Fraunhofer ISI

Collection and Use of Digital Mobility Data, Challenges in Their Anonymization, and Alternative Strategies

Discussion Paper, September 2025

Bernd Beckert, Frederik M. Metzger

Imprint

Collection and Use of Digital Mobility Data, Challenges in Their Anonymization, and Alternative Strategies

Authors

Bernd Beckert, bernd.beckert@isi.fraunhofer.de;
Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe

Frederik M. Metzger, frederik.metzger@isi.fraunhofer.de;
Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe

Recommended citation

Beckert, Bernd; Metzger, Frederik M. (2025): *Collection and Use of Digital Mobility Data, Challenges in Their Anonymization, and Alternative Strategies*. (Discussion Paper) Fraunhofer ISI, Karlsruhe. https://doi.org/10.24406/publica-5338

DOI

10.24406/publica-5338

Published

September 2025

Contact

Fraunhofer Institute for Systems und Innovation Research ISI

Breslauer Strasse 48, 76139 Karlsruhe, Germany
Bernd Beckert, bernd.beckert@isi.fraunhofer.de

Abstract

Digital mobility data, which consist of geolocation or movement information, pose a dual challenge: they require protection under measures like the General Data Protection Regulation (*GDPR*) due to their personal nature, yet they hold significant value for applications such as traffic planning, smart mobility services, and retail strategies, among others. This overview article explores the conflict between the need for privacy and the potential benefits of utilizing mobility data. It provides a comprehensive overview of data collection from smartphones, mobile networks, and connected vehicles, and outlines anonymization methods: data cropping, data generalization, and data perturbation; as well as pseudonymization. The presentation of mobility data use shows that anonymization measures are often insufficient. Although anonymization is applied, two major challenges remain: first, due to their dense collection points, mobility data are highly vulnerable when being intersected with secondary datasets. Second, unique time and spatial patterns make mobility data easily backtraceable to individuals. We conclude by proposing additional and alternative strategies, such as cryptographic pseudonymization, data sharing platforms, and data trustees, as technical and institutional solutions for privacy-preserving mobility data approaches.

Keywords: Mobility; transportation; digital data; data anonymization; homomorphic encryption; privacy-enhancing technologies.

Contents

1 Introduction

Digital mobility data are computational geolocation or movement information that can be recorded by different sources, like smartphones, smartphone apps, or connected vehicles, and stored by manufacturers or operators. Digital movement data are typically recorded on an individual's smartphone. The data traces can reveal personal circumstances. For example, journey tracking can indicate where a person lives and works (Cox 2021). Stores and shopping centers visited can provide clues to certain purchasing habits (Keegan and Eastwood 2023). Regular visits to a dialysis center can indicate certain illnesses, or visits to pregnancy counseling locations can indicate corresponding intentions (Cyphers and Gebhart 2019). Movement data also allow conclusions to be drawn about social or leisure activities (Ramasastry 2015). These examples show that mobility data are special data that are directly linked to the privacy of users. Accordingly, unwanted uses are perceived as invasive or manipulative.

In being personal data, mobility data are legally protected. The European General Data Protection Regulation (*GDPR*) and other data protection regulations prohibit manufacturers and operators from using mobility data without the consent of the users.[1] And even if consent is given, which providers usually obtain through the general terms and conditions, the data use is restricted. According to the *GDPR*, firms are allowed to use mobility data which they have collected themselves for improving their services or for other "legitimate purposes." However, they must provide both a utilization plan and a document which data they use depending on their purpose. It is fundamentally prohibited to make individualized mobility data available to other market players or to resell them. The reason for this is obvious as mobility data can reveal a great deal about an individual.

On the other hand and viewed from a business opportunity or a traffic planning perspective, mobility data are of immense value. This is because digital data traces make it possible, in principle, to optimize routes and means of transport, to better understand people's mobility needs, make traffic safer, adjust urban and transport planning to the respective needs, and also to target advertising to the needs of mobile users, to inform travelers about services along their route, or to advise retail planners where to open new stores (e.g., Francis 2018).

To suffice both using mobility data and ensuring data protection, the rise of anonymization technologies has appeared as a promising avenue in both research and practice. Recital 26, accompanying the *GDPR*, explains that datasets can only be used, shared, and passed on without restrictions if they are fully anonymized. This perspective reflects the legal argumentation, however. From this perspective, anonymization is considered a binary state: datasets are either fully anonymized or personal. Yet, seen from a technical side, anonymized mobility data are aggregated or altered in specific ways so they cannot be associated with a specific person. When bringing together the legal and the technical perspectives, the challenge lies in defining the threshold when a dataset is fully anonymized.

There are different methods of anonymization that can obfuscate the digital data traces to varying degrees. Depending on the type of data and on the anonymization technology used, the utility of the data is limited, but it is still available for various applications. The necessity of anonymization has recently triggered various activities at the technical level. In recent years, a dedicated developer community has emerged around anonymization and privacy-preserving technologies, attempting to anonymize data sets at differing quality levels by employing a panoply of methods. Furthermore, a considerable number of research projects are currently being carried out to develop data

[1] See article 4 of the *GDPR*.

processing methods to optimize the anonymization of data in a broad range of application fields, among others mobility.[2]

As authors of this article, we are ourselves involved in one of these anonymization projects, but in this paper, we want to take a broader look at the question of where mobility data come from and which use cases exist. This paper is based on a web and literature analysis conducted between September 2024 and July 2025 as part of the ANYMOS project (Kneis et al. 2023) funded by the Federal Ministry of Research, Technology, and Space.[3] Although a large part of this report refers to examples from German-speaking countries, the topic of mobility data is an international one. Thus, international sources, such as blog articles, newspaper articles, and research papers are used as a basis to answer our research questions.

The aim of this overview paper is to better understand the ecosystems of mobility data collection and data use and the role of anonymization technologies in this context. Because data anonymization is widely claimed to open up seemingly unlimited use cases, we want to critically uncover what lies behind anonymization technologies by naming and explaining their basic functioning. When starting our work on anonymization technologies, we found that such an overview is currently missing. Our overview thus places the current technology work in the context of actual utilization and factual necessities and provides background information to both practitioners and development projects dealing with anonymization technologies in the mobility sector. The research questions structuring our analysis are:

1) How are mobility data collected?
2) Which are the most important anonymization technologies?
3) How are mobility data used, and what role do anonymization technologies play in the different use scenarios?

The paper proceeds as follows. In the next section, we describe where mobility data are generated and how they are collected. We then look at anonymization technologies and present three basic classes of methods and the further developments that are currently being worked on. This section also presents pseudonymization and cryptographic pseudonymization. The next section deals with the use of mobility data, and in which terms the employment of anonymization techniques can actually be substantiated. In the concluding summary, we present an overview of our findings and discuss alternative ways to use mobility data in a privacy-preserving way. The main argument we find with our analysis is that due to the nature of mobility data and their relatively easy backtraceability to individuals, *de facto* anonymization does not exist. This poses severe problems toward the legal position where only anonymized datasets are exempt from the *GDPR*. The perspective we draw extends from technical solutions to institutional ones. On the technical side, an alternative to the presented anonymization methods consists in pseudonymization through cryptographic methods. On the institutional side, we discuss trust-based solutions, such as data platforms and data trustees.

[2] For instance, the German Federal Ministry of Research, Technology, and Space funds 22 research projects in the framework program on anonymization between 2022 and 2025: www.forschung-it-sicherheit-kommunikationssysteme.de/forschung/it-sicherheit/forschungsnetzwerk-anonymisierung; accessed: 05.07.2024.

[3] https://www.anymos.de; accessed: 09.07.2025.

2 Sources of Mobility Data

This section provides an overview of the different data sources, the devices, and actors in the field of mobility data, while the data usage scenarios are discussed later in the section following the description of anonymization technologies.

2.1 Smartphones

The most important sources for mobility data are smartphones. Smartphones generate mobility data via *GPS* positioning (even when the devices are not in active use) and via recording of acceleration when the device is in motion. Together with the mobile telephone number, the serial number of the smartphone, the advertising ID, and local mobile network information, individual location data are sent periodically to *Apple* or *Google* servers. On average, both *iOS* and *Android* smartphones transmit telemetry data to their "motherships" every 4.5 minutes (Goodin 2021; see also Leith 2021). Whereas smartphone users may prevent the transmission of their device's advertising ID (Becker 2025; Cyphers 2022), the transmission of other location data cannot be switched off. Smartphone providers claim that the continuous transmission of location data is necessary for smartphone services to work at all (Goodin 2021). And in fact, many applications, such as navigation services or real-time traffic information (see section 3) are only made possible by the continuous transmission of location data.

Data protectionists, on the other hand, point out that the increasing use of smartphones also means that personal movements are increasingly being monitored: "We derive benefits from this location-harvesting system (…) But we shouldn't have to accept in return the perpetual and increasingly invasive surveillance of our movements," writes, for example, Shira Ovide in the *Tech Newsletter* of the *New York Times* (Ovide 2021, para. 15).

2.2 Smartphone Apps by External App Providers

The second source of mobility data are external apps that users have installed on their smartphones. External means that they are not included in the operating systems of Apple or Google but are developed by external service providers. External apps which require location data to work properly are, for example, navigation apps like *Waze*, public transport apps like *Moovit*, apps for locating gas or charging stations like *ChargeMap*, weather apps like *AccuWeather*, and more. Here, it depends on the user settings, i.e., the app permissions, which data the app providers are allowed to collect, transmit, and use.

In fact, location data are also transmitted by external apps that are not directly related to mobility. For example, *Facebook*, *Instagram* or even the popular German advice website *gutefrage.net* access the location data of mobile phone users if users have not switched off the function. The list of apps is long that continuously collect mobility data after users have agreed through the terms and conditions of the app or through explicit request of the app provider. In addition to social media apps, there are retail apps, messenger and chat apps, streaming apps, health and fitness apps, apps for financial services, travel apps, etc. that localize the user's device via their functionality, often even when the app is not in active use (Gatzert et al. 2023, p. 12).

