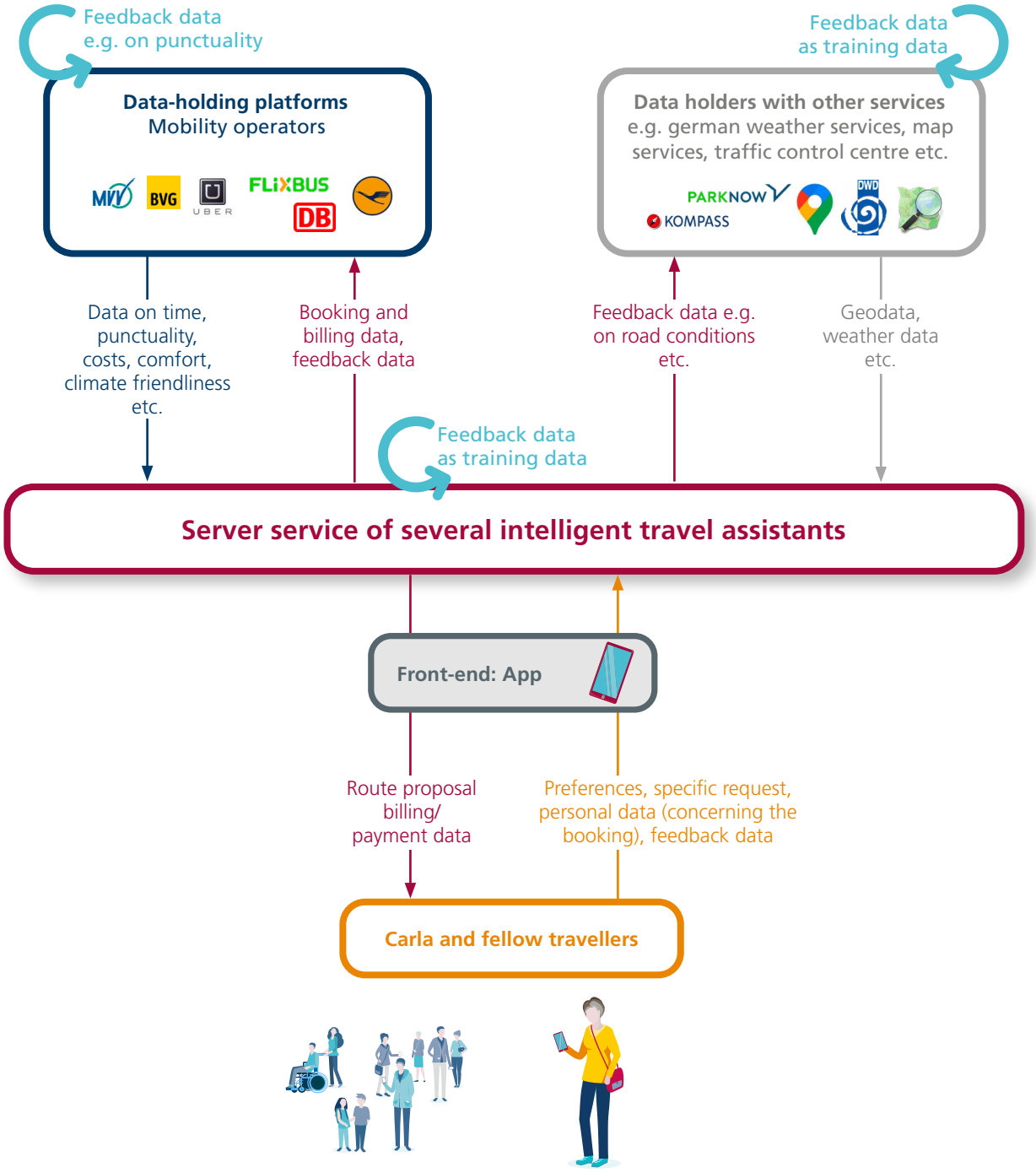
Technical basis – mobility platform: The technical basis of the intelligent travel assistant is a digital mobility platform that is part of a system architecture that voluntarily networks several data holders, such as mobility operators or companies for transport or infrastructure (chapter 2.3.2). The mobility platform itself does not hold any data centrally. This builds a basis for the participation of all actors – from mobility operators to other data holders to users – in a creative trust ecosystem. A key factor for the mobility platform is the trustworthy identification of the mobility providers; flanked by corresponding guidelines as well as legal compliance regarding access rights, data economy, audits or independent certifications.

The operator model of the respective mobility platform to which the intelligent travel assistant is connected can be designed in different ways: A superordinate central platform or a federated decentralised platform are possible (chapter 4.3).

