Connected Vehicles Data Classification and the Influence of a Sustainable Data Governance for Optimal Utilisation of In-Vehicle Data

Ali Karimi[1], Asma Adnane[1], Iain W. Phillips[1] and Elhadj Benkhelifa[2]
[1]*Department of Computer Science, Loughborough University, Loughborough, U.K.*
[2]*Staffordshire University, Stoke-on-Trent, U.K.*
{*A.Karimi, A.Adnane, I.W.Phillips*}*@lboro.ac.uk, E.Benkhelifa@staffs.ac.uk*

Keywords: Data Governance, Connected Cars, CAV, Security, Privacy.

Abstract: The growth of connected vehicles and their associated services has endowed them with the remarkable ability to rapidly generate vast volumes of data. This proliferation has led to an increasing demand for effective data governance solutions. This paper delves into the exploration of currently available in-vehicle data, meticulously assessing the aspects of data velocity and heterogeneity. By scrutinising these factors, the paper aims to pinpoint and address critical gaps in how to deal with in-vehicle data, ultimately striving to create a seamless platform for managing and harnessing in-vehicle data. This project explores approaches for various connected vehicle communications, including V2V, V2I, and V2X, to define data feeds in the connected vehicle data landscape. The results of the study could influence the design of in-vehicle data governance by providing information on a stronger integrated framework, helping data owners and users make informed decisions about managing their data assets.

1 INTRODUCTION

The Intelligent Transport System (ITS) is most effective when vehicles communicate with other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and other smart entities (V2X), known as connected vehicles (Andraško et al., 2021). Equipped with wireless communication, these vehicles can exchange data with various networks. As connectivity increases, vehicles will coordinate through smart infrastructure, improving traffic management for safety and efficiency. Essential in-vehicle technologies include sensor technologies such as VLC, RADAR, LiDAR, infrared; vision technologies such as cameras, SVS, and HD; and positioning technologies like radar cruise control, RBOD, and GPS (Sadaf et al., 2023).

Connected vehicles use data from short-range communication technologies in the 5.9 GHz bandwidth (Tahir et al., 2022), and long-range technologies like 3G, 4G, or 5G networks. They receive and share data with third parties. Entities like public authorities, OEMs, insurers, and service providers responsible for technology updates, safety, security, road traffic, and infrastructure (Andraško et al., 2021) can access these data with restrictions. Data include safety software updates (Dibaei et al., 2020), maintenance requests, personal data of vehicle owners or drivers (Kerber, 2019), traffic rules, vehicle location, speed limits, road conditions, and collision reports.

The EU Commission has implemented guidelines on personal data protection and cybersecurity starting in February 2019, followed by Standard Contractual Clauses in 2021, to regulate event data recorders in vehicles. These measures prioritise data protection, improve the determination of liability in collisions, and address technological advances.

The EU guidelines on cybersecurity call for Original Equipment Manufacturers (OEMs) to design vehicles using state-of-the-art technologies while ensuring compliance with EU data protection regulations. Vehicles must be equipped with robust protections against automated hacking, incorporating design measures, risk assessments, and processes to mitigate, prevent, and respond to cyber threats (EU, 2023/588). Additionally, manufacturers are required to implement safety-critical updates, such as software patches e.g. UNECE Cybersecurity (UN R155 / R156), to maintain cybersecurity throughout the vehicle's lifetime and ensure ongoing protection against emerging threats.

Motivation: An effective data governance would establish an efficient use of in-vehicle data in terms of data ownership, access control, and business im-

Karimi, A., Adnane, A., Phillips, I. W. and Benkhelifa, E.
Connected Vehicles Data Classification and the Influence of a Sustainable Data Governance for Optimal Utilisation of In-Vehicle Data.
DOI: 10.5220/0013371100003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 2*, pages 643-650
ISBN: 978-989-758-735-1; ISSN: 2184-4356

provement. Since a significant amount of data is exchanged, disseminated and processed by connected vehicles. it is crucial to define the various types of in-vehicle data. By categorisation of in-vehicle data, the design of data governance for connected vehicles would be more effective with the appropriate implementation of its main elements (such as data ownership, data use, data assets, security, privacy and safety).

