Autonomous Vehicles: Data Protection and Ethical Considerations

Ioannis Krontiris
Kalliroi Grammenou
Kalliopi Terzidou
Marina Zacharopoulou
Homo Digitalis
Athens, Greece

Marina Tsikintikou
Foteini Baladima
Chrysi Sakellari
Konstantinos Kaouras
Homo Digitalis
Athens, Greece

ABSTRACT

Autonomous vehicles (AVs) are increasingly becoming part of the emerging Intelligent Transportation Systems (ITS) and they are positioned to advance smart mobility. To enable this, new on-board sensors collect and transmit growing types and quantities of data. This raises new and unique privacy considerations around what happens with this data. As the automotive industry becomes more data-driven, getting consumer privacy rights will become increasingly important for establishing trust and customer acceptance of this technology. At the same time, the algorithmic decision making in AVs raises several new ethical issues that can create new safety risks and discriminatory outcomes. In this paper we analyze what are the new privacy and data protection challenges that emerge in AVs and investigate the ethical and liability concerns surrounding algorithmic decision-making, highlighting research gaps and the need to mitigate these issues by acting swiftly.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; **Social aspects of security and privacy**; *Pseudonymity, anonymity and untraceability*.

KEYWORDS

autonomous driving, connected car, data protection, privacy

ACM Reference Format:
Ioannis Krontiris, Kalliroi Grammenou, Kalliopi Terzidou, Marina Zacharopoulou, Marina Tsikintikou, Foteini Baladima, Chrysi Sakellari, and Konstantinos Kaouras. 2020. Autonomous Vehicles: Data Protection and Ethical Considerations. In *Computer Science in Cars Symposium (CSCS '20), December 2, 2020, Feldkirchen, Germany*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3385958.3430481

CSCS '20, December 2, 2020, Feldkirchen, Germany

ACM ISBN 978-1-4503-7621-1/20/06…$15.00
https://doi.org/10.1145/3385958.3430481

1 INTRODUCTION

Automated and autonomous vehicles (AVs) may be the greatest disruptive innovation to travel that we have experienced in a century. AVs promise highly increased traffic safety and fuel efficiency, better use of the infrastructure, the liberation of drivers to perform other tasks. For these reasons, autonomous driving may create a paradigm shift in the way people and goods are transported.

There are two technological advancements that come together and pave the way for the successful implementation of autonomous driving. First, it is connectivity and communication technology – V2V as well as V2X communication. V2X communication enables two key features in AVs: cooperative sensing, which increases the sensing range by means of the mutual exchange of sensed data, and cooperative maneuvering, which enables a group of AVs to drive according to a common decision-making strategy [Hobert et al. 2015]. This connectivity between vehicles and between vehicles and transport infrastructure enables the cooperation between these elements and is expected to significantly improve road safety, traffic efficiency and comfort of driving, by helping the driver to take the right decisions and adapt to the traffic situation [European Commission 2020].

The second technological advancement that enables AVs is Artificial Intelligence. AVs are formally defined as those in which at least some aspects of safety-critical driving control occur without direct driver input. To achieve their goal, AVs require extensive data and machine learning algorithms processing this data for decision-making. Specifically, we are seeing the emergence of vehicles that feature an impressive array of sensors and on-board decision-making units capable of coping with an unprecedented amount of data. According to reports, sensors on AVs will generate data roughly between 1.4 TB/h and 19 TB/h [Heinrich 2017].

Both of these technological advancements underlying AV technology pose new challenges on privacy protection in AVs, given the ubiquitous nature of capturing data in public and the ability to scale without additional infrastructure. Another aspect that complicates things even further is the fact that AVs capture data not only from users, but also from non-users (i.e. pedestrians walking outside the vehicle) with very limited possibilities to offer notice and choice about data practices.

Privacy becomes particularly important since it is the baseline for trust into a system, it is a requirement for customer acceptance of a technology and, consequently, it is a key market enabler. A recent survey on the public opinion on automated driving reveals

that there are worries on safety and privacy aspects of AVs [Kyriakidis et al. 2015]. Bloom et al. [Bloom et al. 2017] also investigated people's conceptions of the sensing and analysis capabilities of AVs and found that scenarios such as tracking and identification caused overwhelming discomfort to people.

As AV technology is still in its infancy, security, trust and privacy aspects are not well addressed [Lu et al. 2014]. Discussions on how to manage privacy risks from the legal perspective have only begun recently. The EU and governments in most countries have developed new regulations to control the access to, use and sharing of personal data, but these are not specific to AVs [Taeihagh and Lim 2019]. As Greenblatt argues in his recent article [Greenblatt 2020], the law is not prepared for the emergence of AVs and is lagging behind. The situation regarding legal protections for pedestrians and other traffic participants against the capture and use of images taken by AVs is – at best – unclear, and the discussion regarding processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) is still ongoing [Data Protection and Privacy Working Group of the C-ITS Platform 2017]. This uncertainty persists over the available technologies and burdens their adoption from the automotive industry.

Secondly, it becomes more clear that we need to design algorithms with ethical considerations to ensure that AVs make ethical driving decisions [Liu 2018]. This is quite challenging, given than ethical approaches are quite subjective and diverse. However, as we argue in this paper, the solution could be found in the field of technology. A connected open problem is that of the liability, meaning which agent is going to be liable in the case of a car crash and to which extent. The lack of specific legal framework on AVs in most countries raises many issues on liability allocation and calls for a harmonized and consistent approach.

Contributions: In this paper we bring forward what we see as open issues and challenges in the privacy and data protection domain of AVs that need to be taken into consideration at an early stage, before deployment outpaces understanding of potential ramifications. We argue that the special characteristics of autonomous driving create an environment where current solutions fall short and we highlight new directions that can help overcome these challenges. The first part of the paper focuses on the technology, related to the new types of data collected and the corresponding data flows created around this data. In the second part, we emphasize on the algorithmic decision-making in AVs and we discuss how both the ethical and liability issues in AVs can undermine public well-being and social equity and become obstacles to real "smartness" and sustainability.

