A Comparative Perspective of Data Regulation Frameworks and their Implications for Connected Vehicles

L. Barrera Cano*
Imperial College London
(UK)

S. Raza*
Imperial College London
(UK)

B. Sekibo*
Imperial College London
(UK)

A. Siafaras*
Imperial College London
(UK)

Q. Wolf*
Imperial College London
(UK)

Z. Yin*
Imperial College London
(UK)

W. Xu
Imperial College London
(UK)

D. Tuncer
Ecole des Ponts ParisTech
(France)

ABSTRACT

The public authority in different parts of the world has started to implement a set of legal frameworks for controlling what one can do with data. In this paper we review the data regulation principles that are essential to support the adoption of connected vehicles and associated applications such as navigation and fleet management. We conduct a comparative analysis of the data protection and privacy legal frameworks currently in place in California, in the EU and in China, which represent key markets for the deployment of connected mobility services. We identify the challenges for the use and processing of personal data in this context and discuss the foundation of these legal frameworks towards providing a high level of data protection and privacy.

CCS CONCEPTS

• General and reference → Surveys and overviews; **• Security and privacy → Privacy protections**; **• Applied computing → Law**.

KEYWORDS

data regulations, data sharing practises, connected and automated vehicles

ACM Reference Format:
L. Barrera Cano, S. Raza, B. Sekibo, A. Siafaras, Q. Wolf, Z. Yin, W. Xu, and D. Tuncer. 2022. A Comparative Perspective of Data Regulation Frameworks and their Implications for Connected Vehicles. In *ACM SIGCOMM 2022 Joint Workshops on (TAURIN+BGI '22), August 22, 2022, Amsterdam, Netherlands.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3538395.3545313

1 INTRODUCTION

The progressive development of vehicles with increasing degrees of automation, *i.e.,* that are capable of performing partial to complete driving tasks autonomously [1], has shown that the future of mobility will strongly rely on connected vehicles. Connected vehicles are expected to be a major contributor to machine-to-machine communication in the coming years, with applications such as fleet management, in-vehicle infotainment or vehicle diagnostics and navigation forming the fastest-growing category of Internet of Thing traffic [2]. In a connected mobility scenario, connected vehicles participate in the exchange of information through a network of connected devices and sensors. The shared information is used to orchestrate mobility, from realizing autonomous driving tasks to monitoring the road environment and managing traffic in real-time [3]. Connected vehicles are expected to generate a substantial amount of data (from 1.4 to 19 TB per hour [4]), collected from a wide range of sources (*e.g.,* cameras, GPS), and stored and exchanged between devices at different timescales (*e.g.,* hourly operational logs *vs.* images stored on vehicle SSD [5]), using different technologies (*e.g.,* cellular, wi-fi) and with different levels of granularity (*e.g.,* real-time vehicle position *vs.* media settings) [6].

The shift towards digitized societies in this first quarter of the XXIst century has led the public authority in different parts of the world to start implementing a set of legal frameworks for controlling what one can do with the data produced through digitalized, connected infrastructures. The European Union was the first to establish regulatory bases for the protection of personal data in 2016 in the form of the General Data Protection Regulation (GDPR) framework [7]. The advent of connected vehicles, and more generally connected mobility services, raises questions with respect to the implications that their deployment poses in terms of data protection [8] and compliance of these technologies with the implemented frameworks.

In this paper we review these implications from the perspective of the data regulation frameworks that are currently in place in three main regions: the General Data Protection Regulation (GDPR) that applies to European countries, the California Consumers Privacy Act (CCPA) as the first law in the US, and the Personal Information Protection Law (PIPL) concerning the People's Republic of China.

[*] The first six authors contributed equally to the paper as part of a group work.

TAURIN+BGI '22, August 22, 2022, Amsterdam, Netherlands
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9394-2/22/08…$15.00
https://doi.org/10.1145/3538395.3545313

Table 1: Connected vehicle data overview.