2 RELATED WORKS

Connected vehicles exchange real-time data on traffic and road conditions with other vehicles and infrastructure. Traditionally, research in this field has focused on communication and network layers, crucial to ensuring secure and reliable data exchange and enabling real-time coordination between vehicles and their surroundings. However, recent advances emphasise the efficient use of data within the connected vehicle ecosystem. The introduction of data ontologies, such as the Connected Traffic Data Ontology (CTDO) and the Vehicle Signal and Attribute Ontology (VSAO), provides structured frameworks for managing and integrating data from connected vehicles. These ontologies enhance interoperability and data use by defining semantic models that establish relationships between data objects. This focus on the data layer is essential for the transition from a communication-based utility to a more data-driven transportation ecosystem.

CTDO, for example, provides a standardised framework for traffic-related data, allowing vehicles from different manufacturers to communicate seamlessly with one another and with traffic systems. Similarly, VSAO standardises the data generated by vehicle sensors and attributes, ensuring that data from various sources can be efficiently integrated and used in the vehicle ecosystem (Klotz et al., 2018). This ontological approach not only improves the functionality of connected vehicles, but also contributes to the development of broader smart city initiatives, where data from connected vehicles can be combined with data from other urban systems to improve traffic management, reduce congestion, and improve overall urban mobility.

Data ontology plays a crucial role in defining the relationships between various data types within the connected vehicle ecosystem, serving as a foundational structure for better data utilisation.When combined with a data governance framework, this structure ensures that data is managed securely and in compliance with privacy regulations and standards, such as GDPR. The framework not only enforces security protocols but also guides how data is shared and accessed, ensuring that it aligns with legal requirements and best practices.

2.1 Interoperability of Data in Connected Vehicles

Due to the high mobility of connected vehicles, along with significant security and privacy concerns, interoperability and system design have become major research areas. It is often assumed that these challenges have been addressed, allowing data within the connected vehicle paradigm to move freely and efficiently across the vehicle infrastructure. Proprietary software components often limit the interoperability between products from different manufacturers, especially in connected vehicles(Lim et al., 2021). A unified data platform processing data from all ecosystem sensors and applications would greatly benefit OEMs, policymakers, and others by enhancing data use and advancing connected vehicle technologies. Recently, advances in cloud technology (Huang et al., 2023) in protocol standards and service availability have improved data interoperability.

2.2 In-Vehicle Data

In-vehicle data covers technical aspects like software updates, maintenance alerts, and more, generated via GPS, sensors, and vision tech. This data ensures vehicle functionality, error correction, and optimisation. Processed data aids road safety, management, and development. Vehicles can receive and process external data (e.g., from RSUs, driver activities) and exchange them with others via V2V, V2I, V2X. Such data is valuable to OEMs, service providers, and companies for personalised services, product improvement, predictive maintenance, and marketing strategies.

Public authorities are also interested in the traffic data captured by connected vehicles (Kerber, 2018) (Sola-Morales et al., 2023). In fact, these data can be used to improve traffic management systems, optimise infrastructure planning, monitor environmental impacts, and enhance public safety initiatives.

Car manufacturers and OEMs currently employ a model in which the captured data is transmitted directly to proprietary servers controlled exclusively by the OEMs (Liu et al., 2020). As a result, OEMs defend the current proposal of extended vehicle concept, where they remain the sole controllers of the data, citing concerns over consumer privacy, security, and safety (Kerber, 2019; Andraško et al., 2021; Monday et al., 2019).

Once data ownership is clearly defined, decisions regarding what data to share and how to share it become considerably less challenging.

3 CLASSIFICATION OF DATA IN CONNECTED VEHICLES

The classification of in-vehicle data is essential to managing its collection, storage, sharing, and protection effectively. Data generated by connected vehicles can be broadly categorised into several types, including personal data (such as driver behavior and preferences), technical data (such as engine performance and diagnostics), environmental data (such as road conditions and weather), and communication data (including vehicle-to-vehicle and vehicle-to-infrastructure exchanges). Understanding these classifications is crucial for developing a robust data governance framework that addresses key concerns such as privacy, security, compliance with regulations, and data ownership.