2 DATA AND ACTORS DEFINED

First it is important to understand what kind of personal data are collected by AVs. To do this, we first need to look at the sensors that such vehicles are equipped with. Typical sensors include GPS for navigation, cameras located in the front, rear, left and right side of the car, and a multitude of ranging sensors like RADAR and light detection and ranging (LiDAR) for generating a 3D map of the environment. Data fusion integrates all this sensor data into an environmental model of a vehicle's surroundings that also includes detection of object types to distinguish, for example, between cars, pedestrians, bikers and solid obstacles.

In addition, AVs also collect data from their surrounding vehicles, since all vehicles broadcast their speed, location and direction data as part of the V2X communication. V2X safety messages can include a Cooperative Awareness Messages (CAM), a Decentralized Environmental Notification Messages (DENM) or a Basic Safety Message (BSM). The CAM and DENM can be used in European (EU) standards [ETSI 2017] and the BSM in United States (US) standards. CAM messages are broadcasted quasi-continuously (at 1-10 Hz) and they contain kinematic data, as well as the dimensions of the vehicle. DENM messages are broadcasted in addition to the CAM messages, but only upon the occurrence of specific events (like accidents) for urgent situations, and they contain geolocation information about the event. The BSM can be both a periodic broadcast and triggered by events. For the sake of simplicity, in what follows we will restrict ourselves only to the European standard messages (CAM and DENM), but the same holds for BSM as well.

Even though CAM and DENM messages do not contain any unique identifier, the Data Protection and Privacy Working Group of the Cooperative Intelligent Transport Systems has issued an analysis, which makes it explicit that these messages are personal data [Data Protection and Privacy Working Group of the C-ITS Platform 2017]. This is because the data subject may be indirectly identifiable through the location data contained in the messages. The EU Commission [European Commission 2016] and the Art. 29 WP [Article 29 Data Protection Working Party 2017] also make it clear that data broadcast by vehicles qualifies as personal data.

In order to make the difference between current vehicle technologies and AVs more clear and set the basis of analysing the privacy challenges in the rest of the paper, we first take a look at what kind of personal data are collected by AVs and categorize them based on how they are collected and disseminated in the system.

Data about vehicle and its passengers, for example:

- data on the drivers and passengers like name, address, account information, but also in-vehicle video and biometric data for the authentication of the driver (e.g., voice-, fingerprint-, video-and other types of authentication) or his monitoring (e.g., image processing for fatigue detection),
- data on personal devices of drivers and passengers like MAC addresses,
- trip information like start and end of trips,
- vehicle location data,
- vehicle identification number,
- vehicle related data (model code, registration date, country of registration).

Data about vehicle-external entities, for example:

- license plates of surrounding vehicles,
- video recordings including identifying information like faces of pedestrians, bikers, etc.,
- sensor data from LIDAR, RADAR, etc. involving other persons,
- data received from other vehicles (location, etc.)

Table 1: Data related to autonomous vehicles.

Kind of data	Example how data is handled
Sensor data (sensors, radars, Lidar)	High-bandwidth sensor data for object avoidance and mapping, and infrared thermal imaging. Data acquired and processed on-board. Under some conditions part of the data may be send off-board for training the machine learning system.
Video Recording (exterior)	Capture high-bandwidth images of vehicles and parties external to the vehicle. Identify external parties and number-plates of other vehicles. Data acquired and processed on-board. Under some conditions part of the data may be sent off-board for training the machine learning system.
Video Recording (interior)	Monitor driver alertness and occupant behaviour. Data acquired on-board and can stay there.
Biometric, biological or health data	Monitor driver alertness and behavior. Recognise drivers and occupants through fingerprints or facial recognition
Crash-related data	Input data from the vehicle in the seconds before and during the crash stored in Event data recorder. Data collected and processed by the vehicle.
V2X Communication data	Data from CAM and DENM messages broadcast in C-ITS containing location information. Data broadcast to surrounding vehicles and infrastructure.

This multitude of data to be considered from a data protection perspective makes it challenging to effectively assess a C-ITS system in a data protection impact assessment. It can be helpful to classify data first and one way to do that is based on the way it can be accessed, for example whether it is broadcast to all or transferred to a private network or just stored somewhere and it can be accessed from there. The International Working Group on Data Protection in Telecommunications has suggested the following categories [International Working Group on Data Protection in Telecommunications 2018]:

- Data collected and processed by the vehicle, including information and entertainment systems built into the vehicle.
- Data exchanged between the vehicle and personal devices connected to it,
- Data exchanged between the vehicle and external entities (e.g., infrastructure managers, vehicle manufacturers, insurance companies, car repairers).
- Data broadcast to surrounding vehicles and infrastructure entities to enable C-ITS.

Another way to categorize data is to look at the source of the data, as proposed in Table 1.

When it comes to actors involved, we first have the data controller, who determines the means and purpose of data processing which takes place in AVs. This term could contain for example car manufacturers (OEMs), insurance companies offering "Pay As You Drive" contracts, or service providers that process personal data to be sent to the driver, such as eco-driving or traffic information or changes in car functionality.

When the processing is carried out on behalf of another entity as data controller, the party carrying out the processing acts as data processor. Examples of data processors can be distributors during the review of the vehicle condition through effective remote monitoring, auto repair shops, technology groups such as IT-Firms which develop the software and the apps for navigation, telematic services, or mobile network operator (MNOs).

As far as the data subject is concerned, it has the right according to GDPR to be informed about the data collected, processed and of course for what purpose. This term could contain the car owner, the driver, which is not always the car owner, the co-driver and other passengers, and pedestrians, which are not always aware of the data processing.

3 PRIVACY AND DATA PROTECTION CONSIDERATIONS

While privacy protection for C-ITS has been investigated for more than a decade and technical solutions have been developed, it appears that autonomous driving will create new challenges or aggravate existing ones. In this section we discuss those emerging privacy challenges and argue that the shortcomings of current practices ought to be adequately addressed by the industry and research community.

3.1 Legal bases for processing personal data

As a general principle, each company processing personal data as a controller needs a legal basis to do so. Article 6(1) GDPR specifies several options that can make processing of personal data lawful. Regarding AVs the legal discussions are still ongoing as to which

of these options apply in which case, since the situation is complex with many different players involved, each having different purposes for the data collected.