Data category	Information type	Enabled-functionality
GPS and SatNav	Location	Navigation
Camera	Environment	Navigation
Touch sensor	Driving activity	Driving assistance and safety
Security status	Vehicle access	Vehicle security
Battery status	Charging behavior	Charge management
Energy provider	Pay scheme	Billing
Vehicle registration	Ownership	Billing
Media and communication	Driver profile	Accessibility

We compare the characteristics of each framework from the perspective of its application principles, its definition of liability, and the scope of responsibility that they entail. Based on the identified characteristics and differences, we highlight the key challenges that need to be addressed in terms of data protection and privacy for connected vehicles, and discuss possible technological solutions that have been proposed to comply with the requirements of legal frameworks.

The rest of the paper is organized as follows. Sect. 2 provides background information on connected vehicles. Sect. 3 presents the three legal frameworks considered in this work and reviews their characteristics. Sect. 4 discusses data regulation principles for connected vehicles and possible technological solutions. Finally, some concluding remarks are reported in Sect. 5.

2 CONNECTED VEHICLES

In a connected vehicle, data is collected from a variety of sensors (*e.g.,* cameras, GPS, radars, sonars, IMU, *etc.*) and on-board devices. The collected data is used to support different tasks. These tasks can be performed directly within the vehicle, *i.e.,* to control and maintain its operations. The data can also be shared externally to support tasks that are executed remotely, based on cloud services for instance [9]. Connected vehicles can communicate in real-time with the connected road infrastructure or with other vehicles using vehicle-to-everything-type of communication protocols [10]. Real-time communication (and the associated data exchange) can be used to identify dangerous situations or detect changing traffic conditions for instance. The exchange of data can also take place offline, when the vehicle is parked, to update vehicle configurations (*e.g.,* driving software and infotainment system updates).

2.1 Connected Vehicle Data

Table 1 presents main categories of data collected by connected vehicles. It also indicates the type of information that the processing of the relevant data can provide and the functionality it enables. In general the collected data can be used to support a variety of functionality, from navigation functions to driving assistance and safety monitoring, as well as energy (charge) management or automatic billing.

Data includes both technical data that is produced by the vehicle's on-board system and sensors, as well as data originating from the vehicle's occupants (the driver and passengers) such as the destinations for navigation, entertainment choices (through the vehicle infotainment) and social communications (telephone contact lists, online shopping preferences, *etc.*) [11], which constitutes forms of personal data. Information provided through the data can either be directly inferred from the read parameters on a sensor (*e.g.,* the battery level informs the need for charging) or can result from the combination of different data sources (*e.g.,* the driving activity is determined by processing speed profiles, journey's history and driver's behavior). Depending on their type, the obtained information can be considered as sensitive.

2.2 Data Stakeholders

The ecosystem of connected vehicles covers an heterogeneous set of stakeholders that ranges from vehicle and equipment manufacturers, automotive suppliers, car dealerships, fleet managers to car insurance companies, telecommunication operators and entertainment providers. It also includes road infrastructure and transport operators, as well as public authorities. Stakeholders can play different roles with respect to how the data produced by and within a connected vehicle is managed and used. In particular, a stakeholder can be the entity that determines the purpose and means of data processing, the entity that performs the processing, or the recipient of the processed data (as a third party for instance). The role also depends on the specific set of data.

In this ecosystem, owner/driver/passengers of connected vehicles constitute central data subjects [12] whose personal data (as individuals) is processed by stakeholders with different requirements and interests. The definition of this personal data, the liability that stakeholders have with respect to this data, and the rights guaranteeing how the data is used and handled necessitate the implementation of regulatory guidelines and foundations that protect data subjects. In the rest of this paper, we review three existing data regulation frameworks and their application to connected vehicles.

3 DATA REGULATION FRAMEWORKS

We focus on comparatively reviewing the specifics of the legal data protection frameworks that have been implemented in three principal economic regions in the world, namely the General Data Protection Regulation (GDPR) framework [7] in the European Union, the California Consumer Privacy Act (CCPA) [13] in California (US), and the Personal Information Protection Law (PIPL) [14] in the People's Republic of China.