The first layer of classification in connected vehicle data processing involves the identification of data subjects. Data subjects are defined as individuals or entities whose data is processed, as outlined in GDPR regulations. Typical data subjects in the context of connected vehicles include drivers, vehicle owners, passengers, service users, and subscribers to connected vehicle services.

Data originated from connected vehicles can be identified in four main groups as follows:

C1- Technical Data. refers to information related to the vehicle as a product, encompassing various elements that ensure the vehicle's operation, maintenance, and overall quality. This includes data on specific vehicle components, such as software versions, hardware specifications, and serial numbers of key parts such as engines, sensors, and control units. It also covers diagnostic data, including error codes generated by vehicle on-board systems, performance metrics (e.g. fuel efficiency, battery status in electric vehicles) and emissions data (Uhlemann, 2015).

C2- Infotainment Data. Refers to individuals whose personal data is handled in the connected vehicle ecosystem, including drivers, vehicle owners, passengers, or service users. This includes a broad spectrum of personal and behavioural data, such as driving patterns (e.g., speed, braking, route choices) and data provided by the individual through activities such as entertainment preferences or mobile device connections to the vehicle infotainment system (Yu and Cai, 2022). It also covers financial and contractual details such as warranties, service agreements, insurance, invoices, and payments.

C3- Environment Data. Consists of information from the vehicle's external environment, which includes metrics such as external temperature, humidity levels, road surface conditions, weather patterns (e.g., rain, snow, fog), and real-time traffic conditions. It also includes data on the presence of obstacles, nearby vehicles, and infrastructure-related details such as traffic signals, signage, and road layout. This type of data is critical for improving situational awareness and enabling advanced driver assistance systems (ADAS) and autonomous driving technologies.

C4- Telematic Data. Telematic data refers to information related to vehicle performance, operational conditions, and real-time status. This category includes data generated by various sensors and systems that monitor vehicle activity and communicate with external systems, often through satellite or cellular networks. Telematic data can include critical performance metrics such as fuel efficiency, vehicle speed, and geographic location (GPS data) (Kumar et al., 2023) (Sadaf et al., 2023). Telematic data play a critical role in the functionality, user experience, and data governance of connected vehicles.

3.1 Illustration of In-Vehicle Data

The list below outlines the data classification framework for connected vehicles by identifying data types within each category. This approach clearly visualises data classes, showing how data are generated, used, and managed. Data categorisation supports a robust governance model that defines data ownership, sharing protocols, and usage. This structure clarifies roles and permissions, improves safety, security, and efficiency in connected vehicle systems.

A- Data Related to Connected Vehicles: These types of data provide details on vehicle components, data related to vehicle quality and maintenance, Vehicle identification:

- Vehicle Identification Number (VIN), which consists of: Registration number, connected vehicle type, model year, component identification number (ID), technical specifications.

- Vehicle Configuration including: type of engine, type of gearbox, hardware and software versions, Electronic Control Unit (ECU) parameters
- Network and Communication: Ip address, Media Access Control (MAC) address of connected vehicle, WiFi password, Bluetooth name of vehicle

B- Data Related to the Data Subjects: such as owner, driver, passenger, subscriber, service user, and data directly provided by the data subject (such as mobile phone, music, etc.).

- Navigation and information: Phone address book and call history, navigation destination, radio preferences, music, movies, pictures, etc.
- Personal attributes: Biometry data captured inside the vehicle
- Dynamic data include: Gear, engine Revolutions Per Minutes (RPM), average fuel consumption, automatic braking, lane departure warning. acceleration, speed, mileage, AdBlue level
- Data from vehicle setting and control: Privacy settings, status of windows and doors, lights on/off, air condition,
- Accounting, warranty and Service subscription: Purchase or leasing invoices, after sale and service invoices.

C- Data Related to Other Subjects Outside of the Connected Vehicles: Data regarding external environment of the vehicle and data from other data subjects: External temperature, video and images captured from outside environment.

In summary, all the above data types represent five distinct yet complementary categories within the connected vehicle ecosystem. Each of these types of data plays a crucial role in advancing the functionality of connected vehicles, but all raise important considerations regarding data governance, security, and privacy.