When users have given permission to an app (via general terms and conditions or app settings) to track their location, the current GPS coordinates of the device are transmitted as well as the device identifier which is usually the advertising ID (*IDFA* for Apple, *AAID* for Android). Name and phone number of the user are not automatically sent along with the location data in this case. However, if the user has actively provided his or her name, phone number or email address to the app—such

as during registration or when creating a profile—this so-called Personally Identifiable Information (*PII*) is also transmitted.

We are especially interested in smartphone apps provided by mobility service providers: transport companies, rail and bus operators, car sharing platforms, e-bike and e-scooter rental companies, etc. usually have their own digital information and booking apps. Users of these mobility apps need a user account for authentication and for the ticketing processes. For the full functionality of these apps, users have to give their consent to be tracked by the app. This means that mobility service providers have a large amount of mobility data at their disposal.

2.3 Mobile Network Data

Smartphones log in and out of mobile phone cells while their owners are traveling. Mobile phone companies can determine their users' approximate location at any time and create movement patterns using log data of the network. Each device generates up to 200 to 400 data points per day, depending on how active the user is.[4]

Mobile phone companies like *Telia*, *Telefonica*, or *Vodafone* divide their networks into geographical areas. Macrocells (used in rural or suburban areas) cover areas from 1 kilometer up to 20 kilometer in radius, microcells (urban environments, high user density) typically cover 400 meters to 2 kilometer in radius, picocells (very dense urban areas, inside buildings) cover areas as small as 4 to 200 meters in radius, and so called Small Cells in 5G networks can cover areas from about 10 meters up to just over 1.6 kilometers, providing highly localized coverage (Bindle et al. 2022; Chandler 2003).

Since cell phones regularly communicate with the mobile network (e.g., when changing cells, making calls, sending text messages, or transferring data), network operators can track their customers' movement patterns and locations. In densely populated areas, the mobility patterns can be more precise than in rural areas. Mobile phone providers are not allowed to share or sell mobility data of their customers to third parties without consent of their customers or without proper anonymization.

2.4 Connected Cars

Another important source of mobility data comes from connected cars. "Connected" can refer to two different things; in both cases mobility data is sent to the servers of car manufacturers or their service providers and is analyzed there. First, a relatively simple way of connecting cars to the Internet is the use of smartphone apps that car manufacturers have developed for the *Apple* or *Google* app ecosystems, like the "me-connect" app by *Mercedes-Benz*, the "My BMW" app by *BMW*, or the "Tesla Mobile App" by *Tesla*. By linking the smartphone and the vehicle's entertainment and diagnostic system, corresponding functions can be used: the driver can use the smartphone's phone functionalities or the playlist via the car's audio system, and car functions like locking or opening doors or windows can be used via the smartphone from outside the parked car. With the Internet connection via the smartphone, various web services can also be used and displayed in the car, such as information on free parking spaces in the vicinity of the vehicle. Even more integrated versions of this connecting car option are "Apple CarPlay" and "Android Car." These are used in *Volkswagen* vehicles, among others, and allow for even greater integration of car functions.

The second way of connecting cars to the Internet, respectively to the servers of car manufacturers, is to provide the vehicle systems with SIM cards as in the case of connected cars systems "BMW ConnectedDrive," "Mercedes me," "VW Car-Net," "Audi connect," "Ford SYNC," and others.

[4] https://business.teliacompany.com/crowd-insights/how-it-works; accessed: 09.07.2025.

Connected car systems collect position data as well as vehicle data. According to Gatzert et al. (2023, p. 14), connected car systems periodically transmit navigation data (routes, destinations), location and movement data (position, speed, acceleration and braking) as well as operating data (engine, speed, battery level, consumption), safety data (distance, lane keeping), and fault and maintenance data (oil level, brakes, wear). In addition, driver status data (fatigue detection, reaction time) is often transmitted to the servers of manufacturers.

Providers of connected car systems may only disclose mobility or other data from their service to third parties or share it with others if the users concerned have explicitly consented to this. Users generally give this consent by agreeing to the general terms and conditions of the service.

2.5 Other Car-Related Data Sources

Other car-related data sources which capture mobility data are roadside sensors to optimize traffic flows or video cameras capturing number plates in parking facilities. Roadside-mounted *LiDAR* (Light Detection and Ranging) sensors can provide highly accurate, real-time data on vehicle movements, including speed, volume, density, and classification. They can also detect abnormal events such as accidents or stalled vehicles. *LiDAR* systems are usually installed by transportation authorities or city governments to manage traffic flows. The data typically consist of anonymized object trajectories, the output is usually an object list (e.g., "car," "truck," "motorcycle") with movement patterns, not personal data (Ilic et al. 2023).

Using Automatic Number Plate Recognition (*ANPR*) cameras, vehicles can automatically be identified upon entry and exit in parking facilities, enabling seamless, ticketless access. Also, the data can be used to optimize parking lot management. In principle, operators gain valuable analytics on parking patterns, duration of stays. However, according to the *GDPR* the data may only be shared with third parties if it is essential for service provision (e.g., technical service providers, payment processors) or if the user has given explicit consent for further sharing or commercial use (Woods 2017).[5]

2.6 Market Research or Research Projects

Market research surveys, passenger surveys or surveys of research projects can also be sources for mobility data. Usually, mobility diaries or tracking apps are used to record and analyze the mobility behavior of passengers using public transport or of test persons over a certain period of time. These surveys are subject to specific regulations governing what may be done with the data collected and with whom it may be shared. The gathered data must be used exclusively for the purposes stated at the time of collection and cannot be repurposed without a new legal basis or explicit user consent.

Ministries and statistical offices also collect mobility data. For example, the German Federal Motor Transport Authority (*KBA*) regularly collects data in the areas of road freight transport, air transport, public transport and vehicle population.[6] In addition, there is the German Mobility Panel (*MOB*),[7] which conducts its own surveys on behalf of the German Federal Ministry of Transport (*BMV*). These official mobility data are only available in aggregated form and are claimed to not allow for the reconstruction of individual mobility patterns.

[5] See also: https://makewise.pt/blog/license-plate-identifier-how-complies-with-gdpr/; accessed: 12.07.2025.

[6] https://www.kba.de/EN/Statistik_en/statistik_node.html; accessed: 11.07.2025.

[7] https://mobilitaetspanel.ifv.kit.edu/english/index.php; accessed: 11.07.2025.

2.7 Summary

The presentation of the various sources of mobility data has shown that there are essentially three different types of data collection:

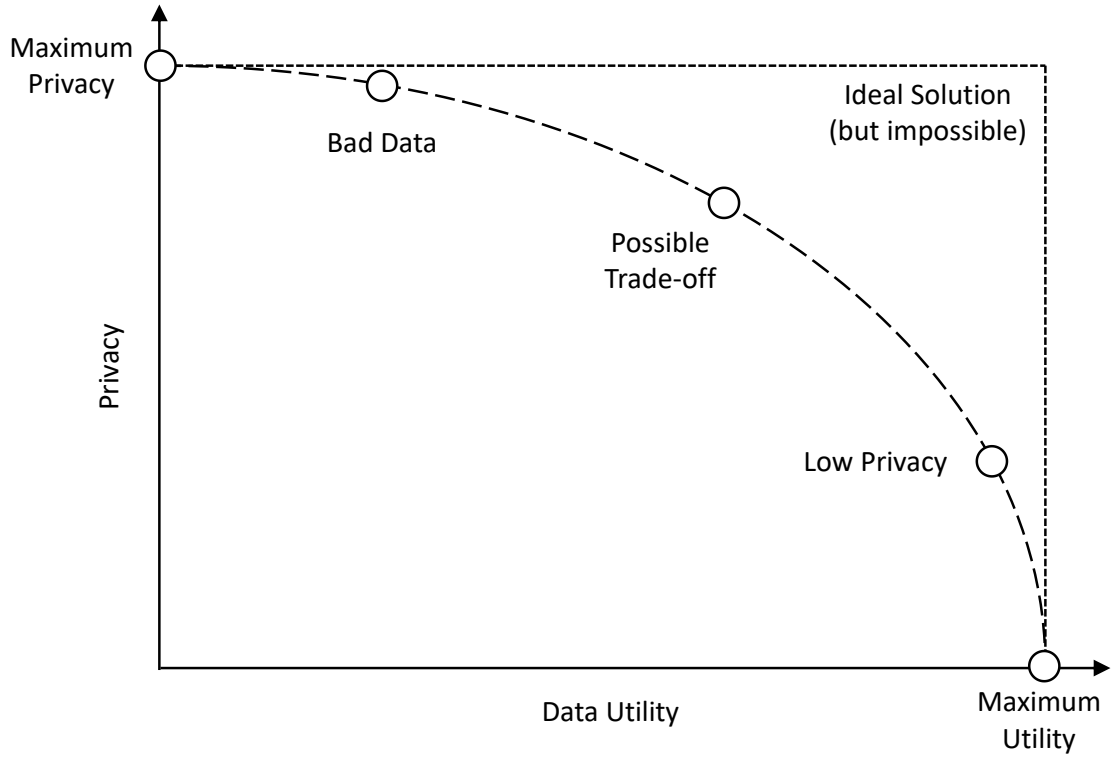
1) Mobility data that are *necessary for the functioning of devices and basic services*: Google's and Apple's location data from smartphones as well as network data from mobile phone providers.
2) Mobility data that external apps send to their providers and for which they obtain *implicit consent* from users by agreeing with general terms and conditions.
3) Mobility data that external apps send to their providers and for which users have *explicitly agreed* that it may be linked to their personal identifiable information, for example to enable integrated payment services.

Under no circumstances may personalized mobility data be shared or sold with third parties. However, this legal requirement is handled differently in practice. Providers' behavior is often not transparent, and there are sometimes ways to collect individual mobility patterns by combining datasets from different sources. To prevent this and to give providers the option of using mobility data in a way that complies with data protection regulations, anonymization technologies are available, which are described in the following section. Because, as already mentioned, the restriction that mobility data may not be shared or sold does not apply if the data have been fully anonymized according to legal terms, rendering it impossible to draw any conclusions about individual persons.