3.1 Overview

The GDPR was established in 2016 as the world's forerunner initiative in personal data protection regulation. It covers the European Economic Area (EEA), including Sweden, Italy, France, and especially Germany, the hubs of the world's leading automotive companies. The CCPA was established in 2020 mainly as a response to the Cambridge Analytical scandal in 2018. The federal legislator in the United States does not regulate data privacy and only gives recommendations in the form of a Code of Conduct, which leaves the individual state regulator in charge. California, the economically most powerful and populated state in the US, that has been a hub to many big data processing companies, established with the CCPA the first major data protection regulation in the US. Two new laws around data privacy were created in China, the most populated country and the second largest economy in the world: the Data Security Law (DSL) [15] and the PIPL. Both came into effect in 2021. In contrast to the other frameworks, the DSL mainly regulates storage and transmission of data in a broad sense but offers poor coverage of data subjects' rights.

The main features of each framework are presented in Table 2[1]. These are grouped into eight main categories that represent *i)* data protection principles, *ii)* sanctions against protection infringement, *iii)* rights for data subjects, *iv)* duties upon data subjects, *v)* scope of personal data, *vi)* liable entities, *vii)* response time for data access, as well as *viii)* special features.

3.2 Comparative observations

The three frameworks protect data subjects by offering similar rights to protect personal data such as the right to request information regarding the processing of one's data, the right to erase or rectify one's data, and the right to transfer one's data to another party (data portability). While the PILP is very similar to the GDPR (it builds on the European framework), it gives stricter fines in case of infringements (up to 5% of the annual revenue compared to 4% maximum under the GDPR) [16]. In addition, the PIPL imposes the disgorgement of illegal gains [16]. The fines can also be converted into penalties under the Chinese national social credit system. Only the CCPA has a limit on the amount of the fine of 7,500$ per case but requires the compensation of victims (750$ per victim per case) (Art 1798.155) [13].

Both the GDPR and the PIPL provide a holistic structure in terms of rights and principles (*e.g.,* purpose and data minimization, transparency, integrity and confidentiality, *etc.*) (Art 5 [7]; Art 5&7 [14]). In contrast the CCPA mainly focuses on transparency principles and does not define specific regulations for the processing of data. For instance, the prohibition of sensitive information processing (*e.g.,* health, ethnicity, sexuality, religion, *etc.*) (Art 9 [7]; Art 28&29 [14]) does not appear in the CCPA framework, only discrimination is explicitly prohibited. In addition, the CCPA adopts an "opt-out" system regarding the selling of data to third parties (Art 1798.135 [13]), whereas the GDPR and the PIPL are based on an "opt-in" system where the data subjects explicit their consent for a specific data processing.

All data types, including technical data, are considered as personal data under the CCPA [17]. In the GDPR and the PIPL, technical data is only considered as personal if it enables a person to be identified (Art 4 [7]; Art 4 [14]). Liability is however more narrowly defined in the CCPA given that only for-profit businesses meeting certain criteria can be responsible for data breaches or unlawful processing (Art 1798.140 [13]). In contrast, any organization, government, business, or individual can be made accountable for how they process the data under the GDPR and the PIPL (Art 4 [7]; Art 73 [14]).

Regarding the geographical coverage of the frameworks, the CCPA covers data subjects in the state of California only, while the GDPR and the PIPL cover all data processing at the European and national level, respectively. In addition, entities need a legal basis for processing data in the GDPR and the PIPL, while this is not specified in the CCPA.

Finally, while cybersecurity obligations using technical and organizational measures (*e.g.,* encryption) are implicated in the CCPA, they are not as explicit as in the GDPR or the PIPL ("privacy by design and default") (Art 25 [7]; Art 6 [14]). The GDPR and the PIPL also require data risk impact assessment to be carried prior to data processing (Art 35 [7]; Art 51 [14]).

4 DATA REGULATION PRINCIPLES FOR CONNECTED VEHICLES

The application of regulatory principles regarding the use of data is crucial to the deployment of connected mobility services. Between the frameworks presented in Section 3, only the GDPR and the PIPL provide some specific guidelines for connected vehicles [18–20]. In this section, we discuss in more detail the needs for data regulation applied to connected vehicles by focusing on key principles for *i)* lawfulness, fairness and transparency, *ii)* right to access, erasure and rectification, *iii)* sensitive information, *iv)* liability in a multi-stakeholder ecosystem and *v)* right to data security.