The case of legal basis for processing CAM and DENM messages in the context of C-ITS and connected car is perhaps an indicative example. The Data Protection WG of the C-ITS Platform [Data Protection and Privacy Working Group of the C-ITS Platform 2017] has analysed each of the above options for legal basis and it has given comments on the feasibility of each one. Regarding informed consent, it makes it clear that this form of legal basis is simply impossible in practice. The Art. 29 WP [Article 29 Data Protection Working Party 2017] has analysed this further and has given several reasons for the difficulty of implementing consent as legal basis. They mainly have to do with the fact that car owners and car users have to be treated separately and that the broadcasting nature of the communication makes it impossible to set a mutual recognition mechanism between the data subject (sender) and the controller (recipient). The Working Group 29 considers that the preferred solution in the long term for lawfully processing personal data in the context of C-ITS should be carried out in accordance with a legal obligation where processing data is necessary for the performance for a task carried out in the public interest. However, this processing would require the enactment of an EU-legal instrument which is now missing.

More recently, the Guidelines published by the European Data Protection Board (EDPB) communicate the view that consent should generally be the legal basis for the processing of personal data in relation to connected vehicles. The connected vehicles and every device connected to them are considered as a "terminal equipment" in view of the EDPB, hence, the provisions of art 5.3 of the e-Privacy Directive apply and as a rule, prior consent for the "storing of information or the gaining of access to information already stored in the terminal equipment of a user" is necessary [European Data Protection Board 2020]. This interpretation raises various questions on its applicability towards the applications and services in the connected vehicles, and has quite an important impact for the car manufacturing industry. Further guidance is necessary to be provided by the European Authorities, as to which systems and use cases prior informed consent will be a requirement.

As far as biometric data is concerned, it should be noted that these categories of personal data are considered special categories of personal data under Article 9 of the GDPR and their processing is prohibited, unless there is an exemption that allows such processing. Such exemption might be the explicit and freely given consent of the driver and/or occupant. That said, such consent shall be freely given and the provision of the service must not be conditional on consent to the processing of personal data that is not necessary for the provision of the service. In this case, the EDPB has pointed out that when considering the use of biometric data, guaranteeing the data subject full control over his or her data involves providing for the existence of a non-biometric alternative (e.g. using a physical key or a code) without additional constraint (that is, the use of biometrics should not be mandatory) [European Data Protection Board 2020].

Another important case to consider is the video data captured by several cameras attached on an AV. As we said in the previous section, personal data is inevitably captured and recorded in this case, for example people on the street, cyclists or other road users, as well as license plates. Although it is not the intention to identify any of the persons in the video, the data collection may not take place without a legal basis, unless an exemption applies.

In a report from the Bavarian Data Protection Authority it is made clear that the purpose of recording as well as the duration of recording play a decisive role in the compliance to the data protection regulation [Bayerisches Landesamt für Datenschutzaufsicht 2019]. For example, the case of recording of the traffic situation from a dash cam for the purpose of preserving evidence in the event of a traffic accident may be considered compliant to data protection law, given that a balancing test between the interests of the controller and the fundamental rights and freedoms of the data subject needs to be carried out. That means, making sure by technical means that only a short-term event-related recording takes place in connection to the accident and those data are minimised and protected. In addition, information on the camera-based processing taking place should be provided to the data subjects in a concise and transparent manner [Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2018], for example by marking the recording vehicles with a clearly visible sign or sticker and keeping a sheet with detailed information about the data controller, the legal basis of data collection, the purposes of the processing and all information required under Articles 12 and 13 of the GDPR [Irish Data Protection Commission 2018].

However a permanent and continuous recording of the traffic situation with a video camera that takes place without specific and clearly-defined purposes is not permitted under data protection law [Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2019]. Under Article 89 (and Recital 159) of the GDPR, there is an exemption that permits the processing of personal data for scientific research purposes which is even strengthened by some national or state-level regulation. The Bavarian Data Protection Authority has indicated that it considers that the use of dash cams for the purposes of research and development of autonomous vehicles could fall within this exemption [Bayerisches Landesamt für Datenschutzaufsicht 2019] and §13 in the state-level data protection regulation in Baden-Württemberg points in a similar direction [Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2018]. However, it should be noted that there is no broader consensus on a European level at this point.

So there is a need for clear guidance to help controllers and programmers determine on what legal basis for processing to rely on and implement the corresponding solutions. On one side, it is important that these legal issues are clarified as soon as possible so that technological development is not prevented. On the other side, technological development is not a free ticket to through data protection principles overboard, since this would seriously affect citizens' trust in these new technologies.

3.2 Transparent and Interpretable Processing

As emphasized by Art. 29 WP [Article 29 Data Protection Working Party 2017], users need to be fully aware of the scope of the processing of the data they broadcast through their vehicles. Who receives these data (e.g. other vehicles, OEMs, road managers, etc.) and how

they process these data should also be transparent to the data subjects. The Data Protection and Privacy Commissioners also urge the involved parties to give data subjects comprehensive information as to what data is collected and processed in the deployment of connected vehicles, for what purposes and by whom [International Working Group on Data Protection in Telecommunications 2017]. However, there are currently only limited possibilities to interact with the data subject within the vehicle and provide sufficient and appropriate information about the processing of personal data.

Outside the vehicle, a company deploying cameras typically has no direct relationship with the individuals who may pass through the dash cam's field of view, which makes it more challenging to provide those individuals with the required information. The Guidelines suggest the use of a "layered" approach, with the most important information displayed on a highly visible sign (e.g., a sticker on the outside of the vehicle) alerting individuals to the fact that a dash cam is being used, and providing a means of obtaining further information (e.g., using a QR code that individuals can scan with a smartphone, and that links to an online privacy notice setting out the required information).

3.3 Data Minimization and Data Retention

In a world where a vast amount of data is being collected for the vehicle's journey, the principle of data minimization constitutes a challenge. Controllers should only collect personal data relevant, adequate and not excessive with regard to the specific purposes of processing, and the boundaries of these limitations are quite unclear. In-car technology enablers such as sensors are usually powered by machine learning, thus, the collection of a large amount of datasets is unavoidable. In this landscape, industry players have the tendency to collect an enormous amount of data from different sources, far beyond the needs of the provided services. This data can be used in data analytics to create anonymous, aggregated, statistical data as well as to identify the data subjects and apply profiling or targeted marketing activities, raising significant data protection concerns.