3 Anonymization and Pseudonymization Methods

Data anonymization encompasses methods to ensure users' privacy by transforming datasets in a way that single data entries cannot be ascribed to one individual anymore. The advantage of anonymizing datasets lies in sidestepping the *GDPR*, as Recital 26 to the *GDPR* explains. However, data anonymization comes at a loss of granularity, accuracy, or variance in the data set. The utility of an anonymized dataset will be necessarily lower than that of the original data set (Kapp and Mihaljević 2023). Figure 1 depicts in a symbolic manner this privacy-utility trade-off. When contrasting both the degree of privacy and the degree of data utility, the two cannot be attained at once. High data utility means that privacy will be low, while high data privacy simultaneously means bad data (low data utility). An ideal solution, in which both privacy and utility are high, is impossible with anonymization methods. A possible trade-off could be somewhere in-between high data privacy and high data utility.

Figure 1: Privacy-Utility Trade-off of Anonymization Methods



Source: https://aircloak.com/background/analytics-and-privacy/power-of-anonymization, accessed: 09.07.2024.

Anonymization methods belong to the broader group of privacy-enhancing technologies. Next to anonymization, privacy-enhancing technologies also encompass encryption or privacy-preserving data mining and machine learning (Elmimouni et al. 2023; Hafiz 2013), and pseudonymization, including cryptographic pseudonymization. For the sake of this paper's scope, we focus on data anonymization and pseudonymization and group the methods into four classes: (1) data cropping, (2) data generalization, (3) data perturbation, and (4) pseudonymization. In the following, each subsection will elaborate on the respective methods by briefly describing its characteristics, procedures, their relative and inherent level of securing data, and the negative impact on data utility. Table 1 provides an overview of the data anonymization and pseudonymization methods treated here.

Table 1: Overview of Data Anonymization and Pseudonymization Methods

Group	Method	Procedure	Inherent Security Level	Negative Impact on Data Utility
Data Cropping	Data Truncation	Reducing precision of data	Moderate	Moderate
	Field Removal (Data Redaction)	Completely remove fields or attributes from data set	Strong	Significant
	Subsetting	Select subset of data that is less sensitive or less identifiable	Strong	Significant
	Data Binning	Group continuous data into bins or categories (like histograms)	Moderate	Moderate
Data Generalization	Data Aggregation	Combine data from multiple records to create summary statistics (aggregate information)	Strong	Moderate to significant
	k-Anonymity	Ensure that each record is indistinguishable from at least k – 1 other records	Moderate	Moderate
	l-Diversity	Extend k-Anonymity by ensuring diversity within sensitive attributes	Stronger than k-Anonymity	Moderate to significant
	t-Closeness	Ensure that the distribution of sensitive attributes within a k-anonymous group is close to the overall distribution	Stronger than l-Diversity and k-Anonymity	Moderate to significant
Data Perturbation	Data Masking	Replace sensitive data with random or obfuscated values	Strong if masking process is robust and irreversible; vulnerable if masking pattern is predictable	Moderate
	Differential Privacy	Provides mathematical guarantees of privacy by adding controlled noise to data or query results	Strong, but depending on the choice of privacy budget parameter (ε)	Depending on privacy budget parameter (ε)
Pseudonymization	Pseudonymization in a narrow sense	Replaces identifiable information identifiers with pseudonyms; used when linkage of records is required for analysis (e.g., payment data)	Vulnerable if mapping is compromised	Moderate
	Cryptographic pseudonymization	Transforms readable values into encrypted ones, with which mathematical operations can be run, and delivers a result that can be decrypted via a private key	Relatively high due to modern architectures	None if only interested in the calculated results

Sources: Article 29 Data Protection Working Party (2014); Kapp (2022); Li et al. (2007); Machanavajjhala et al. (2007); Sweeney (2002).

3.1 Data Cropping

In general, *data cropping* is a privacy-enhancing measure that involves selectively removing, truncating, or aggregating parts of a data set to protect sensitive information. The goal of data cropping is to reduce the risk of identifying individuals or revealing sensitive attributes while maintaining as much data utility as possible for analysis and decision-making. These procedures typically remove data selectively by reducing precision and aiming for data utility high enough to eventually use and process a given data set (in the context of computer networks: Aleroud et al. 2021). In what follows, we present data truncation, field removal, subsetting, and data binning as data-cropping methods.

Data truncation removes parts of data fields to reduce specificity. It is commonly used for numerical data and dates. Numerical truncation removes decimal places or significant digits (e.g., replacing 123.456 with 123.4). Date truncation removes specific date components (e.g., replacing "2023-10-15" with "2023-10" or "2023"). As for the security level, data truncation reduces the precision of the data, making it harder to identify individuals. It provides moderate security, but the remaining data may still be identifiable if other attributes are available.

Field removal (data redaction) exhibits as characteristics to completely remove specific fields or attributes from the data set. It is often used for fields that contain highly sensitive or identifiable information. The procedure to do so is to identify fields that are sensitive or not necessary for analysis. These fields are then entirely removed from the data set (e.g., removing Social Security numbers or exact addresses). In so doing, this procedure provides strong security by eliminating sensitive information, but it may significantly reduce the utility of the data if important attributes are removed.

Subsetting selects a subset of the data that is less sensitive or less identifiable. Hence, this technique reduces the risk of identification by limiting the amount of information available. To attain subsetting, one can choose a random or non-random subset of records (e.g., selecting 10 percent of the total dataset). When performing it, it is important to ensure that the subset does not contain identifiable or sensitive information. Subsetting provides strong security by reducing the amount of data available for analysis. The effectiveness depends on the method used to select the subset; random selection typically offers better privacy than non-random subsetting.

Data binning as a procedure groups continuous data into bins or categories. This reduces the precision of the data to protect privacy. To do so, the algorithm defines ranges or bins for continuous data (e.g., ages 20 – 29, 30 – 39) as known from histograms. This replaces exact values with bin labels or categories. From the security side, data binning provides moderate data safety by reducing the precision of the data. The level of security depends on the size of the bins, as smaller bins offer less privacy but more utility.

3.2 Data Generalization

Overall, the group of *data generalization* as an anonymization method reduces the specificity of data to make it less identifiable. It often involves replacing specific values with broader categories by maintaining the overall structure and distribution of the data. The procedure to generalize is to replace exact values with ranges (e.g., replacing ages 25, 26, and 27 with the range 25 – 30) and to use higher-level categories. Compared to data binning presented before, data generalization can also be applied to non-continuous data types (e.g., replacing specific job titles with broader occupational categories). It provides privacy protection by making it harder to identify individuals. Data generalization may reduce data utility if too much generalization is applied and is vulnerable to re-identification if external information is available. In what follows, we present data aggregation, k-anonymity, l-diversity, and t-closeness as data-generalizing anonymization methods.

Data aggregation combines data from multiple records to create summary statistics and obscures individual data points by presenting aggregated information. It is commonly used in statistical reporting and analysis. This procedure calculates averages, sums, or other aggregate statistics (e.g., average income by region). As an additional level of security, publishing aggregated groups can be restricted to the number of group members trespassing a certain threshold (indistinguishability; Kapp 2022, p. 449). Overall, the method provides strong privacy protection by preventing access to individual data points. This can limit the granularity and utility of the data for detailed analysis and is less effective if the aggregated groups are too small.

k-Anonymity ensures that each record is indistinguishable from at least $k - 1$ other records (Sweeney 2002). This is achieved through generalization and suppression of data and aims to prevent identification through quasi-identifiers. The procedure generalizes quasi-identifiers to ensure each combination appears in at least k records, suppresses or removes attributes that cannot be generalized without violating k-anonymity. It is effective against identity disclosure but can be vulnerable to homogeneity and background knowledge attacks. The level of security depends on the value of k; higher values provide stronger privacy but may reduce data utility.

l-Diversity extends k-anonymity by ensuring diversity within sensitive attributes (Machanavajjhala et al. 2007). This method aims to prevent attribute disclosure by ensuring that sensitive attributes have at least l distinct values within each k-anonymous group. When applying l-diversity, k-anonymity is first performed and then ensured that sensitive attributes are sufficiently diverse within each group. The method uses techniques such as slicing or partitioning to achieve l-diversity. The security level provides stronger privacy protection than k-anonymity by addressing homogeneity attacks. The level depends on the value of l; higher values provide stronger privacy but may reduce data utility. Thus, it is still vulnerable to certain attacks, such as skewness attacks.

t-Closeness is characterized by ensuring that the distribution of sensitive attributes within any k-anonymous group is close to the overall distribution (Li et al. 2007). This method aims to prevent attribute disclosure by preserving the global distribution of sensitive attributes. The procedure is to apply k-anonymity and then measure the distance between the distribution of sensitive attributes within each group and the overall distribution. One has to ensure that the distance (measured by a chosen metric) does not exceed a threshold t. The method provides stronger privacy protection than k-anonymity and l-diversity by maintaining distributional similarity. The level of security depends on the value of t; lower values provide stronger privacy but may reduce data utility. It is effective against skewness and similarity attacks.

3.3 Data Perturbation

In general, *data perturbation* adds noise to data values to obscure the original data and ensures that individual data points cannot be precisely identified. This group of methods maintains overall data patterns and distributions. Data perturbation adds random noise to numerical values (e.g., adding small random values to salaries) and uses techniques such as randomization, swapping, or perturbation functions (in the context of data mining: Kargupta et al. 2003). It generally secures if the noise addition process is robust, and the noise is sufficiently random. It is vulnerable if the noise can be statistically removed or minimized. These methods are suitable for applications where data analysis requires approximate values rather than exact ones. This section presents data masking, pseudonymization, and differential privacy as methods of data perturbation.