4 IN-VEHICLE DATA ACCESS

An important part of the current controversial policy discussion is about the control and access of data captured by connected vehicles or data in vehicles (Kerber, 2019). Car manufacturers or Original Equipment Manufacturers (OEMs) use a concept to transmit captured data directly to a server (Liu et al., 2020) (Song et al., 2021), which is proprietary to the OEMs (extended vehicle concept). The aim of introducing this concept by OEMs is to have exclusive control over in-vehicle data with the argument of preserving data security and privacy. However, stakeholders and many independent service providers also demand access to in-vehicle data with the argument of ensuring fair and undistorted competition to provide maintenance and after-sales services to connected vehicles (Kerber, 2019) (Tahir et al., 2022).

In a short-term solution, a shared platform might be a solution to allow all parties to access in-vehicle data on demand. In the long term, the development of a technological solution such as an on-board application platform allows the vehicle owner to control access to the vehicle or to the in-vehicle data. Some key considerations regarding in-vehicle data access and sharing within the context of connected vehicles are as follows:

4.1 Privacy and Security

In-vehicle data frequently contains sensitive and personally identifiable information (PII) related to the driver, passengers, vehicle performance, and its surrounding environment (Majid, 2023). These data include, but are not limited to, driving patterns, location history, biometric data, and real-time telemetry, all of which can be vulnerable to security breaches or unauthorised access if not properly protected.(Figure 1).

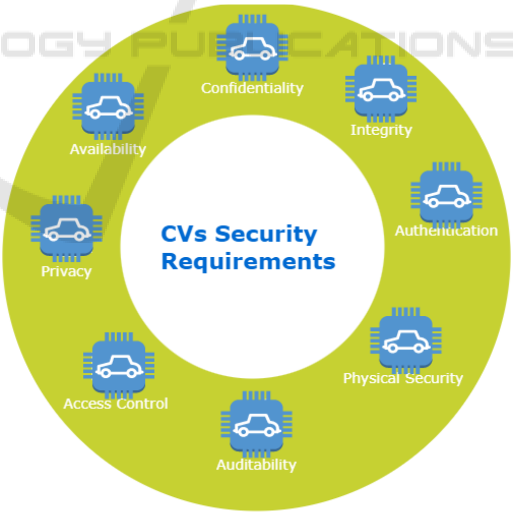

Figure 1: Requirements for CVs data privacy and security.

To safeguard these sensitive data, a multilayered approach to security must be adopted, incorporating measures such as end-to-end encryption, Access controls, anonymisation and pseudonymisation techniques are essential to protects data in transit and to protect the privacy of individuals by ensuring that personal data cannot be directly linked to a specific person particularly when shared with third-parties.

4.2 Data Ownership

The question of who should control or have access to in-vehicle data remains a contentious issue among vehicle manufacturers, OEMs, leasing companies, insurers, and service and maintenance providers (Kerber, 2018). Although the European Union (EU) is actively working to regulate in-vehicle data ownership, the process faces significant challenges. OEMs and connected vehicle manufacturers are resisting specific regulations, citing concerns related to consumer safety, data privacy, and security (Andraško et al., 2021). The European Automobile Manufacturers Association (ACEA) has affirmed that the EU automotive industry is committed to providing access to in-vehicle data, but emphasises that uncontrolled access to such data could pose major risks in terms of security, data protection, safety and privacy (Monday et al., 2019).

Data insights can optimise predictive maintenance and usage-based insurance pricing, cutting costs, and enhancing service quality. However, ensuring access requires strict security, privacy and data governance to prevent data misuse, balancing accessibility and protection (Schellekens, 2022) (Khan et al., 2023). Clear data ownership is crucial for governance, simplifying decisions on data sharing. The next section outlines key principles for sharing in-vehicle data.

4.3 Data Sharing

Connected vehicle manufacturers may already be heading down a familiar path of controlling data (Xu and Guo, 2022). Such control over in-vehicle data could lead to an anticompetitive market and a concentration of power, resulting in monopolistic practices. The European Commission is currently in the process of defining the scope of its Data Act to ensure fairness in digital environments, promote opportunities for data-driven innovation , stimulate a competitive data market and make data more accessible to all (Sola-Morales et al., 2023).