From a human input perspective, the experts involved in building and deploying AI systems in cars and other devices are likely to have a wider range of backgrounds than usual, including traditional software engineering, system administration, data science, etc. This entails that security and minimisation practices and expectations may vary significantly, and for some there may be less understanding of broader compliance requirements, as well as those of data protection law more specifically.

This issue emphasizes the significant role of the privacy by design practice, which requires the development of a privacy-centric design prior to the use of a new product or service in the connected vehicle, enforcing the data minimization principle and providing privacy-protective default settings [European Data Protection Board 2020].

Data cannot be stored indefinitely and a specific retention period based on the purposes of processing shall be defined. For instance, the car manufacturer cannot retain for an unlimited period the technical details of the vehicle for the purpose of product improvement, unless they are anonymized [Commission Nationale de l'Informatique et des Libertés (CNIL) 2017]. However, in complex scenarios as is the case with the connected vehicles, the exchange of personal data with other vehicles and the involvement of advanced IT systems, increases the risks for excessive data storage. The ICO guidance [Information Commissioner's Office (ICO) 2020] recommends deleting any intermediate files containing personal data as soon as they are no longer required (e.g. compressed versions of files created to transfer data between systems).

Incidents have been referred to in car sharing services where car users have been able to access personal data of previous users and even exert control over the car functions in a remote manner [Supervisor 2019]. It is crucial therefore for the car manufacturer to ensure that after the fulfilment of a defined purpose and specific service, the data should be deleted or genuinely anonymized within a limited timeline. The EDPB recommends the development of a simple functionality in the vehicle, which will enable the users to delete all personal data from the dashboard in an easy and fast manner [European Data Protection Board 2020].

3.4 Implications of GDPR on AI and Image Recognition

As we saw above, huge amounts of video data are being collected with the goal of creating environmental models to train the intelligent algorithms or to validate complex autonomous driving functionality. Images or videos recorded in public areas may contain personal data such as license plates and people's faces. AVs cannot give all pedestrians and drivers they encounter notice and choice. So another permitted solution to respect privacy rights is to anonymize the recorded data immediately, so that no conclusion about personal information can be drawn.

Early methods have been relying on obfuscation with a solid colored box, pixelization, random pixel shuffling, Gaussian blur and distortion. Schnabel et al. [Schnabel et al. 2019] evaluated several techniques and concluded that anonymization of personal data in the training set can impact the detection of vehicles at various degrees. However one would expect that anonymization would have a different impact on detection performance, depending how important the region we target is for feature learning. For example, perhaps blurring license plates could have a different impact on the performance of a car detector, than the impact of blurring faces on the human detector. More extensive experimental evaluation is definitely needed in this area. Another approach is to replace faces or number plates in the video with generated ones, in order to de-identify subjects in images or videos, while preserving non-identity-related aspects of the data and consequently enabling better data utilisation.

3.5 Explainability of AI

The GDPR mandates a right to explanation, which aims to increase the interpretability and transparency of automated decisions by requiring firms to provide data subjects with "meaningful information about the logic involved" in "concise, intelligible and easily accessible" forms [Goodman and Flaxman 2017]. However, legally it would be very tough to challenge an algorithm embedded in a hardware and explainability may become impossible at this stage. The GDPR does not seem to fully guarantee or grant the right to explanations. There is no specific guarantee to this right in the

articles of the GDPR and the right to explanation only appears in recital 71 which has no binding nature [Wachter et al. 2017a].

The right to explanation stems from article 22 of the GDPR, which introduces the right to object to decision "based solely on automated processing". This entails that in cases of highly automated driving[1] where the driver is capable of taking control of the car, the decision that might lead to an accident (e.g. confusing an object for a human being) is unlikely to be considered as a decision *solely based* on automated processing.

Also, the rights to information provided for in Articles 13 (2) (f), 14 (2) (g) of GDPR introduce an obligation for the data controller to provide, where automated decision-making exists, "meaningful information about the logic involved, as well as the significance and the envisaged consequences for data subjects". However, the fact that the information obligations enshrined in articles 13 and 14 of the GDPR precede the decision-making and that prior to the processing only explanation on the system functionality may be reasonably expected and provided [Wachter et al. 2017b], lead to the conclusion that the right to explanation is not granted by the GDPR and the scope of information to be provided to the data subject is not clearly defined either[2].

Consequently, in the case of a fully automated car, precisely defined accountability mechanisms are not yet available. The ICO guidance on AI suggests that in solely automated contexts, human intervention is only required on a case-by-case basis to safeguard the individual's rights, whereas for a system to qualify as not solely automated, meaningful human intervention is required in every decision [Information Commissioner's Office (ICO) 2020]. In cases of robotics making automated decisions that may have a serious impact on individuals, tools to explain the "logic" and "rationale" of robotic behaviour and decision-making are required but remain undefined [European Parliament 2017].

The intention of GDPR in mandating a right to an explanation for automated decisions is to increase transparency around algorithmic decision-making, in order to tackle bias and discrimination. In the section that follows, we refer to this topic, as part of the overall ethical considerations in AVs.

4 ETHICAL CONSIDERATIONS

The topic of explainable AI needs to be unpacked in relation to both the users for whom the explanations are needed, and the different types of explanations required. We argue that explanation of processing and explanation of representation are of different natures and play different roles. In addition, we argue that trustworthy AI in the context of autonomy is a broader concept than explainable AI. Explanation of processing, which maps inputs to outputs and treats the AI as a black box model, may be considered more relevant for assurance and more explainable by nature than explanation of representation, which treats the AI as a grey or white box model. However, the challenge in assurance is not the interpretability or explainability itself, but rather if the set of explanations combined can suffice as valid, complete and convincing assurance evidence while at the same time they match all the ethical aspects that lay beneath because we have not created a universal moral code yet.

Manufacturers and deployers should develop and implement user-centred methods and interfaces for the explainability of relevant AV applications of algorithm and/or machine learning based operational requirements and decision-making. They should ensure that the methods and vocabulary used to explain the functioning of AV technology are transparent and cognitively accessible, the capabilities and purposes of AV systems are openly communicated, and the outcomes traceable. This should ensure that individuals can obtain factual, intelligible explanations of the decision-making processes and justifications made by these systems, particularly in the event of individually or group-related adverse or unwanted consequences and be able to challenge decisions made by the autonomous system, so as to hold manufacturers accountable.