Data Masking replaces sensitive data with random or obfuscated values, which ensures that the original data cannot be easily recovered. It is often used when the exact values are not needed for analysis. The procedure replaces sensitive data with random characters or predefined patterns (e.g., replacing credit card numbers with "XXXX-XXXX-XXXX-1234"). Thus, data masking uses techniques

such as shuffling or substitution to mask data values. This method is generally secure if the masking process is robust and irreversible, but vulnerable if the masking pattern is predictable or if masked data can be linked to external information. Data masking is suitable for protecting data in environments where exact values are not critical.

Differential privacy provides mathematical guarantees of privacy by adding controlled noise to data or query results. It ensures that the inclusion or exclusion of any single individual's data does not significantly affect the outcome and is widely used in statistical analysis and machine learning. The procedure is to add random noise to query results based on a privacy budget parameter (ε) by introducing noise with techniques such as the Laplace or Gaussian mechanisms. The method offers strong theoretical guarantees of privacy, as the level of security depends on the value of the privacy budget (ε). Lower values provide stronger privacy but may reduce data utility (Dwork 2006).

3.4 Pseudonymization

Generally speaking, *pseudonymization* replaces unique information identifiers (e.g., names, Social Security numbers) with pseudonyms (Sampaio et al. 2023, p. 3834). This allows data to be linked without revealing the actual identities. This method is often used when the linkage of records is required for analysis, for instance, for payment data or mailing addresses. We distinguish pseudonymization in a narrow sense and encrypted pseudonymization, depending on whether random, hashed, or encrypted values maintain a mapping between pseudonyms and original values in a secure location. The procedure provides privacy protection by obscuring direct identifiers, and depending on the method used, i.e., random, hashed, or encrypted values, vulnerability of the mapping between pseudonyms and original values varies. Vulnerability is higher for random and hashed values, and very low when performed with cryptographic methods. It is suitable for applications where data linkage is necessary but direct identification is not required (European Data Protection Board 2025).

Despite the seeming weakness of re-linkage—and thus re-identification—of individuals, pseudonymization can represent a realistic alternative to anonymization in the context of mobility data. Cryptographic methods, such as Homomorphic Encryption (*HE*), allow for performing calculations with the encrypted content. The calculated results are then readable with the help of a private key (Acar et al. 2018). In this manner, data are saved securely, the mathematical operations are performed on the encrypted data, and only through a private key is it possible to access the results, i.e., not the data as such.

Next to *HE*, Trusted Execution Environments (Sabt et al. 2015) and Confidential Computing (Mulligan et al. 2021) can be named as realistic alternatives to anonymization. The former offers isolated processing environments to securely execute applications, irrespective of the rest of the system. The latter provides strong integrity and confidentiality guarantees to both code and data contained within it.

4 Use of Mobility Data and the Role of Anonymization Technologies

In this section, we present how mobility data is being used by different market players. The market players can be differentiated according to whether they collect mobility data themselves, such as smartphone operators or mobility providers, or whether they only use it, such as municipal traffic planners or data brokers. Some services use mobility data from more than one source and link, for example, smartphone data with roadside sensors. When presenting the respective use scenarios, we ask to what extent anonymization technologies contribute to ensuring privacy-enhancing use of mobility data.

4.1 Smartphone App Providers

The tech companies *Google* and *Apple* use location data from smartphones for a variety of purposes, including navigation systems with real-time traffic notifications and location-based services such as the display of nearby stores and offers. For example, *Google* can identify common locations like home and work based on time and position and suggest relevant routes based on this information. Also, *Google Maps* shows "Popular Times" and live crowdedness information for businesses and public places, based on anonymized, aggregated location data from users' smartphones. In addition, both companies are involved in the development of autonomous driving technologies and use mobility data to analyze driving behavior, traffic flows, and environmental conditions to train and improve their systems.

During the COVID-19 pandemic, *Apple* released a mobility trends tool that uses aggregated data from *Apple Maps* to show changes in the volume of people driving, walking, or using public transit. These data were generated by counting the number of direction requests in *Apple Maps* and were shared in an anonymized, aggregated format.[8]

Google and *Apple* neither directly sell location data collected from smartphones, nor do they provide access to third parties. They use the data exclusively to develop and maintain their own services. And although both companies prohibit app developers in their app ecosystems from selling personal and sensitive user data, including device location, they cannot fully control the collection and sale of such data by external app providers (see Keegan and Ng 2022 and next section on app service providers).

Furthermore, the fact that *Google* and *Apple* sell location-based advertising slots to external partners (but not the location data itself) through their real-time bidding (*RTB*) systems, is interpreted by some experts as an indication that personal data are disclosed through this process and that data are used for applications that users have not actively approved (Cilento 2024).

In its data protection terms, *Google* points out that anonymization processes such as generalization (k-Anonymity) and noise (Differential Privacy) are used to share data securely with external partners.[9] However, the number of organizational data was actually shared which seems limited and was obviously related to coping with the effects of the COVID-19 pandemic: Between 2020 and 2022 mobility data were shared to a number of academic and public health researchers for studying

[8] https://www.apple.com/newsroom/2020/04/apple-makes-mobility-data-available-to-aid-covid-19-efforts/; accessed: 09.07.2025.

[9] https://policies.google.com/technologies/anonymization?hl=de; accessed: 09.07.2025.

the effects of COVID-19 and supporting public health responses, according to a report by the *Future of Privacy Forum*.[10]

Other than that, *Google* maintains partnerships with data companies like *Trafi* to improve the reliability of public transport data in *Google Maps* by integrating and curating real-time and scheduled mobility data from cities worldwide. *Google* says that this partnership is focused on enhancing service quality and not about sharing individual user data.[11] Another example of enhancing its own services is *Google's* partnership with motorway operator *Albertis* which aims to optimize mobility management using cloud-based analytics and aggregated mobility insights. Again, no individual mobility data are said to be used.[12]

4.2 Mobile App Providers, Especially Public Transport and Shared Mobility Providers

External app providers also use mobility and location data of smartphones; however, they cannot access the device data directly but require the users' consent to track their respective positions. This consent is usually given when users accept the terms and conditions of the service.

The community-based navigation app *WAZE* (a *Google* subsidiary since 2013) is an example of an external navigation app using mobility data from smartphones, input by the users and data from cities and municipalities. Beneath suggestions that users can get for alternative routes in case of traffic congestion, the app also informs others about traffic jams, roadworks, accidents, police checks, etc. (Hoseinzadeh et al. 2020).

Another example of an external smartphone app using mobility data is charging station finder apps by car makers (*Tesla Supercharger*), electricity providers (*EnBW mobility+*) or software companies (*Chargemap*, *easyCharging*). These apps use data from roadside sensors, connected cars and smartphones and help owners of electric vehicles to find available charging stations on their route. Some apps can combine users' mobile phone location data, the vehicle's current battery charge level, and the selected destination to suggest free charging stations and to make reservations (see, e.g., Darley 2025).

Public transport providers can use mobility data to optimize bus and railway traffic or to plan for new lines. For this, they can rely on data from their own apps but also on other mobility data like data from surveys, from mobile telecom providers, or even from data brokers.

Drawing on data from their own apps, mobility service providers like railway or bus companies can use mobility data to improve their services. With data from their apps they can not only analyze the movement patterns of their customers but are also able to carry out in-depth evaluations of customer behavior as they can link the mobility data to the user profile in their customer database. Movement data from their apps may not be shared with other actors except when it is properly anonymized.

One example of using data from mobile apps for mobility services in Germany is *Deutsche Bahn's* "DB Navigator" which provides information about connections, delays and alternative routes based on the location of the user. Real-time data for this service is provided by the public transport data hub (German: "Datendrehscheibe") which is fed by different in-house data systems such as the Intermodal Transport Control System (*ITCS*) or passenger information systems. In fact, *Google Maps* also has access to these data (see Driftschröer 2023) and can display delays and alternative public

[10] https://fpf.org/uncategorized/google-covid-19-community-mobility-reports/; accessed: 09.07.2025.

[11] https://maas-alliance.eu/2024/10/10/google-maps-and-trafi-extend-partnership-to-improve-global-travel-information/; accessed: 09.07.2025.

[12] https://www.abertis.com/news/abertis-partners-with-google-cloud-to-transform-interurban-mobility-management/; accessed: 09.07.2025.

transport connections via *Google Maps* as well. However, not all local and regional public transport systems operated by *Deutsche Bahn* and its partners are integrated yet.

Other examples of how public transport providers can use mobility data are capability planning (additional buses or trains, longer or shorter trains, faster timing, route optimization, etc.) and personnel resource planning. The conventional way of obtaining passenger data has been via passenger surveys; an automated way would be via digital ticketing or check-in/check-out data from smart cards like the *Oyster* card which is used in London. In addition to using their own data, public traffic providers can use telecom data in an aggregated form to analyze mobility patterns and identify bottlenecks.

Mobility-as-a-Service apps go beyond the provision of delay information and can display the location, availability, etc. of various means of transport (e.g., train, bus, rental bikes, scooters, etc., see Metzger and Krauss 2024). Car-, bike-, and scooter-sharing companies can use mobility data to optimize their fleet management and service quality. Here, mobility data can be used to position vehicles close to predicted demand and to plan the fleet size. Fleet data, including the position of the vehicle, last trips, battery level, etc. are transmitted constantly to the provider and can be analyzed accordingly. Again, individual mobility data may not be shared with third parties unless it is properly anonymized (Widhalm et al. 2023).

4.3 Telecom Companies' Cellphone Data

Aggregated and anonymized network data from mobile telecommunication providers are used to offer consulting services or to be sold to third parties. For example, the Swedish telco company *Telia* offers routing reports to municipalities to help them decide where to situate public facilities such as car parking, food kiosks, and bicycle stands. According to *Telia*, the company delivers data daily—and as part of the anonymization process with a 36-hour delay. They can also deliver data going back two years or more which could be used to better understand mobility patterns and trends. The data allow for the analysis of crowd movements between different parts of the city, for example, where people commute to and from each day. *Telia* has developed solutions that can aggregate data in real time and trigger alerts when the number of people in an area exceeds a predefined threshold, such as on beaches to prevent overcrowding. This suggests that near-real-time crowd density information is possible. However, for most applications, especially those involving public dashboards or analytics for city planning, data is not provided in real time. There is typically a delay (often 24 to 48 hours) due to legal and ethical requirements for anonymization and aggregation, according to *Telia*.[13] *Telia* mobile network data can also be used to analyze crowd flow at large-scale events. Target groups of *Telia*'s consulting services termed "Crowd Insights" are municipalities, urban planners, real estate developers, the retail sector, and public transport providers.