Trade-off between usability and data protection

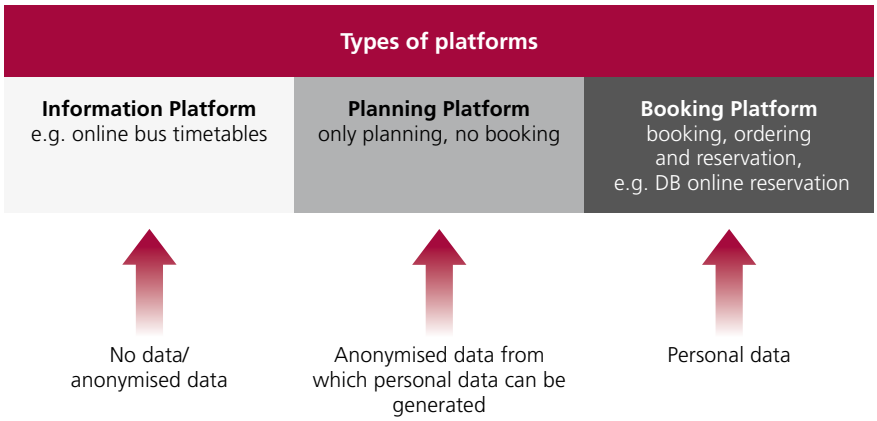
In addition to possible options for the design of digital travel assistants, the authors outline the trade-off between usability and data protection by using the scenario to show where and when which types of data are generated by which actors within the entire mobility ecosystem (see Figure 1).

Figure 1: Overview on the whole data path including all actors in the mobility data ecosystem



In such a complex data ecosystem the functionality of intelligent travel assistants themselves and the large amount of generated data – sometimes also sensitive customer data – place high demands on IT safety and security and data protection. Therefore, the type of data and also the required level of IT security depends on the type of platform on which the intelligent travel assistant is based (see Figure 2).

Figure 2: Relationship between the type of platform and the type of data



The authors' aim is therefore to identify possible risks in the use of an AI-based travel assistant and to suggest possible solutions (chapter 4). In principle, the "safety and security by design" approach should be applied here, especially in the development phase in order to integrate security measures, especially for the protection of personal data.

Possible design options

The authors propose concrete design options which they address to different actors, in order to realise intelligent travel assistants as safely and securely as possible and in compliance with data protection:

Users of AI travel assistants should...

- take precautions to avoid potential risks regarding IT safety and security and also data protection. This requires a reflective handling of one's own data when using intelligent travel assistants ("smart trust").
- be careful when choosing the provider of smart travel assistants.
- keep data details to a minimum. The rule is: "Only as much as necessary".
- be open to accept existing information offers on how AI systems work.

Platform operators should...

- as responsible for the quality of the offer, ensure that an adequate level of data protection and IT safety and security is maintained. This also includes the participating mobility providers.
- make a conscious and targeted selection of participating mobility providers.
- continuously check compliance with the specified requirements.
- let check their own offers, including the algorithms, by independent certification and audits.
- strive for a high level of IT safety and security on their own responsibility.

Mobility providers should...

- always enable checks of their own system to demonstrate seriousness to the platform operator.
- strive for a high level of IT safety and security on their own responsibility.

Policy makers should...

- promote plurality of providers of intelligent travel assistants to ensure a high level of quality.
- promote education in the use of AI systems and functionalities and promote it through public projects that serve science communication, so that the users can handle their data responsibly, make reflective decisions and be more educated about how AI systems work and how to handle them.

Research and development should...

- develop solutions to solve the conflict between data economy and usability with regard to IT safety and security.
- promote explainable AI (XAI for short).

In addition, socially relevant questions that need to be specifically discussed and answered in a broad social and political discourse need to be clarified in terms of participation, fairness, responsibilities etc.

Intelligent, personal travel assistants will soon be feasible and operational with the methods of AI and machine learning. With this paper the experts would like to provide orientation on how intelligent travel assistants can be realised as safely and securely as possible and in compliance with data protection. If all these aspects are taken into account and implemented, this can create trustworthiness in such AI-based systems, which is a prerequisite for the use of travel assistants.

Imprint
Editor: Lernende Systeme – Germany's Platform for Artificial Intelligence | Managing Office | c/o acatech | Karolinenplatz 4 | D-80333 München | kontakt@plattform-lernende-systeme.de | www.plattform-lernende-systeme.de | Follow us on Twitter: @LernendeSysteme | Status: June 2021 | Photo credit: Tempura/iStock/Title

This executive summary is based on the white paper *Secure and safe travel with AI – Data management and data security with AI-based travel assistants,* Munich, 2021. The authors are members of the working group IT Security, Privacy, Legal and Ethical Framework as well as Mobility and Intelligent Transport Systems of Plattform Lernende Systeme. The original version of this publication is available at: https://www.plattform-lernende-systeme.de/publikationen.html

SPONSORED BY THE

Federal Ministry of Education and Research

acatech
NATIONAL ACADEMY OF SCIENCE AND ENGINEERING