4.1 Lawfulness, fairness & transparency

Both the GDPR and the CCPA require the data collected to be processed under their legal and technical requirements, which applies to all the stakeholders involved in the chain of data processing. In particular, Original Equipment Manufacturers (OEMs) have the responsibility to inform the owners of a vehicle of data collection requirements (from and within the vehicle) and obtain their consent and permissions. As such, the collection purposes need to be explained and agreed upon by contract or consent *e.g.,* [21]. In practice, drivers (and / or passengers) may not always be *adequately* informed about the processing of data that takes place in or through the vehicle. This can happen, for instance, if the information is only provided to the owner of the vehicle (and not to the driver/passenger). This can also happen when the provision of consent is not achieved on time[2][22].

4.2 Access, erasure, and rectification rights

Users of connected vehicles need to be provided with access guarantees to their personal information. In addition, users (including drivers and passengers) have the right to delete and correct data. While these guarantees are in line with the principles applied by the GDPR and the PIPL, they cover only erasure support in the case of the CCPA. In practice, the multi-stakeholder nature of connected mobility use cases, where miscellaneous service terms can

[1] As of June 2022, 1 US dollar amounts to 6.69 Chinese RMB and 0.95 Euro.

[2] It should be noted that a scenario where data consent is provided to the driver in real-time via a digital interface would be distracting and would go against satisfying user experience [23].

Table 2: GDPR, CCPA and PIPL comparison.

Areas of Interest	**Data Regulation Framework**		
	GDPR	***CCPA***	***PIPL & DSL***
Jurisdiction	EEA	State of California in the U.S.	The People's Republic of China
Implementation Year	2016	2020	2021
Infringement Sanctions	Up to 4% of annual revenue	2500$ to 7500$ fine + 100$ - 750$ compensation for a victim per case	RMB 50 million, up to 5% of annual revenue and disgorgement of all illegal gains (PIPL)
Principles	Purpose and data minimization	Protect consumers through transparency of data use	Similar to GDPR
	Transparency		Data, national and individual security (DSL)
	Integrity and confidentiality		Promote data development and utilization
Rights for Data Subjects	Right to erasure or restrict	Right to erasure	Right to get informed and decide about processing of personal data
	Prohibited processing of sensitive data	Right to get information	Right to restrict or refuse processing
	Right of access	Right to Opt-out	Right to access and copy from data processor
	Right to rectification	Right to complain & to sue	Right to correct or supplement personal data
	Explicit consent	Right of equality	Right to erase
	Right to data portability	Right to data portability	Right to get informed about processing rules
	Right to object (sue)		
	Right not to be subject to automated processing		
Duties upon Data Subjects	Privacy by design and default	Obligation to fulfil information right	Consent Requirements
	Cybersecurity	Provide Opt-out button ("Do not sell my personal Information" – button)	Data Localization and Data Deletion Requirements
	Data breach notification to supervisory authority and data subject	Special contracts with data processing providers	Restrictions on transfer of personal information to third parties and overseas
		No discrimination	General compliance requirements
Personal data scope	All data that can be used to identify a person (but doesn't necessarily include technical data about devices)	All data that can be used to identify a person (includes technical data about devices)	Various information recorded electronically or otherwise relating to an identified or identifiable natural person, excluding anonymized information
Liable entities	Any individual, public body or business of any size based, offering goods in the EU or monitoring behaviour of EU people	Only for-profit businesses (trash holds)	Organizations (including governments) and individuals who independently decide the purpose and method of processing and using personal data
Request response time	Within a month	Within 45 days	"In time" used but not specified
Special Features	Requires risk impact assessment and a legal basis for data collection and use	Businesses must provide Opt-out button ("Do not sell my personal Information")	Separated in two laws focusing on "data" and "personal" info respectively + National cybersecurity and information department responsible for planning, management of data protection work

be defined based on the obligations set by laws [12], makes the implementation of access, erasure, and rectification rights not straightforward. While a digital interface inside the connected vehicle can provide a mean for the driver and the passengers to exert their rights, it still needs to be configured in such a way that it covers all data. More specifically, this necessitates the availability of an effective method for delivering data usage instructions, as well as the support of a liability framework, which is missing today.