In Germany, data-science company *Invenium Data Insights* uses aggregated mobility data from the mobile phone company Telefonica to analyze visitor flows. For example, they were able to identify the most popular fairground attraction of Munich's *Oktoberfest* or the hometown and arrival routes to a football match in Munich's *Allianz Arena*.[14]

4.4 Car Manufacturers and Insurances

Car manufacturers have different strategies concerning the use of the data collected from their connected car apps. In general, automakers in Europe as well as the United States cannot freely dispose of the collected data. They are required to inform users of their apps about data collection

[13] https://www.telia.fi/business/article/privacy-comes-first-newsroom; accessed: 09.07.2025.

[14] www.telefonica.de/partner/wholesale/enabling-services/mobility-insights.html; accessed: 09.07.2025.

and give them options to access, delete, and opt out of the collection and use of their personal data. Data can only be shared with third parties when users explicitly designate those parties. Nonetheless, car manufacturers have shared and sold connected car data with third parties in the past and obviously continue to do so. The e-journal *LLRX*, operated by editor and publisher Sabrina I. Pacifici, collects various violations by car companies especially in the USA in the use of mobility data, for example of selling data to insurance companies, advertising and market research companies, service providers or commercial data brokers.[15] One of the problems, according to Pacifici, is that privacy statements are "buried in terms of service on everything you use, and for the most part, are automatically set to 'opt-in,' requiring you to locate and 'opt-out' of processes which in many cases, will continue regardless of your actions." (see ref. in footnote 12; see also Cox 2021).

According to a Mozilla study from 2023, which analyzed the privacy policy statements of 25 international car manufacturers, 84% of car manufacturers said they can share personal data with service providers, data brokers, and other businesses. What is more, 19 (76%) of the car brands examined, the privacy documents indicate that the manufacturers reserve the right to sell the data in an aggregated or otherwise anonymized way. The authors of the study question whether the anonymization is really done and state that the data flows between connected cars and third parties are very opaque: "We can't know how that information is handled. What we do know is that there's a booming industry based on selling data from cars" (Caltrider et al. 2023, para. 25). Furthermore, there are car manufacturers that share their data with specialized data firms or on platforms with the aim of supporting open-source-developed new services (Strategiedialog Automobilwirtschaft BW 2024).

While some car manufacturers sell mobility data to generate an additional source of income, other manufacturers use the data from the connected car app to create their own value-added services or to improve their services. For example, sensor data from connected cars are measuring the shock absorber movement. Combined with location data, these data can be used to identify potholes in roads and automatically inform road maintenance teams to repair them. Also, sensors measuring *ABS*- or *ESP*-events can indicate critical street conditions and warn other drivers about slippery or icy roads or inform winter service vehicles. For example, *Volvo*, *Audi* and *Skoda* have developed such systems.[16]

Car insurance companies can offer their customers individual rates based on their driving needs and behavior. The mobility data for such "pay as you drive"/"pay how you drive" services is either collected by a special telematics device ("black box") which can be installed in the car, or a mobile app on the driver's smartphone which automatically records driving data.

These systems can monitor the total distance driven, the time of day when the car is driven, driving behavior (e.g., acceleration, braking, cornering) and the location data (via GPS). The collected data are transmitted to the insurer who uses them to calculate the individual insurance fee. Safer and less frequent drivers can benefit from lower insurance costs. While there are at least no legal concerns here, because consent for tracking has been explicitly obtained, the handling of the data collected can prove problematic. This is because car insurance companies are highly motivated to obtain mobility data in order to better assess risks and to save costs. In 2024, it became known that US-insurance company *Allstate* and its data subsidiary *Arity* unlawfully collected, used, and sold data about the location and movement of 45 million US citizens using mobile apps. *Allstate* did not only use the data for their own optimization purposes but also sold the data to other insurance companies without user consent or anonymization (Hill 2024; Paxton 2025).

[15] www.llrx.com/2025/01/automakers-are-collecting-sensitive-data-and-selling-it-without-your-permission; accessed: 09.07.2025.

[16] See for example https://www.media.volvocars.com/global/en-gb/media/pressreleases/251381/volvo-models-across-europe-to-warn-each-other-of-slippery-roads-and-hazards; accessed: 09.07.2025. For further examples see Lober (2023).

4.5 Municipalities and Urban Planners

Municipalities and urban planners use mobility data to realize smart city concepts which may include managing parking spaces, connected mobility, sustainability goals, or the prevention of overtourism. For example, in the German city of Füssen, a solution called *OptiPark* was implemented. Location data from parking sensors and connected cars are used. Data from parking sensors are not considered personal data and thus do not need to be anonymized. Data from connected cars can be used with user consent and if properly anonymized. The *OptiPark* system accesses the data via the German mobility data platform "Mobilithek." Depending on the situation, drivers entering the city will be shown the availability of parking spaces on display boards or in a special smartphone app (Urban Institute [ui!] 2021).

Urban traffic planners can also use mobility data to optimize traffic flows and traffic light waiting times. Movement data from connected cars, for example, can be used for this purpose. According to a study by the University of Michigan, data from a small number of connected cars is sufficient to optimize traffic light patterns and to achieve a 20% to 30% decrease in the number of stops at signalized intersections (Wang et al. 2024).

Municipalities in cooperation with charging point operators and electricity providers can use mobility data to determine the best location of future charging stations (see for example Radermecker and Vanhaverbeke 2023). For that matter, data from connected cars or smartphone location data can be used to analyze vehicle movements and combine these with demographic data from statistical offices or from data brokers (median income of a neighborhood, population density), existing points of interest, or number of electric vehicle registrations in city districts. New charging stations thus can be built where demand is expected. Here, too, mobility data can be used for better planning, provided it has been anonymized accordingly (see, e.g., Eurelectric 2024).

City planners and public administrations can use aggregated mobility data to improve the overall interaction of all modes of transport in order to optimize traffic flows and/or to achieve sustainability goals for their city or region. Municipalities can use mobility data from different sources, including data from ministries and statistical offices, to plan for mobility hubs (in cooperation with transport providers), bicycle roads, parking facilities, pedestrian zones, etc. (Chitturi and Puentes 2023; Müller-Eie and Kosmidis 2023).

Municipalities can also use mobility data to prevent overtourism or to direct flows of people in case certain attractions are overcrowded. Mobility data from telecom companies, from data brokers, or data platforms can be used to gain insights about mobility patterns of tourists (where do they go, what do they visit?). For example, in Venice, Italian telecom provider *TIM* tracks mobility patterns of tourists on behalf of the municipality. The analysis is based on connections to the mobile network (such as when a device connects to a cell tower or uses data services), not on the advertising ID of smartphones. According to *TIM*, the data is anonymized and aggregated before being processed, with device identifiers changing regularly (e.g., every 24 hours) to prevent tracking of individuals over time (Mizzi 2022). Using cell network data and SIM data of tourists' smartphones, their country of origin can be determined. Also, tourists are analyzed concerning their kind of visit—such as a day trip or overnight stay—and where they are most likely to go, with Saint Marks Square being one of the most populated areas (Bubola 2021).

4.6 Advertising Companies and Retailers

Advertising companies and retailers use mobility data to target individuals or to plan new stores at commercially interesting locations. "Targeted marketing," "proximity marketing," "geofencing," or "geolocation-aware marketing" are the keywords for strategies of advertisers and marketing departments to target consumers with information related to shops and offers in their proximity. By

utilizing mobility data, businesses can send targeted messages, promotions, and content to users based on their location.

Advertisers and businesses can use consumer profiles created by *Google Analytics*, *Apple's Visitor Analytics* or *Facebook Users* which analyze users' web history and preferred places. These data can be used to build detailed consumer profiles, which can include demographics, interests, past behavior, and location data—if users have granted location permissions to apps. This location can be matched with the user's profile to deliver targeted ads in real time, often through programmatic ad exchanges that sell ad space within seconds (see section "Smartphone App Providers"). While platform providers claim to anonymize or aggregate data, much of the ad targeting relies on persistent identifiers (cookies or advertising ID of smartphones) that are not strictly anonymous. True anonymization (where the identifier cannot be traced back to an individual) is rare in digital advertising, as the effectiveness of targeted ads depends on the ability to link data points to a unique user or device.

For retailers, mobility data can be helpful when deciding about locations for new stores. Retailers want to identify areas with high foot traffic and areas where their target groups are present. Data from mobile telecom providers or data brokers can be used for that matter, combining demographic information (age, gender, purchasing power, etc.) time of visit, and origin of trip. This type of use of mobility data can take place at an aggregated level and be realized with anonymized data.

4.7 Data Brokers

When listing the various data sources, it became clear that mobility data often remain with the service providers, thus forming the basis for their own services. However, mobility data are often sold to other companies like data brokers. Data brokers are companies that buy, collect, and analyze data about individuals or from devices to turn them into structured data sets and sell them to customers. Also, data brokers offer consulting services based on their data analysis. Data brokering is a multi-billion Dollar business which is mainly focused on marketing and advertising, financial services as well as health services (see Azcoitia and Laoutaris 2022). The added value of data from data brokers lies in the linking of mobility data with socio-demographic characteristics and interest profiles of customers. Examples for use cases are location-based advertising, identifying locations for new stores, insurance liability assessment, traffic routing, or urban planning.