If OEMs allowed third-party access to in-vehicle data, several fundamental principles must be considered (Figure 2.

The following lists explain the importance of data sharing principles in connected vehicles and why these elements should be considered for sharing in-vehicle data.

- In-vehicle data: Before introducing regulations on data sharing and making in-vehicle data available for third-party services, it is essential to ensure the protection of driver personal data, ensuring the secure and safe operation of the vehicle, not undermining the liability of the vehicle manufacturer, and avoiding damage to intellectual property rights of the vehicle.

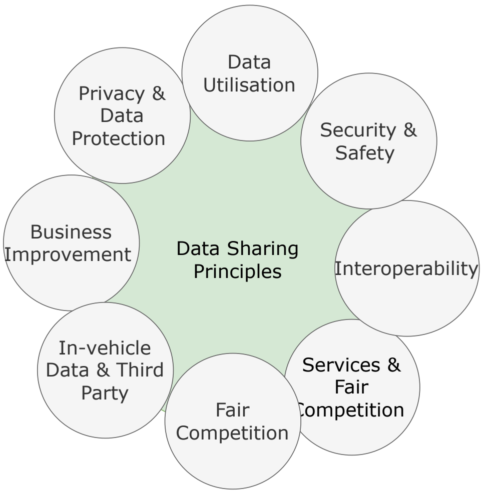

Figure 2: Principles of Sharing In-vehicle Data.

- Maintenance option and fair competition: Drivers and vehicle users can obtain services from different garages that have concluded an agreement with OEMs, the vehicle manufacturer, or its network of authorised maintenance providers and independent aftermarket organisations.
- Data protection and privacy: In accordance with EU data protection and privacy law and GDPR personal data must be protected and not to be shared without the consent of the owners.
- Security and safety: Third-party access to vehicular electronic devices may jeopardise safety, integrity, and security of the vehicle. Thus, any access outside of the regulated access to in-vehicle data such as repair, maintenance, emissions control, and diagnosis data access must occur via an off-board process.
- Interoperability: For third-party and independent service providers to access in-vehicle data, mean of access and the interfaces must be standardised to ensure interoperability. The International Organisation for Standardisation (ISO) developed for this purpose to provide web access to the Extended Vehicle (ExVe) as defined in ISO 20077-1 (ExVe consists of a vehicle with external hardware and software extensions that are developed, implemented and managed by the ExVe manufacturer).
- Business improvement: The vehicle manufacturer

and the OEM invest significant amounts of funds and resources to develop and introduce the final product to the intended market. In addition, maintaining, managing, and keeping the available data is also a costly process, which could add to the initial production costs. It is a clear mission for every business to expect Return on Investment (RoI).

Connected vehicles produce extensive data in various categories. However, not all of this data is shared with third parties or service providers. Specifically, shared data excludes personally identifiable information (PII) related to the vehicle driver, such as contact lists from mobile devices, destination and trip histories, and other sensitive personal data. Furthermore, data received from RSUs, infrastructure, V2V communications, or other road users may also be restricted from being shared with external parties.

4.4 Data Access Control

OEMs and third-party service providers may require access to in-vehicle data for various purposes, such as vehicle diagnostics, maintenance, and personalised services. Clear agreements and guidelines should be established to govern data access and specify the scope and purpose for which the data will be used. This helps ensure that data sharing is conducted in a fair and transparent manner.

Even if ownership is attributed to a specific entity, the discussions revolve around who has access and control over the data. Data governance frameworks should address access rights, data sharing agreements, and mechanisms to obtain consent from drivers for specific uses of their data.

4.5 Legal and Regulatory Considerations

Data access and sharing in connected vehicles are governed by various legal and regulatory frameworks, which differ between regions and encompass data protection laws, privacy regulations, and industry-specific guidelines. For example, in the European Union, the General Data Protection Regulation (GDPR) imposes strict requirements on how personal data, including in-vehicle data, are processed, stored, and shared. GDPR mandates clear consent from data subjects and the application of privacy-by-design principles to ensure that data handling practices prioritise security and privacy. Similarly, the California Consumer Privacy Act (CCPA) in the United States provides a regulatory framework for data privacy, giving consumers greater control over their personal information and requiring businesses to disclose how they collect and share data (Shatz and Lysobey, 2022).