The fast-growing research area concerning explainable AI (XAI) and Fairness, Accountability and Transparency (FAT) in algorithmic systems should be encouraged by policymakers. Also, researchers should aim to develop explainability-enhancing technologies in relation to data collection and algorithms used for AV decision-making. They should formulate methods for designing AV systems which guarantee that datasets and algorithms are thoroughly documented, meaningfully transparent and explicable in a way that is adapted to the expertise of the parties concerned (e.g., individual users, policymakers, etc.) More broadly, further empirical, technical, normative/philosophical and legal research is needed to explore methods and safeguards of explainable AI that help to mitigate against biases and discrimination risks.

Autonomy of vehicles, allocation of moral responsibility of actors and bias are some of the main issues in the current debate on ethics. The use of the term "Autonomy" in AV technology is considered an oxymoron, as "autonomy", in its original (philosophical and ethical) sense is an important aspect of human dignity that "ought not to be relativised"[European Group on Ethics in Science and New Technologies 2018].

When it comes to moral standards and responsibility, the wider public tends to misattribute intelligence in AVs, whereas their performance highly depends on humans and the deep learning behind the system (as defined by humans programming the AVs). This paradox has been described in the concept of moral crumple zone[3] [Elish 2016].

Also, feeding autonomous systems with algorithms and performing data-wrangling of different sorts contains traps, as it can lead to algorithmic bias. AVs are able to absorb huge amounts of data through deep learning and are expected to apply requirements inserted to those systems, but they are unable to *grasp the spirit of the law* and the rationale behind the applicable standards; they can therefore reiterate bias and discrimination[4].

[1] Automation levels 3 and 4 in the SAE taxonomy[SAE International 2018]

[2] Article 22 (3) of the GDPR states that the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

[3] Moral crumple zones is a concept introduced by the anthropologist Madeleine Clare Elish. It describes how responsibility for an action may be misattributed to a human actor who had limited control over the behavior of an automated or autonomous system. Just as the crumple zone in a car is designed to absorb the force of impact in a crash, the human in a highly complex and automated system may become simply a component—accidentally or intentionally—that bears the brunt of the moral and legal responsibilities when the overall system malfunctions.

[4] For example, a report published by NIST [NIST 2019], shows that the demographic effects of face recognition vendor tests demonstrate significant identification error characteristics by race and sex. Facial recognition algorithms may contain more images

This aspect also raises questions as to the *reliability* of algorithmic systems which may prove unfit for use in AVs (e.g. misclassifying pedestrians as objects or vehicles). The recent technical report of the Joint Research Center [Hamon et al. 2020] sets out two indicators that may be used to assess the lack or reliability: poor performances (the AI system in a vehicle does not perform well in carrying out tasks that are normal for humans) and vulnerabilities leading to malfunctions (occurring either naturally, in the course of the execution of the program, or being intentionally provoked by an adversary with malicious intentions).

The main issue examined in this section is that autonomous systems used in self-driving cars must replicate — or do better than — the human decision-making process in the event of a car accident. These decisions require a sense of ethics, which is hard to embed to the algorithmic system. The ethical dilemma of the trolley problem is presented below.

4.1 The Trolley Problem

The Trolley Problem has troubled ethicists for decades. It arises from a set of moral dilemmas, most of which involve trade-offs between causing one death and preventing several others. The descriptive problem is to explain why, from a psychological point of view, people tend to approve of trading one life to save several other lives in some cases but not in others [Greene 2016].

Consider the two most widely discussed cases: people responding to the standard switch case (a.k.a. bystander) tend to approve of hitting a switch that will redirect a trolley away from five people and onto one. By contrast, people responding to the standard footbridge case tend to disapprove of pushing one person off a footbridge and in front of a trolley, killing that person but saving five further down the track [Gogoll and Müller 2016].

4.2 Ethical Approaches

4.2.1 Deontology. "Do nothing and let five people die, because steering the trolley would amount to actively killing someone, which is inherently wrong." An agent must decide for a specific ethics setting. What is the right ethics setting and who should be able to choose the ethics for the AV drivers, consumers, passengers, manufacturers, programmers? Should we collectively mandate a specific ethics setting for the whole of society, or should every driver have the choice to select his own ethics setting? [Vallor et al. 2018]

Deontology is an ethical theory that focuses on the actions themselves, instead of their consequences. It is often described as duty based ethical theory because at the core of deontology is the notion of obligation to follow rules and/or laws. The goal of avoiding collisions with other road users can be expressed in the control law as constraining the vehicle motion to paths that avoid pedestrians, cars, cyclists and other obstacles. The vehicle programmed in this manner would never have a collision, if a feasible set of actions or control inputs existed to prevent it [Gerdes and Thornton 2015]. Kant's ethical theory is deontological precisely because at its core are rules and not people's desires, which means that an action is inherently right or wrong regardless of the consequences and that results in the killing of the individual on the other track.

Taking the idea of prioritizing human life and the most vulnerable road users and phrasing the resulting hierarchy in the spirit of Asimov's laws gives:

(1) An automated vehicle should not collide with a pedestrian or cyclist.
(2) An automated vehicle should not collide with another vehicle, except where avoiding such a collision would conflict with the First Law.
(3) An automated vehicle should not collide with any other object in the environment, except where avoiding such a collision would conflict with the First or Second Law [Gerdes and Thornton 2015].

4.2.2 Utilitarianism. Another ethical approach to the trolley problem comes from utilitarianism or consequentialism. This theory looks into the consequence of an action rather than the action itself and deems that the utility of a given action is judged by the amount of pleasure that it offers to the greater amount of people [Kaptein and Wempe 2011].

If utilitarianism is applied to the trolley problem, the optimal solution would be to save the lives (pleasure) of as many people as possible. To provide an example on AVs, if the system of the self-driving car had to choose between saving the lives of its single passenger versus the lives of a group of four friends crossing the street, it would choose to sacrifice its passenger to spare more lives [MIT 6 30]. However, the moral dilemma can be trickier. What if the passengers of the AV are a mother and her newborn child and the car is about to hit old people crossing the street. Which option will the car choose? Another point that might complicate the situation would be whether the pedestrians cross the street through a crosswalk and whether they wait for their green light to turn on, abiding to traffic laws. It seems that an assessment on numbers does not always provide an answer to life and death scenarios, since it fails to consider other contributing factors [Millar 2017].