The website *Datarade.ai* provides a comprehensive list of commercial data brokers for geospatial data. It displays many companies providing mobility data like *CITYDATA.ai*, *Factori Mobility Data*, *Irys Map Data Insights*, *Redmob Mobility Data*, or *Quadrant Mobile Location Data*. These data brokers differ in terms of origin and scope of the mobility data used, their coverage and specialization in fields of application.[17]

Important data brokers for car mobility are, for example, *INRIX*, *CARUSO*, *Verisk*, and *LexisNexis*, according to a 2022 study (Keegan and Ng 2022; see also Sanchez 2024). Mobility data collected originate from connected cars or are collected through smartphone apps that have obtained user consent for location tracking. It includes anonymized movement patterns, location visits, and dwell times, allowing businesses and mobility providers to analyze mobility patterns and consumer behaviors. *INRIX* offers parking, traffic, and navigation data to transportation agencies, car manufacturers, and software developers looking to add mobility features. *CARUSO* offers a data marketplace for European vehicle data. Its "data catalog" section of its API documentation lists 245 distinct vehicle data points. *Verisk* and *LexisNexis* offer their own vehicle data exchanges, addressing their services to both car manufacturers and insurance companies (Keegan and Ng 2022).

[17] https://datarade.ai/data-categories/mobility-data; accessed: 27.11.2024.

An interesting example of a data broker is the San Francisco-based company *citydata.ai*. The company is active worldwide and claims its data-as-a-services products are used for smart city programs, economic development, urban planning, mobility and transportation, tourism, disaster impact analysis, sustainability and resilience.[18] The company focuses on civic projects. Concerning privacy and anonymization, the website of *citydata.ai* states:

> Our datasets do not include any PII (Personally Identifiable Information) or personal data. In other words, we do not collect or store names, emails, phone numbers, dates of birth, credit cards, transactions, or national identifiers in our cloud. Our technology platform incorporates privacy by design. We hash identifiers for anonymization, perturb geo coordinates for obfuscation, and aggregate data over a grid for privacy compliance. We also apply differential privacy techniques in the form of Laplacian noise.[19]

Similar statements emphasizing that mobility data are anonymized data and only used to identify patterns and trends at the group level, not to track individual behaviors, can be found on the websites of other data brokers as well. They also claim that their anonymization platforms are designed to meet all relevant data protection standards, such as *GDPR*. However, according to many sources, the mobility data business remains a legal grey area. Criticism from data protectionists is directed in particular toward the practice of using mobility data from the tracking of smartphone apps. They argue that there is no conscious consent to tracking if this consent is hidden in the app's terms and conditions or in opaque menus (see, e.g., Dachwitz 2023; Gadotti et al. 2024). Taking these objections seriously, the issue in the area of data brokers is less about the correct use of anonymization technologies than about the circumstances of data collection and the dubious business practices of the respective companies.

[18] See citydata.ai website; accessed: 27.11.2024.

[19] https://citydata.ai/#Privacy, accessed 06.07.2025.

5 Summary and Outlook

In this article, we provided an overview of data sources, anonymization and pseudonymization methods, and the various fields of application for mobility data. In so doing, we have pursued the question of how mobility data can be used for innovative value-added services in compliance with data protection regulations and have focused on the question of whether anonymization technologies are a suitable privacy-preserving method. Next to data anonymization methods, we also presented pseudonymization as an alternative to protect mobility data. Pseudonymization through cryptographic methods (Homomorphic Encryption; *HE*) seemed a particularly suitable alternative to anonymization of mobility data. Because data exchange via commercial data brokers is fraught with certain difficulties, as described above, alternatives have been tested for some time in which data is exchanged via non-commercial platforms.

In this section, we first summarize the challenges tied to mobility data anonymization, then present three alternatives to pure data anonymization: a technical measure and two institutional measures. First, we present cryptographic pseudonymization as a stronger and more flexible way of protecting data as a technical method. A second measure consists of mobility data exchange platforms, and a third of data trustees.

5.1 Challenges in Mobility Data Anonymization

In the last case discussed—the use of mobility data by data brokers—we have seen the ambivalence lying in this sector: while data brokers claim that they use the latest anonymization technologies, the real problem rather seems to be the lack of trust in data protection-compliant business practices of these actors. And it turned out that this problem already arises during the collection and transfer of data, which to a certain extent relativizes the anonymization issue. In other fields of application, however, we have shown that anonymization technologies can be a very important tool for enabling innovative services, i.e., for deriving benefits from anonymized data.

In fact, anonymization is fundamentally challenged for two reasons. The first lies in the density of mobility data, i.e., its high frequency of collecting data points, and cross-tabulating these data with secondary datasets. While effective anonymization is often claimed by operating companies and organizations, intersecting mobility datasets with census data (Hsu et al. 2021), real-time *Google Maps* traffic data (Akhavan et al. 2019), or local household surveys as well as data generated by the US Department of Transportation (Adler et al. 2017) means that anonymization is *de facto* impossible. The second reason lies in the inherent nature of mobility data. Because of their longitudinal—that is temporal—characteristic repeated movement patterns in space can easily be brought back to individuals. Human mobility traces are found to be highly unique and are moderated by the hourly rate and the spatial resolution chosen. De Montjoye et al. (2013) found that for mobility data collected via mobile networks four spatial-temporal points are sufficient to uniquely identify 95% of the individuals of the sample. Anonymization is therefore often a "mission impossible" (Borges 2021, p. 24).

Recently, the European Data Protection Board (*EDPB*) launched a guideline on data pseudonymization (European Data Protection Board 2025). Even though the focus lies on pseudonymization in contrast to anonymization, important conclusions can be drawn from this document. With data anonymization, data are processed in a way individuals *cannot* be identified, whereas with pseudonymization, data can no longer be attributed to a specific individual *without additional information*, which, however, is kept separate or secret. Whereas anonymized data are not considered personal data and are exempt from data protection laws (Recital 26 tied to the *GDPR*), pseudonymized data are still considered personal data and fall under data protection regulations.

Because of the findings outlined above and seen in view of the definition of anonymization versus pseudonymization, we argue that in many cases pseudonymization should be preferred. This is because even if anonymization methods are employed to treat mobility data, the existence of secondary datasets and the very nature of these data *de facto* downgrade anonymization technologies to pseudonymization methods. The linkage between an individual and his or her movement pattern is re-identifiable by its very nature and can be done at a practical level if one applies the appropriate effort.

5.2 Cryptographic Pseudonymization as a Realistic Alternative

Seen in light of the difficulty of truly anonymized motion and location data, the measures taken by data-collecting companies and data brokers are often insufficient to grant privacy at the level of legal requirements. To recall, Recital 26 to the *GDPR* stipulates that the "principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." Although data brokers widely claim "anonymization" of these data and even if anonymization methods named in the previous section are used, like data aggregation (Gebhart 2022), the nature of longitudinal and repeated patterns allows for de-identification of individuals (de Montjoye et al. 2013).

Modern forms of Homomorphic Encryption (*HE)* allow for the calculation of all mathematical operations (so called Fully Homomorphic Encryption, *FHE*; Gentry 2009), and newer developments in the computational architecture (Trusted Execution Environments/Confidential Computing; e.g., Beskorovajnov et al. 2025) make the practical use of *HE* a realistic case. Viewed from this perspective, while being a form of pseudonymization, the advantage of *HE* promises it to be a serious alternative to anonymization methods. The main advantage of *HE* as a pseudonymization method is its practical irreversibility due to the computational architecture and the trust-based securities.

And yet, because there is no privacy-utility trade-off in cryptographic pseudonymization, this method seems a better choice than seemingly anonymized data. The latter comes at a double cost: lower utility and anonymization that *de facto* is not given. As we concluded earlier in this section, although anonymization methods are applied to mobility data, their de facto state is only a pseudonymized one because of the low barriers to intersecting them with secondary datasets or to identifying the unique movement patterns of individuals. Consequently, from a technical perspective, it seems more promising to remain in the domain of pseudonymization. That would mean taking the highest technical measures possible today and using cryptographic pseudonymization. As a consequence, the *GDPR* would apply because of the non-provable anonymity of the dataset. Consent then would be needed from the users. However, the security level will be higher than anonymization.

5.3 Mobility Data Exchange Platforms

In order to promote innovative mobility services, mobility data platforms have been initiated in recent years that focus on the idea of exchanging mobility data between providers and users. In most cases, these data platforms have been financed by public authorities to promote standardization and exchange. The background to this is the observation that data providers, such as vehicle manufacturers, public transport companies, or public administrations on the one hand, and data users on the other often do not know what datasets are available and how they can be accessed.

In Germany, the Mobility Data Marketplace (*MDM*) has been established as such a data ecosystem for publicly available mobility data, published by public administrations. The marketplace is funded

by the German Federal Ministry of Transportation (*BMV*) and was transferred to the new "Mobilithek"[20] in 2023.

Another mobility data ecosystem which focuses on data from companies (and not from public bodies) is the "Mobility Data Space (*MDS*)".[21] This project is privately funded and co-financed by the German federal government. In the *MDS*, companies can share their mobility data securely and transparently while maintaining data sovereignty. A car manufacturer, for example, offers anonymized parking data from its vehicles for parking space searches and parking space planning services. Standardized terms of use apply to all participants in the data space and a specific software, known as a "Konnektor," which guarantees the secure delivery and removal of data (Beirat Digitalstrategie Deutschland 2023). From a technical point of view, the *MDS* does not store data—it only describes them in a catalogue. The data are only ever exchanged on a peer-to-peer basis between the transaction partners. This gives the data provider control over who receives their data and the associated terms and conditions. According to the description on its website,[22] one big advantage of the *MDS* is that it is a standardized platform, as an industry-standard interface is used for accessing the data catalogue and for data transmission. This means that participants do not need their own individual data exchange interfaces and formats. Furthermore, the platform's technical design complies with EU data space standards and is compatible with other data spaces and the European data infrastructure Gaia-X. Another benefit of the *MDS* is its community, "where mobility professionals can link up and develop new use cases," as one self-description puts it (Mobility Data Space 2024, p. 1). In the year 2023, data of *Mobilithek* were integrated into the MDS and can since be accessed via the latter.[23]

5.4 Data Trustees

Another option for exchanging mobility data between stakeholders is the data trustee model. Data trustee models are always advantageous when there are conflicts of interest between the parties involved and transparency and confidentiality are required at the same time. Conflicts of interest exist, for example, between vehicle manufacturers, suppliers, service providers and users in financing, fleet management, car sharing, or in the field of automated driving (ETA 2024).