4.3 Sensitive information

Some of the data collected by connected vehicles qualify as sensitive information. This is in particular the case of biometric data (*e.g.,* fingerprints to obtain vehicle access) or driver's setting profile [24]. For instance, while the processing of these categories of data is prohibited under the GDPR and the PIPL, it is unprotected under the CCPA. Sensitive information can also be obtained indirectly, by being derived from the collected data. Religious beliefs or sexuality information can, for instance, be inferred from location data (*e.g.,* going to a specific place of worship) or from the usage of streaming/browsing services via the vehicle infotainment.

While some strategies can be followed to protect such data such as using gyroscope or employing limited and temporal storage, it may not always be effective. For instance even when deactivating the GPS, it is still possible to track one's mobility by using driving speeds, distance travelled and/or home location [25]. In addition, this also raises questions regarding the collection of criminal offense data such as speed limits or red lights violations [24]. While this type of data is protected under the GDPR and the PIPL by authorizing its processing only by official authorities (Art 10 [7]; Art 34-37 [14]), it is not protected under the CCPA and could in practice be used by private entities.

4.4 Liable Entities

As shown in Table 2, the three frameworks define liable entities with different requirements. In the context of connected vehicles, vehicle manufacturers constitute a key liable entity, as they provide information such as the type of stored data, the storage location, the storage duration, and the means to ensure security, data protection, and access to the data [11]. Given the wide range of stakeholders involved in the connected vehicle ecosystem [12], to define responsible entities as one homogeneous group is challenging. An illustrative example is the case of road traffic accident prevention using vehicle-to-vehicle communication. Data subjects cannot be identified here and the GDPR, for instance, cannot be applied [11]. Joint *controllership*, which is highly relevant to the connected mobility scenario, constitutes a challenging issue and is currently only covered by the GDPR (Art. 26 [7]). More specifically, under the GDPR, every controller would be held liable in case of damage cause in the context of a road traffic accident prevention system based on vehicle-to-vehicle communication.

4.5 Right to Data Security

As any connected devices, connected vehicles constitute vectors for cyberattacks. These can target in particular personal data that is stored and handled in the vehicle, *e.g.,* social network messages, travel plans, login credentials to bank accounts, *etc.* [26]. Cybersecurity obligations are essential to protect user data. Today organizational measures such as encryption is implicated in the CCPA but is not as explicit as in the GDPR and the PIPL.

A number of initiatives in the recent years have been investigating the use of blockchains for building privacy-preserving solutions for managing vehicle's data *e.g.,* [27–29]. These solutions take advantage of the decentralized, multi-party trust relationship nature of blockchain to enable data protection. To Aggregate or to mask data, to use trusted third parties to collect and to store the data, to have users agree on being tracked, or to strictly follow privacy legislation aid secure data collection. In the view of state authorities, however, public safety and security may supersede individual or carrier's right to privacy [30].

4.6 Discussion

The challenges associated with data protection are likely to be exacerbated as vehicles reach higher degrees of automation. Automated vehicles (AVs) require real-time access to both internal and external data to operate. Through enhanced data supply and improved vehicle-to-everything communications, AVs are able to "make" better decisions, given that their ability to select the most beneficial behavior is improved as more information becomes available.

Frameworks embedding ethical principles are essential to lift the ambivalence that exists between, on one hand, the "promise" of improved road safety through driving task automation [32] and on the other, the requirements for stricter data protection guarantees. In that regards, data regulation frameworks appear as crucial tools to control the use and processing of AV-related data. In particular, these frameworks need to be pivotal to the handling of key ethical issues in this domain, such as for instance the ones associated with the implementation of a life-death decision-making logic for driverless vehicles [33].

In practice, the requirements of data regulation frameworks not only call for the application of relevant data handling techniques such as privacy-preserving mechanisms (*e.g.,* differential privacy, federated learning). They also call for the implementation of principled approaches to the development of these technologies, *e.g.,* the *privacy-by-design* principles [35], that embed data handling and protection from the conception phase as an integral component of the design of the system. To make ethics the central piece of the implementation and use of connected and automated vehicles among all relevant stakeholders (*i.e.,* legislator, manufacturers, operators, and the public) is determining to the development of a technology that *effectively* works towards the common good [31].