4.2.3 Virtue Ethics. The final ethical approach to be discussed is virtue ethics. This theory focuses on the agents behind the action and claims that their skills and motives must be virtuous and their actions must be habitually practiced and aim at the ultimate good, which Aristotle called *eudaemonia* [Kaptein and Wempe 2011].

Virtue ethics offer flexibility for engineers, since they can pick the specific set of virtues that they want to embed in the AV's system. These virtues include but are not limited to liberality, justice, prudence, truthfulness and wittiness [Vallor et al. 2018]. The problem with this approach is, again, that it is highly subjective: different humans have different ideas about morality, that depend on their ethnic, social, and cultural environment. There is simply no universal moral code. Furthermore, software designers can take advantage of the flexibility that this theory is offering to code the virtuous traits that they consider less restrictive on innovation.

4.3 Final Remarks on Ethics

The application of the three ethical approaches in the context of self-driving cars is highly volatile. Deontological approaches vary

of people with light skin than black skin, leading to racial bias and lack of capacity to properly and accurately identify people of all different racial backgrounds.

according to what each society deems as a moral action. Utilitarianism may be more homogeneous as an approach, in that it is independent of existing rules. However it diminishes humans to numbers, thus failing to value their inherent dignity. Lastly, approaches in virtue ethics depend on the set of virtues of each individual, leading to the same issue as in deontology: the approaches are highly subjective and diverse. As long as there is not a standardized code of virtues by which engineers can adhere to, it is risky to rely on this approach.

This open-ended and subjective character of the three ethical approaches on the trolley problem offers designers of AVs systems a wide margin of discretion. Currently, they might be choosing to avoid embedding a specific ethical approach in their systems in order to: a) avoid controversies with potential buyers of the cars that are primarily concerned with promoting their own safety and b) enable innovation without ethical restrictions.

Even if designers and manufacturers find it difficult or undesired to choose one of the above theories, the solution could nevertheless be found in the field of technology. The Independent Expert Report on Ethics of Connected and Automated Vehicles of the European Commission [Horizon 2020 Commission Expert Group (E03659) 2020] recommends, among others, the study of current traffic collision statistics, the results of which designers can use to reduce disproportionality in the rates of harm of road users depending on their road exposure. Other technological solutions on semi-autonomous driving include the adoption of advanced facial recognition systems to discern human beings and their behavior on the road and the promotion of Internet of Things allowing the communication among smart vehicles and the exchange of useful information on road traffic, notwithstanding the privacy and bias concerns that arise [Cunneen et al. 2020]. Finally, a combination of neural networks, with benefits including "parallel computing, distributed information storage, fault tolerance, adaptive learning",and fuzzy logic, "a process of uncertain and nonlinear reasoning" similar to human reasoning, can be applied to solve the dilemma of the trolley problem [Li et al. 2018].

In any case, the adoption of a solution to the trolley problem would shed some light on the liability issue, that is which agent is going to be liable in the case of a car crash and to which extent. Depending on the choice of moral theory, the number of affected parties in the event of a car crash may vary, affecting the degree of liability for the actors involved, being the driver, the designer of the autonomous system and/or the manufacturer of the car. As a preliminary point, in order for the judge to decide the liability or responsibility of the defendant, in practice the manufacturer, in a case of a car crash caused by an autonomous vehicle, he or she must assess the intention of the manufacturer and the reasonableness of the prevention of a car crash, taking into consideration the safety of the driver and of third parties and, the utility to the consumer. This in turn would require a further balancing test of the following factors: "the feasibility of an alternative design, the likelihood and gravity of expected harm, and the disadvantages of the plaintiff's proposed alternative design" [Wendel 2018]. We elaborate further on this issue in the following section.

5 LIABILITY

Whereas in the majority of conventional car accidents the driver retains some control thus assumes primary liability for the vehicle's fate, in driverless cars, part or all of the liability will shift onto the AV as accidents become more of an issue of product safety or efficacy [Taeihagh and Lim 2019].

Liability linked to AVs raises issues mainly because the lack of clear-cut responsibility, standards and regulatory frameworks for accident investigation may hamper efforts to investigate accidents [European Parliament: Panel for the Future of Science and Technology 2020]. On the other hand, the lack of regulatory provisions on AVs testing limits the possibility of manufacturers to observe the "behavior" of AVs on public roads and identify any possible sources of accidents. Hence, liability, as a notion related to traditional legal notions of civil law, plays a crucial role in case of AVs accidents. Although AVs are designed to substitute human judgement in order to ensure higher driving performance, accidents can and do happen [Harris 2020].

Existent approaches in EU level and the UK address liability for defective products under the "state of the art" criterion and litigation will probably evolve around it in the absence of other denominators[5].

The following scenario allows us to understand in practical terms what liability issues and challenges may arise in the context of AVs: Mr. X drives his AV and activates the autonomous driving mode[6]. Despite an alarm warning from the vehicle, he does not react because he perceives no danger/obstacle on the road. The vehicle, driving in an autonomous mode, abruptly turns and injures a pedestrian crossing the road. The victim brings an action for damages both against Mr. X and the manufacturer of the AV. The question now is how liability will be allocated.

Establishing liability under civil law requires fault or negligence which causes the damage but the causal connection between negligence and damage must be established. Although this seems simple, in this example it would be difficult to determine with whom lies the fault and/or negligence: to the driver that does not react to the warning and does not take control of the vehicle or to the manufacturer for defects?

In traditional car accidents, there seems to be a presumption that liability lies with the driver having the control and being in contact with the object moving. The reply is again complicated, depending on whether it is proven that by activating the autonomous mode the driver did no longer retain control.

Furthermore, a key concept to be assessed is the notion of "defect". It is argued that the failure to program the AV for a particular driving situation which gives rise to an accident will constitute a "defect" provided that the parties are able to show this. Examples of defects may include: a deliberate software choice (e.g. colliding with a car to avoid a pedestrian); a defect in the sensors, so as the AV received incorrect information about the external world or commands not being executed accurately [Sanitt et al. 2017].