In addition, cross-border data sharing in the context of connected vehicles also introduces complexities, as differing regulatory requirements between regions can create challenges (Miller, 2022). For example, the EU-U.S. Privacy Shield, although invalidated in 2020, highlighted the need for robust data transfer mechanisms between regions with different privacy standards. Current frameworks like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) are now employed to facilitate cross-border data flows while ensuring compliance with stringent data protection standards. Given the global nature of the automotive industry, manufacturers and stakeholders must navigate a landscape of evolving regulations.

5 THE IMPORTANCE OF DATA CLASSIFICATION

Figure 3 illustrates the data interconnection within the connected vehicle ecosystem. All these processes, including data generation, processing, and sharing, occur within the vehicle's network, managed by the central processing unit (CPU) and data controller unit, as represented by the circle surrounding data classification and data types. This signifies that manufacturers or data controllers have direct access to all categories of in-vehicle data, such as technical, telematics, infotainment, and environmental data. Given this comprehensive access, it is imperative to implement a robust data governance scheme specifically designed for in-vehicle data.

This approach is critical in mitigating the risks of data security breaches, safeguarding data privacy, and preventing cyberattacks.

6 DISCUSSION AND CONCLUSION

The discussion of in-vehicle data in connected vehicles highlights the critical role of data ontology in defining the relationships between various data types and their interactions within the vehicle ecosystem.

Connected vehicle data classification systems categorise data into groups such as telematics, information technology, technical, and environmental. This organisation clarifies data handling, sharing, and protection, primarily addressing data governance, ownership, privacy, and security. It helps in creating data

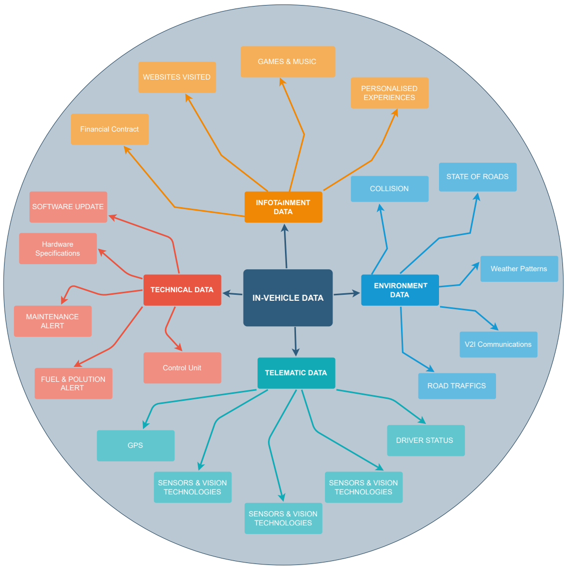

Figure 3: Connection of data classification in connected vehicles.

sharing methods that balance privacy, innovation, and safety.

Moreover, connected vehicles have revolutionised mobility and data-driven transportation. Their success depends on effective data governance. This involves not only data quality and security, but also compliance with regulations and responsible data handling to build trust. The diverse types of data require a structured governance approach to gain insight, improve safety, and improve efficiency. Furthermore, the monetisation of data presents a significant opportunity, and data governance is key to balancing data utilisation for economic purposes with the preservation of individual privacy.

7 FUTURE WORK AND RECOMMENDATION

Future work focuses on the development of a comprehensive data governance framework that enables relevant organisations to effectively utilise in-vehicle data while addressing critical elements of cybersecurity and privacy. Additionally, it is recommended to introduce a model designed to assess an organisation's current data governance capabilities, accompanied by a structured approach for identifying areas of improvement and implementing targeted enhancements.

REFERENCES

Andraško, J., Hamuľák, O., Mesarčík, M., Kerikmäe, T., and Kajander, A. (2021). Sustainable data governance for cooperative, connected and automated mobility in the European Union. *Sustainability (Switzerland)*, 13(19).