5 CONCLUSIONS

The digitalization of the mobility domain comes with key issues in terms of data privacy and security. Intelligent transportation systems and their associated applications (*e.g.,* photo enforcement, GPS tracking, electronic tolling, *etc.*) necessitate the development of data management solutions that on one hand supports the development of enhanced services for users (such as eco-friendly route planning [34] or driving assistance) and on the other, offers the right level of personal data protection. Limited regulation exists for these applications, which requires a revision of data frameworks.

In this paper, we review the three main data regulation frameworks currently enforced in the European Union, California, and China, and analyze their characteristics with respect to connected vehicle use cases. We show that sensitive information collected (or derived) on connected vehicles is only protected under the GDPR and the PIPL frameworks. We also show that in terms of liability, the GDPR and the PIPL provide unambiguous information by stating privacy-by-design and requiring that technical and organizational measures are in place. In contrast, the CCPA does not explicitly specify that aspect.

In future work, we will focus on the specific case of data handling in mobile applications for route planning in connected vehicles and investigate their functionality with respect to the data regulation principles discussed this paper. Another direction is to investigate how the current privacy-preserving technologies comply with the three frameworks for vehicle data applications and the potential implications of linked datasets under different regulations (such as vehicle and energy data, *e.g.,* [36]).

REFERENCES

[1] R. Coppola, and M. Morisio, "Connected car: technologies, issues, future trends," *ACM Computing Surveys*, vol. 49, no. 3, pp. 1-36, 2016.

[2] Cisco Annual Internet Report (2018–2023), White Paper, 2020. [Online]. Available: https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/. Accessed 10-05-2022.

[3] J.Locke, "What Is Connected Vehicle Technology and What Are the Use Cases?," *Digi International*, 17 June 2020. [Online]. Available: https://www.digi.com/blog/post/what-is-connected-vehicle-technology-and-use-cases.. Accessed 10-05-2022.

[4] S. Wright, "Autonomous cars will generate more than 300 TB of data per year," 2021. [Online]. Available: https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/. Accessed 10-05-2022.

[5] B. Yu, W. Hu, L. Xu, J. Tang, S. Liu and Y. Zhu, "Building the Computing System for Autonomous Micromobility Vehicles: Design Constraints and Architectural Optimizations," in proc. *53rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pp. 1067-1081, 2020.

[6] J. Obstfeld, "Connected Car – The Driven Hour," *Cisco - Whitepaper Edition*, 2019. [Online]. Available: https://blogs.cisco.com/sp/connectedcar-thedrivenhour-wp. Accessed 10-05-2022.

[7] General Data Protection Regulation. [Online]. Available: https://gdpr-info.eu/. Accessed 10-05-2022.

[8] Ryan D. Junck, *et al.*, "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies," *Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates*, 2021. [Online]. Available: https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws. Accessed 10-05-2022.

[9] P. Arthurs, et al., "A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[10] S. Chen, et al., "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G," in *IEEE Communications Standards Magazine*, vol. 1, no. 2, pp. 70-76, 2017.

[11] J. Andraško, O. Hamuľák, M. Mesarčík, T. Kerikmäe, and A. Kajander, "Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union," *Sustainability*, vol. 13, no. 19, pp. 10610, 2021.

[12] European Data Protection Board, "Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications," version 2.0, 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-12020-processing-personal-data_en. Accessed 10-05-2022.

[13] California Consumer Privacy Act. [Online]. Available: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article. Accessed 10-05-2022.

[14] Xinhua, "Personal Information Protection Law of the People's Republic of China," www.gov.cn, Aug. 20, 2021. Available: http://www.gov.cn/xinwen/2021-08/20/content_5632486.htm. Accessed 10-05-2022.

[15] Xinhua, "Data Security Law of the People's Republic of China," www.gov.cn, Jun. 11, 2021. Available: http://www.gov.cn/xinwen/2021-06/11/content_5616919.htm. Accessed 10-05-2022.

[16] X. Ke, V. Liu, Y. Luo, Z. Y, "Analyzing China's PIPL and how it compares to the EU's GDPR," *The International Association of Privacy Professionals - News*, Aug. 2021. [Online]. Available: https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/. Accessed 10-05-2022.