[5]UK consumer act provides the definition of the state of the art: "the state of scientific and technical knowledge at the relevant time was not such that a producer of products of the same description as the product in question might be expected to have discovered the defect."

[6]There are different levels of autonomy, but for the example we consider the level 4 under the SAE taxonomy (high automation with the possibility of human intervention)

According to the EU Directive on liability for defective products [European Parliament 1999], it is sufficient to prove that the product is constructed in a way that does not guarantee the safety level that a person is entitled to expect[7]. The question is how this safety level is defined and assessed, since it is quite a subjective notion.

Moreover, since AVs are subject to various external communications (e.g. sensors, cloud data), there is a significant risk that auto manufacturers will be able to tamper with sensors generating data for evidence to evade liability. To tackle this issue, a BlockChain (BC) based framework that integrates the involved parties in the liability model and provides untampered evidence for liability attribution and adjudication has been proposed [Oham et al. 2018]. There have been several projects proposing leveraging blockchain technology to store and use vehicle data for AVs[8].

As a concrete example of liability allocation, reference can be made to the UK, one of the few European countries with concrete allocation of liability[9]. The Vehicle technology and aviation Bill [UK Parliament 2017] clarifies the liability of insurers and AV owners in the event of an accident and under a wide range of circumstances. The UK legal framework is a very interesting and concrete example for the following reasons:

- Insurance obligations are regulated: the UK framework resolves significant ambiguity regarding liability and insurance implications under various accident scenarios (reflecting the government's toleration-based approach) [Taeihagh and Lim 2019].
- Standard common law notion of damage is introduced (personal injury or death and third party property). Regarding insurance law, the Bill states that where the car is driving automatically, and causes the incident, first instance liability is on the insurer and the (human) driver is also covered [Butcher et al. 2017]. This has led to some manufacturers (but not all) offering to self-insure their AVs while they drive in automated mode [Department for Transport 2016].

To sum up, the lack of specific legal framework on AVs in most EU countries raises many issues on liability allocation. So far, only the UK developed specific legislation on this matter; Germany issued legislation providing for the use of a black box in order to determine liability[10]. A harmonized and consistent approach is urgently needed on EU level. Policy makers are expected to develop specific strategies and governments need to adopt specific legislative measures in order to reply to the emerging legal gaps, while opting for a technology-neutral approach to encourage innovation. Countries like the UK, US and Australia, which apply light-control strategies, aim to align expectations regarding safety standards without imposing overly restrictive barriers to innovation [Taeihagh and Lim 2019]. Given the above considerations, we expect common law countries to stick to this approach by also regulating insurance liability, whereas civil law countries might follow Germany's example, opting to apportion liability between the manufacturer and the driver[11]. The inconvenience of this approach is that it will be extremely challenging to determine the time that drivers were supposed to take control of the vehicle in order to allocate liability in case of an accident.

6 CONCLUSIONS

To conclude, we believe that a critical part of any effort to achieve consumer acceptance of AVs will be ensuring consumers that the involved technologies do not pose a significant threat to privacy and have been designed to help protect against vehicle tracking by any government or company participating in the ecosystem. There are several open research challenges in the area of privacy respecting machine learning and AI in automated and autonomous driving. We especially noted that applying anonymization of video recorded by vehicle cameras can impact the detection quality of vehicles at various degrees, which is something that is not well understood so far. There is also great need for more harmonization efforts between different legal data protection regimes world-wide. We highlighted the areas where more clear instructions and guidance must be given to the industry in order to overcome legal uncertainties. For example, a) the case of legal basis for processing CAM and DENM messages in the context of C-ITS and b) video captured by dashcams are two characteristic cases. At the same time, EU regulators recommend a prudent approach to AI, although it is recognised that wide use of AI in transport services is considered "essential"[Wiewiórowski 2020]. Regarding ethical issues, more research is needed to analyze the trade-offs from using different types of ethical rules for AVs. In tandem, there are still several liability issues and who bears responsibility for accidents involving AVs is not yet straightforward. Another challenge that machine learning poses is how to consider the system requirements that are necessary to support a meaningful human review from the design phase, so as to reduce the risk for incorrect classifications and bias. Overall, there is a need to act swiftly in responding to the above open issues, since uncertainty might impact the degree to which the technology is adopted and lead to the investors' interest to cool, due to the perception that this technology simply does not live up to the hype.

ACKNOWLEDGMENTS

The research in this paper has been made possible through the open platform offered by the Greek civil society organization Homo Digitalis[12], which sparked our discussions and brought us together to write this paper.

The authors would also like to thank the anonymous referees for their valuable comments and helpful suggestions.

[7] Article 6 of Council Directive 85/374/EEC of 25 July 1985, as amended by Directive 85/374/EC. The circumstances to be taken into account include: the presentation of the product; the use to which it could reasonably be expected that the product would be put; the time when the product was put into circulation.

[8] For instance the Mobility Open Blockchain Initiative (MOBI). GM has filed a patent application for blockchain database application for data exchange between vehicles and entities.

[9] Apart from the UK which has developed a comprehensive and extended legislative framework on AVs, Singapore is classified by KPMG Global as the second most well prepared country to introduce AVs in everyday life, especially in terms of policy and regulation [KPMG International 2019].

[10] Federal Law Gazette of 20 June 2017, Part I No. 38, p. 1648. In particular, both liability of the driver and the manufacturer is possible, but the use of black box allows to clarify who had the control of the car. Hence, the German law does not shift the liability directly to the manufacturer.

[11] According to the German framework, manufacturers are made responsible for accidents where the AV system is in charge.

[12] https://www.homodigitalis.gr/en

REFERENCES

Article 29 Data Protection Working Party. 2017. *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).* Document.

Bayerisches Landesamt für Datenschutzaufsicht. 2019. *8. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für die Jahre 2017 und 2018.* Report.

Cara Bloom, Joshua Tan, Javed Ramjohn, and Lujo Bauer. 2017. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA, 357–375.

Louise Butcher, Lorraine Conway, and Tim Edmonds. 2017. *Vehicle Technology and Aviation Bill 2016-17.* Briefing Paper Number CBP 7872.