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., and Yu, S. (2020). Attacks and defences on intelligent connected vehicles: a survey. *Digital Communications and Networks*, 6(4):399–421.

Huang, J., Wan, J., Lv, B., Ye, Q., and Chen, Y. (2023). Joint computation offloading and resource allocation for edge-cloud collaboration in internet of vehicles via deep reinforcement learning. *IEEE Systems Journal*.

Kerber, W. (2018). Data Governance in Connected Cars The Problem of Access to In-Vehicle Data. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law (jipitec)*, 9(2016):310–331.

Kerber, W. (2019). Data sharing in iot ecosystems and competition law: the example of connected cars. *Journal of Competition Law & Economics*, 15(4):381–426.

Khan, R., Mehmood, A., Iqbal, Z., Maple, C., and Epiphaniou, G. (2023). Security and privacy in connected vehicle cyber physical system using zero knowledge succinct non interactive argument of knowledge over blockchain. *Applied Sciences*, 13(3):1959.

Klotz, B., Troncy, R., Wilms, D., and Bonnet, C. (2018). VSSo-A vehicle signal and attribute ontology (Short paper). *CEUR Workshop Proceedings*, 2213(October):56–63.

Kumar, V., Zhu, D., and Dadam, S. R. (2023). Connected vehicle data–prognostics and monetization opportunity. Technical report, SAE Technical Paper.

Lim, K. L., Whitehead, J., Jia, D., and Zheng, Z. (2021). State of data platforms for connected vehicles and infrastructures. *Communications in Transportation Research*, 1(September):100013.

Liu, X., Sun, S. X., and Huang, G. (2020). Decentralized Services Computing Paradigm for Blockchain-Based Data Governance: Programmability, Interoperability, and Intelligence. *IEEE Transactions on Services Computing*, 13(2):343–355.

Majid, A. (2023). Security and privacy concerns over iot devices attacks in smart cities (2022). *Journal of Computer and Communications*, 11(1):26–42.

Miller, L. (2022). Public sector integration of connected and automated vehicles: Considerations, benefits and sharing data across borders. In *Automated Road Transportation Symposium*, pages 40–50. Springer.

Monday, H. N., Ukwuoma, C. C., Li, J. P., Agomuo, D., Nneji, G. U., and Nneji, R. I. (2019). Ensuring Data Governace and Enhancing Data Security in a Private Cloud Environment. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018*, pages 1018–1024.

Sadaf, M., Iqbal, Z., Javed, A. R., Saba, I., Krichen, M., Majeed, S., and Raza, A. (2023). Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. *Technologies*, 11(5):117.

Schellekens, M. (2022). Data from connected cars for the public cause. *Computer Law & Security Review*, 45:105671.

Shatz, S. P. and Lysobey, P. J. (2022). Update on the california consumer privacy act and other states' actions. *Bus. LAw.*, 77:539–540.

Sola-Morales, O., Sigurdhardottir, K., Akehurst, R., Murphy, L. A., Mestre-Ferrandiz, J., Cunningham, D., and de Pouvourville, G. (2023). Data governance for real-world data management: a proposal for a checklist to support decision making. *Value in Health*, 26(4):32–42.

Song, X., Guo, Y., Li, N., and Zhang, L. (2021). Online traffic flow prediction for edge computing-enhanced autonomous and connected vehicles. *IEEE Transactions on Vehicular Technology*, 70(3):2101–2111.

Tahir, M. N., Leviakangas, P., and Katz, M. (2022). Connected vehicles: V2v and v2i road weather and traffic communication using cellular technologies. *Sensors*, 22(3):1142.

Uhlemann, E. (2015). Introducing connected vehicles [connected vehicles]. *IEEE vehicular technology magazine*, 10(1):23–31.

Xu, Y. and Guo, G. (2022). Event triggered control of connected vehicles under multiple cyber attacks. *Information Sciences*, 582:778–796.

Yu, Z. and Cai, K. (2022). Perceived risks toward in-vehicle infotainment data services on intelligent connected vehicles. *Systems*, 10(5):162.