Data trustees are neutral bodies that anonymize mobility data and process them in accordance with data protection regulations in order to make them available to other stakeholders (Specht-Riemenschneider and Kerber 2022).

Data trustee models for mobility data have been developed and tested in various publicly funded projects since 2022. Examples in Germany include the *MobiDataSol* project in Solingen, Germany, which aims to establish its own data ecosystem in the smart city context, the *KomDatIS* project in Mönchengladbach, Germany, which aims to establish a municipal data trustee for mobility data, and the *TRANSIT* project for logistics data. Mobility platforms like the above-mentioned *MDS* can also be integrated into data trustee models.

A core aspect of data trustee models is the implementation of robust data protection measures, for which anonymization technologies and procedures for personal mobility data are being developed and applied. Considered by politicians and stakeholders to be an important path for the future, the successful realization of comprehensive data trustee models currently requires above all practical implementations and an exchange of best practices (see, e.g., Data Spaces Support Centre 2024).

[20] https://mobilithek.info; accessed: 27.11.2024.

[21] https://mobility-dataspace.eu; accessed: 27.11.2024.

[22] https://mobility-dataspace.eu; accessed: 27.11.2024.

[23] https://mobilithek.info/blog/die-mobilithek-im-datenraum; accessed: 23.07.2025.

Acknowledgments

The present paper was part of the work performed in the *ANYMOS* project (*Anonymisierung für vernetzte Mobilitätssysteme*), funded by the German Federal Ministry of Research, Technology and Space (BMFTR) under the grant no. 16KISA087. We are grateful for valuable feedback by Lukas Kneis and Wasilij Beskorovajnov (both *Forschungszentrum Informatik*, *FZI*, Karlsruhe).

References

Acar, Abbas; Aksu, Hidayet; Uluagac, A. Selcuk; Conti, Mauro (2018): A Survey on Homomorphic Encryption Schemes: Theory and Implementation. In: ACM Comput. Surv. 51 (4), p. 79:1-79:35. https://doi.org/10.1145/3214303

Adler, Thomas; Bernardin, Vince; Dumont, J.; Flake, Leah; Sadrsadat, Hadi; United States. Federal Highway Administration (2017): The Promise and Limitations of Locational App Data for Origin-Destination Analysis: A Case Study. (Nr. FHWA-HEP-20-022).

Akhavan, Armin; Phillips, Nolan Edward; Du, Jing; Chen, Jiayu; Sadeghinasr, Bita; Wang, Qi (2019): Accessibility Inequality in Houston. In: IEEE Sensors Letters 3 (1), pp. 1–4. https://doi.org/10.1109/LSENS.2018.2882806

Aleroud, Ahmed; Yang, Fan; Pallaprolu, Sai Chaithanya; Chen, Zhiyuan; Karabatis, George (2021): Anonymization of Network Traces Data through Condensation-based Differential Privacy. In: Digital Threats 2 (4), p. 30:1-30:23. https://doi.org/10.1145/3425401

Article 29 Data Protection Working Party (2014): Opinion 05/2014 on Anonymisation Techniques.

Azcoitia, Santiago Andrés; Laoutaris, Nikolaos (2022): A Survey of Data Marketplaces and Their Business Models. In: SIGMOD Rec. 51 (3), pp. 18–29. https://doi.org/10.1145/3572751.3572755

Becker, Leo (2025): Standort-Daten bei Apple: Worauf Sie achten sollten, bevor Sie Apps eine Standortfreigabe erteilen. Der Spiegel. 1.7.2025.

Beirat Digitalstrategie Deutschland (2023): Ist das Ökosystem für Mobilitätsdaten schon auf dem Weg? Available online at https://digitalstrategie-deutschland.de/oekosystem-mobilitaetsdaten, last accessed on 10.07.2025.

Beskorovajnov, Wasilij; Eilebrecht, Sarai; Jiang, Yufan; Mueller-Quade, Jörn (2025): A Formal Treatment of Homomorphic Encryption Based Outsourced Computation in the Universal Composability Framework. https://eprint.iacr.org/2025/109

Bindle, Abhay; Gulati, Tarun; Kumar, Neeraj (2022): Exploring the alternatives to the conventional interference mitigation schemes for 5G wireless cellular communication network. In: International Journal of Communication Systems Wiley, 35 (4). https://doi.org/10.1002/dac.5059

Borges, Georg; Stiftung Datenschutz (ed.) (2021): Potenziale von Künstlicher Intelligenz mit Blick auf das Datenschutzrecht - Gutachten. Leipzig. Available online at https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Gutachten-Studien/Stiftung-Datenschutz_Gutachten-Georg-Borges-Potenziale-Kuenstliche-Intelligenz-Datenschutzrecht-2021-12.pdf, last accessed on 23.07.2025.

Bubola, Emma (2021): Venice, Overwhelmed by Tourists, Tries Tracking Them. The New York Times. 04.10.2021.

Caltrider, Jen; Rykov, Misha; MacDonald, Zoë (2023): What Data Does My Car Collect About Me and Where Does It Go? Mozilla Foundation. Available online at https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/, last accessed on 27.11.2024.

Chandler, Colin (2003): CDMA 2000 and CDMA 450. Available online at https://www.itu.int/ITU-D/tech/events/2003/slovenia2003/Presentations/Day%203/3.3.1_Chandler.pdf, last accessed on 09.07.2025.

Chitturi, Anusha; Puentes, Robert (2023): Data for Environmentally Sustainable and Inclusive Urban Mobility. Heinrich-Böll-Stiftung. Available online at https://www.boell.de/sites/default/files/2023-06/e-paper-data-for-environmentally-sustainable-and-inclusive-urban-mobility-endfassung_1.pdf.

Cilento, Carlo (2024): Does Google sell your data? Available online at https://www.simpleanalytics.com/blog/does-google-sell-your-data, last accessed on 27.11.2024.

Cox, Joseph (2021): "Privacy Protecting" Car Location Data Seemingly Shows Where People Live, Work, and Go. VICE. Available online at https://www.vice.com/en/article/car-location-data-not-anonymous-otonomo/, last accessed on 27.11.2024.

Cyphers, Bennett (2022): How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now. Electronic Frontier Foundation. Available online at https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now, last accessed on 10.07.2025.

Cyphers, Bennett; Gebhart, Gennie (2019): Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance. Electronic Frontier Foundation. Available online at https://www.eff.org/wp/behind-the-one-way-mirror, last accessed on 08.04.2025.

Dachwitz, Ingo (2023): Werbetracking: Wie deutsche Firmen am Geschäft mit unseren Daten verdienen. netzpolitik.org. Available online at https://netzpolitik.org/2023/adsquare_theadex_emetriq_werbetracking-wie-deutsche-firmen-am-geschaeft-mit-unseren-daten-verdienen/, last accessed on 10.07.2025.

Darley, James (2025): Top 10: EV Charging Apps. Available online at https://evmagazine.com/top10/top-10-ev-charging-apps, last accessed on 10.07.2025.

Data Spaces Support Centre (2024): Data Spaces' synergies. (Final Report) Munich: c/o Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. Available online at https://dssc.eu/space/DSSE/758350768/Data+Spaces'+Synergies, last accessed on 27.11.2024.

Driftschröer, Anna (2023): Mobility-as-a-Service: Google Maps will die Nummer eins für nachhaltiges Reisen werden. Available online at https://www.manager-magazin.de/unternehmen/autoindustrie/mobility-as-a-service-wie-google-maps-die-nummer-eins-fuer-nachhaltiges-reisen-werden-will-a-20abc14b-986a-4832-a401-66235e3b80b2, last accessed on 27.11.2024.

Dwork, Cynthia (2006): Differential Privacy. In: Michele Bugliesi, Bart Preneel, Vladimiro Sassone and Ingo Wegener (eds.): Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part I. Berlin, Heidelberg: Springer Berlin Heidelberg, (Lecture Notes in Computer Science), pp. 1–12. https://doi.org/10.1007/11787006_1

Elmimouni, Houda; Shusas, Erica; Skeba, Patrick; Baumer, Eric P.S.; Forte, Andrea (2023): What Makes a Technology Privacy Enhancing? Laypersons' and Experts' Descriptions, Uses, and Perceptions of Privacy Enhancing Technologies. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 13972 LNCS , pp. 229–250. https://doi.org/10.1007/978-3-031-28032-0_20

ETA (2024): ETA-Position zum Datentreuhänder. Berlin: Expertenkreis Transformation der Automobilwirtschaft (ETA). Available online at https://expertenkreis-automobilwirtschaft.de/home/veroeffentlichungen, last accessed on 27.11.2024.

Eurelectric (2024): Data interoperability: an essential for the e-mobility ecosystem. Available online at https://evision.eurelectric.org/report-2024/, last accessed on 10.07.2025.

European Data Protection Board (2025): Guidelines 01/2025 on Pseudonymisation.

Francis, Paul (2018): Can Anonymized Data Still be Useful? Part Deux. Aircloak. Available online at https://aircloak.com/can-anonymized-data-still-be-useful-part-deux/, last accessed on 09.07.2024.

Gadotti, Andrea; Rocher, Luc; Houssiau, Florimond; Creţu, Ana-Maria; De Montjoye, Yves-Alexandre (2024): Anonymization: The imperfect science of using data while preserving privacy. In: Science Advances 10 (29), eadn7053. https://doi.org/10.1126/sciadv.adn7053

Gatzert, Nadine; Knorre, Susanne; Müller-Peters, Horst; Wagner, Fred; Jost, Theresa (2023): Big Data in der Mobilität: Akteure, Geschäftsmodelle und Nutzenpotenziale für die Welt von morgen. Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-40511-3

Gebhart, Gennie (2022): Bad Data "For Good": How Data Brokers Try to Hide Behind Academic Research. Electronic Frontier Foundation. Available online at https://www.eff.org/deeplinks/2022/08/bad-data-good-how-data-brokers-try-hide-academic-research, last accessed on 10.07.2025.