[17] activeMind AG, "Das California Consumer Privacy Act (CCPA) für EU-Unternehmen," May 2020. [Online; in German], Available: https://www.activemind.de/magazin/ccpa/. Accessed 10-05-2022.

[18] China Cyber Security Administration of the Ministry of Industry and Information Technology, "Five departments jointly issued 'Several Regulations on Automobile Data Security Management (Trial)'," Cnii.com.cn, Aug. 20, 2021. [Online]. Available: https://www.cnii.com.cn/zcjd/202108/t20210820_303015.html. Accessed 10-05-2022.

[19] China Ministry of Industry and Information Technology, "Opinions of the Ministry of Industry and Information Technology on Strengthening the Access Management of Intelligent and Connected Vehicle Manufacturers and Products," www.gov.cn, Jul. 30, 2021. [Online]. Available: http://www.gov.cn/zhengce/zhengceku/2021-08/12/content_5630912.htm. Accessed 10-05-2022.

[20] European Commission, Mobility and Transport, "Cooperative, connected and automated mobility (CCAM)." Available: https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/cooperative-connected-and-automated-mobility-ccam_en. Accessed 10-05-2022.

[21] J. J. Asiag, "Vehicle Data Sharing - Secure and Easy: Otonomo's Consent Management Hub," *otonomo blog post*, April 2021. [Online]. Available: https://otonomo.io/blog/consent-management-for-vehicles/. Accessed 10-05-2022.

[22] F. Vallet, "The GDPR and Its Application in Connected Vehicles—Compliance and Good Practices," in *Electronic Components and Systems for Automotive Applications*, Springer, Cham, pp. 245-245, 2019.

[23] R. H. Thaler and C. R. Sunstein, "Nudge: Improving decisions about health, wealth, and happiness," in *London: Penguin Books*, 2008.

[24] D. Skalli, "Connected vehicles and the GDPR, what data needs your special attention." [Online]. Available: https://www.dpoconsultancy.com/artikel/connected-vehicles-and-the-gdpr-what-data-needs-your-special-attention/. Access 10-05-2022.

[25] V. Kaplun, and M. Segal, "Breaching the privacy of connected vehicles network," in *Telecommunication Systems*, vol. 70, no. 4, pp. 541-555, 2019.

[26] X. Zheng, L. Pan, H. Chen, and P. Wang, "Investigating security vulnerabilities in modern vehicle systems," in proc. of *International Conference on Applications and Techniques in Information Security*, pp. 29-40, 2016.

[27] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," in *IEEE Network*, vol. 32, no. 3, pp. 78-83, 2018.

[28] M. Cebe, et al., "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles," in *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50-57, 2018.

[29] C. Kaiser, et al., "Towards a Privacy-Preserving Way of Vehicle Data Sharing – A Case for Blockchain Technology?," in *Dubbert, J., Müller, B., Meyer, G. (eds) Advanced Microsystems for Automotive Applications*, Lecture Notes in Mobility, Springer, Cham, 2018

[30] R. N. Fries, et al., "Meeting privacy challenges while advancing intelligent transportation systems," in *Transportation Research Part C: Emerging Technologies*, vol. 25, pp. 34-45, 2012.

[31] P. Lin, "Why ethics matters for autonomous cars," in *Autonomous driving*, Springer, Berlin, Heidelberg, chap. 4, pp. 81-97, 2016.

[32] Editorial, "Safe driving cars," Nature Machine Intelligence, Nature, Feb. 2022. https://doi.org/10.1038/s42256-022-00456-w

[33] Moral Machine, Available: https://www.moralmachine.net/. Accessed 10-05-2022.

[34] O. Dukkanci, Ö. Karsu, B. Y. Kara, "Planning sustainable routes: Economic, environmental and welfare concerns," in *European Journal of Operational Research*, vol. 301, no. 1, pp. 110-123, 2022.

[35] S. Barth, D. Ionita, and P. Hartel, "Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines," in *ACM Computing Surveys (CSUR)*, vol. 55, no. 3, pp. 1-37.

[36] F. Teng et al., "Balancing privacy and access to smart meter data," Energy Futures Lab briefing paper, Imperial College London, UK, 2022.