Gentry, Craig (2009): A fully homomorphic encryption scheme. (Dissertation) Stanford University.

Goodin, Dan (2021): Android sends 20x more data to Google than iOS sends to Apple, study says. Ars Technica. Available online at https://arstechnica.com/gadgets/2021/03/android-sends-20x-more-data-to-google-than-ios-sends-to-apple-study-says/, last accessed on 27.11.2024.

Hafiz, Munawar (2013): A pattern language for developing privacy enhancing technologies. In: Software: Practice and Experience 43 (7), pp. 769–787. https://doi.org/10.1002/spe.1131

Hill, Kashmir (2024): Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies. The New York Times. 11.3.2024.

Hoseinzadeh, Nima; Liu, Yuandong; Han, Lee D.; Brakewood, Candace; Mohammadnazar, Amin (2020): Quality of location-based crowdsourced speed data on surface streets: A case study of Waze and Bluetooth speed data in Sevierville, TN. In: Computers, Environment and Urban Systems 83, 101518. https://doi.org/10.1016/j.compenvurbsys.2020.101518

Hsu, Chiawei; Fan, Chao; Mostafavi, Ali (2021): Limitations of gravity models in predicting fine-scale spatial-temporal urban mobility networks. arXiv. https://doi.org/10.48550/arXiv.2109.03873

Ilic, Mario; Margreiter, Martin; Álvarez-Ossorio, Martinez; Pechinger, M.; Bogenberger, K. (2023): Roadside LiDAR sensors for data privacy conform VRU detection. In: 10th International Symposium on Transportation Data & Modelling (ISTDM2023): Ispra, 19 22 June 2023 : booklet of abstracts. Ispra: Publications Office, pp. 337–340.

Kapp, Alexandra (2022): Collection, usage and privacy of mobility data in the enterprise and public administrations. In: Proceedings on Privacy Enhancing Technologies 2022 (4), pp. 440–456. https://doi.org/10.56553/popets-2022-0117

Kapp, Alexandra; Mihaljević, Helena (2023): Reconsidering utility: unveiling the limitations of synthetic mobility data generation algorithms in real-life scenarios. SIGSPATIAL '23: 31st ACM International Conference on Advances in Geographic Information Systems. Hamburg Germany, November 13, 2023. https://doi.org/10.1145/3589132.3625661

Kargupta, H.; Datta, S.; Wang, Q.; Sivakumar, Krishnamoorthy (2003): On the privacy preserving properties of random data perturbation techniques. Third IEEE International Conference on Data Mining. November 2003. https://doi.org/10.1109/ICDM.2003.1250908

Keegan, Jon; Eastwood, Joel (2023): From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You – The Markup. Available online at https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you, last accessed on 08.04.2025.

Keegan, Jon; Ng, Alfred (2022): Who Is Collecting Data from Your Car? – The Markup. Available online at https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car, last accessed on 10.07.2025.

Kneis, Lukas et al. (2023): Anonymität und Mobilität - Whitepaper zum Begriffs- und Domänenverständnis des Kompetenzcluster ANYMOS – Anonymisierung für vernetzte Mobilitätssysteme. Karlsruher Institut für Technologie (KIT). https://doi.org/10.5445/IR/1000161584

Leith, Douglas J. (2021): Mobile Handset Privacy: Measuring the Data iOS and Android Send to Apple and Google. In: Joaquin Garcia-Alfaro, Shujun Li, Radha Poovendran, Hervé Debar and Moti Yung (eds.): Security and Privacy in Communication Networks. Cham: Springer International Publishing, (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), pp. 231–251. https://doi.org/10.1007/978-3-030-90022-9_12

Li, Ninghui; Li, Tiancheng; Venkatasubramanian, Suresh; Labs, T (2007): t-Closeness: Privacy Beyond k-Anonymity and -Diversity. Istanbul, Turkey, April 15, 2007. https://doi.org/10.1109/ICDE.2007.367856

Lober, Yannick (2023): Which use cases can be realised with Connected Car Data in 2023? Available online at https://www.high-mobility.com/blog/which-use-cases-can-be-realised-with-connected-car-data-in-2023-opendevtalk9, last accessed on 10.07.2025.

Machanavajjhala, Ashwin; Kifer, Daniel; Gehrke, Johannes; Venkitasubramaniam, Muthuramakrishnan (2007): l-Diversity: Privacy beyond k-anonymity. In: ACM Transactions on Knowledge Discovery from Data 1 (1), 3. https://doi.org/10.1145/1217299.1217302

Metzger, Frederik M.; Krauss, Konstantin (2024): Clarifying new urban mobility services based on a threefold business model framework. In: Transportation Research Interdisciplinary Perspectives 27, 101207. https://doi.org/10.1016/j.trip.2024.101207

Mizzi, Chiara (2022): Big data analytics and modeling for Human Mobility. (Dissertation) Bologna, Italy: Università di Bologna.

Mobility Data Space (2024): Optimising fleet utilisation through data exchange. Available online at https://mobility-dataspace.eu/fileadmin/05_presse_medien/Pressemitteilungen_EN/2024-02-06_MDS_FuhrparkMobility_EN.pdf, last accessed on 27.11.2024.

de Montjoye, Yves-Alexandre; Hidalgo, César A.; Verleysen, Michel; Blondel, Vincent D. (2013): Unique in the Crowd: The privacy bounds of human mobility. In: Scientific Reports Nature Publishing Group, 3 (1), 1376. https://doi.org/10.1038/srep01376

Müller-Eie, Daniela; Kosmidis, Ioannis (2023): Sustainable mobility in smart cities: a document study of mobility initiatives of mid-sized Nordic smart cities. In: European Transport Research Review 15 (1), 36. https://doi.org/10.1186/s12544-023-00610-4

Mulligan, Dominic P.; Petri, Gustavo; Spinale, Nick; Stockwell, Gareth; Vincent, Hugo J. M. (2021): Confidential Computing—a brave new world. 2021 International Symposium on Secure and Private Execution Environment Design (SEED). September 2021. https://doi.org/10.1109/SEED51797.2021.00025

Ovide, Shira (2021): The Nightmare of Our Snooping Phones. The New York Times. 21.7.2021.

Paxton, Ken (2025): Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies | Office of the Attorney General. Available online at https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45, last accessed on 10.07.2025.

Radermecker, Victor; Vanhaverbeke, Lieselot (2023): Estimation of Public Charging Demand Using Cellphone Data and Points of Interest-Based Segmentation. In: World Electric Vehicle Journal 14 (2), 35. https://doi.org/10.3390/wevj14020035

Ramasastry, Anita (2015): Too Much Sharing in the Sharing Economy? Uber's Use of Our Passenger Data Highlights the Perils of Data Collection via Geolocation. Available online at https://verdict.justia.com/2015/02/10/much-sharing-sharing-economy, last accessed on 08.04.2025.

Sabt, Mohamed; Achemlal, Mohammed; Bouabdallah, Abdelmadjid (2015): Trusted Execution Environment: What It is, and What It is Not. 2015 IEEE Trustcom/BigDataSE/ISPA. August 2015. https://doi.org/10.1109/Trustcom.2015.357

Sampaio, Silvio; Sousa, Patricia R.; Martins, Cristina; Ferreira, Ana; Antunes, Luís; Cruz-Correia, Ricardo (2023): Collecting, Processing and Secondary Using Personal and (Pseudo)Anonymized Data in Smart Cities. In: Applied Sciences 13 (6), 3830. https://doi.org/10.3390/app13063830

Sanchez, Catalina (2024): Car Makers Shouldn't Be Selling Our Driving History to Data Brokers and Insurance Companies. Electronic Frontier Foundation. Available online at https://www.eff.org/deeplinks/2024/06/car-makers-shouldnt-be-selling-our-driving-history-data-brokers-and-insurance, last accessed on 10.07.2025.

Specht-Riemenschneider, Louisa; Kerber, Wolfgang (2022): Designing Data Trustees – A Purpose-Based Approach. Datentreuhänder – Ein problemlösungsorientierter Ansatz. Berlin: Konrad-Adenauer-Stiftung e. V.

Strategiedialog Automobilwirtschaft BW (2024): SDA-Sprint-Mission "Open-Source-Software-Entwicklung in der Au- tomobilwirtschaft" – Aufbau einer FOSS Community in Baden-Württemberg: Vision und Mission der Community. Available online at https://www.e-mobilbw.de/fileadmin/media/e-mobilbw/Publikationen/Broschueren/240708_SDA_FOSS_VIsion.pdf, last accessed on 08.04.2025.

Sweeney, Latanya (2002): k-anonymity: A model for protecting privacy. In: International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems 10 (5), pp. 557–570. https://doi.org/10.1142/S0218488502001648

Urban Institute [ui!] (2021): Smartes Parkraummanagement mit [ui!] OptiPark. [ui!]. Available online at https://www.ui.city/aktuelles/blog-archiv/smartes-parkraummanagement-mit-ui-optipark, last accessed on 10.07.2025.

Wang, Xingmin et al. (2024): Traffic light optimization with low penetration rate vehicle trajectory data. In: Nature Communications 15 (1), 1306. https://doi.org/10.1038/s41467-024-45427-4

Widhalm, Peter; Ponweiser, Wolfgang; Markvica, Karin; Dragaschnig, Melitta (2023): GPS-based analysis of shared e-mobility services. In: Transportation Research Procedia (TRA Lisbon 2022 Conference Proceedings Transport Research Arena (TRA Lisbon 2022),14th-17th November 2022, Lisboa, Portugal), 72 , pp. 3489–3496. https://doi.org/10.1016/j.trpro.2023.11.764

Woods, Lorna (2017): Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places. In: Journal of Information Rights, Policy and Practice 2 (1). https://doi.org/10.21039/irpandp.v2i1.35