Commission Nationale de l'Informatique et des Libertés (CNIL). 2017. Connected Vehicles and Personal Data. https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf.

Martin Cunneen, Martin Mullins, Finbarr Murphy, Darren Shannon, Irini Furxhi, and Cian Ryan. 2020. Autonomous Vehicles and Avoiding the Trolley (Dilemma): Vehicle Perception, Classification, and the Challenges of Framing Decision Ethics. *Cybernetics and Systems* 51, 1 (2020), 59–80.

Data Protection and Privacy Working Group of the C-ITS Platform. 2017. *Processing personal data in the context of C-ITS.* Document.

Department for Transport. 2016. *Pathway to Driverless Cars: Proposals to support advanced driver assistance systems and automated vehicle technologies.* Report.

M Elish. 2016. Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction (WeRobot 2016). *SSRN Electronic Journal* (January 2016).

ETSI. 2017. *Intelligent Transport Systems (ITS); Security; Security Header and Certificate.* Technical Specification TS 103 097.

European Commission. 2016. *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility.* COM(2016) 766 final.

European Commission. accessed January 29, 2020. Intelligent transport systems - Cooperative, connected and automated mobility (CCAM). https://ec.europa.eu/transport/themes/its/c-its_en.

European Data Protection Board. 2020. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.* Guidelines Open for Feedback.

European Group on Ethics in Science and New Technologies. 2018. *Statement on artificial intelligence, robotics and 'autonomous' system.* Report.

European Parliament. 1999. *Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products* . OJ L 141, 4.6.1999.

European Parliament. 2017. European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html.

European Parliament: Panel for the Future of Science and Technology. 2020. *The ethics of artificial intelligence: Issues and initiatives.* Study.

J. Christian Gerdes and Sarah M. Thornton. 2015. *Implementable Ethics for Autonomous Vehicles.* Springer Berlin Heidelberg, 87–102.

Jan Gogoll and Julian Müller. 2016. Autonomous Cars: In Favor of a Mandatory Ethics Setting. *Science and Engineering Ethics* 23 (July 2016).

Bryce Goodman and Seth Flaxman. 2017. European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". *AI Magazine* 38, 3 (Oct. 2017), 50–57.

Nathan Greenblatt. accessed January 29, 2020. Self-Driving Cars Will Be Ready Before Our Laws Are. https://spectrum.ieee.org/transportation/advanced-cars/selfdriving-cars-will-be-ready-before-our-laws-are.

Joshua Greene. 2016. Solving the Trolley Problem. In *A Companion to Experimental Philosophy*. John Wiley & Sons, 173–189.

Ronan Hamon, Henrik Junklewitz, and Jose Sanchez Martin. 2020. Robustness and Explainability of Artificial Intelligence. Publications Office of the European Union.

Mark Harris. accessed January 29, 2020. NTSB Investigation Into Deadly Uber Self-Driving Car Crash Reveals Lax Attitude Toward Safety - IEEE Spectrum. https://spectrum.ieee.org/cars-that-think/transportation/self-driving/ntsb-investigation-into-deadly-uber-selfdriving-car-crash-reveals-lax-attitude-toward-safety.

Stephan Heinrich. 2017. Flash Memory in the emerging age of autonomy. In *Flash Memory Summit 2017 Proceedings.*

L. Hobert, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovacs. 2015. Enhancements of V2X communication in support of cooperative autonomous driving. *IEEE Communications Magazine* 53, 12 (Dec 2015), 64–70.

Horizon 2020 Commission Expert Group (E03659). 2020. *Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility.* Publication Office of the European Union: Luxembourg.

Information Commissioner's Office (ICO). 2020. ICO guidance on AI - "How do we ensure individual rights in our AI systems?". https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/.

International Working Group on Data Protection in Telecommunications. 2017. *Resolution on Data Protection in Automated and Connected Vehicles.* Resolution from the 39th International Conference of Data Protection and Privacy Commissioners, Hong Kong.

International Working Group on Data Protection in Telecommunications. 2018. *Connected Vehicles.* Working Paper from the 63rd meeting, 9-10 April 2018, Budapest, Hungary.

Irish Data Protection Commission. 2018. *Guidance for Drivers on the Use of Dash Cams.* Report.

Muel Kaptein and Johan Wempe. 2011. Three General Theories of Ethics and the Integrative Role of Integrity Theory. *SSRN Electronic Journal* (October 2011).

KPMG International. 2019. *2019 Autonomous Vehicles Readiness Index: Assessing countries' preparedness for autonomous vehicles.* Report.

M. Kyriakidis, R. Happee, and J.C.F. de Winter. 2015. Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. *Transportation Research Part F: Traffic Psychology and Behaviour* 32 (2015), 127–140.

Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg. 2018. *34. Tätigkeitsbericht 2018.* Report.

Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg. 2019. *Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen(sog. Dashcams).* Report.

Sixian Li, Junyou Zhang, Shufeng Wang, Pengcheng Li, and Yaping Liao. 2018. Ethical and Legal Dilemma of Autonomous Vehicles: Study on Driving Decision-Making Model under the Emergency Situations of Red-Light Running Behaviors. *Electronics* 7 (10 2018), 264.

Hin-Yan Liu. 2018. Three Types of Structural Discrimination Introduced by Autonomous Vehicles. *UC Davis Law Review Online* 51, MAY 2018 (5 2018), 149–180.

N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark. 2014. Connected Vehicles: Solutions and Challenges. *IEEE Internet of Things Journal* 1, 4 (Aug 2014), 289–299.

Jason Millar. 2017. *Ethics Settings for Autonomous Vehicles.* Oxford University Press, 5.

MIT. Accessed: 2020-06-30. Moral Machine. https://moralmachine.mit.edu/.

NIST. 2019. Face Recognition Vendor Test (FRVT)Part 3: Demographic Effects. https://doi.org/10.6028/NIST.IR.8280.

Chuka Oham, Salil S. Kanhere, Raja Jurdak, and Sanjay Jha. 2018. A Blockchain Based Liability Attribution Framework for Autonomous Vehicles. arXiv:1802.05050 [cs.CR]

SAE International. 2018. *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.* Standard J3016_201806.

Adam Sanitt, Marcus Evans, Shiv Daddar, Huw Evans, and Seiko Hidaka. 2017. Autonomous vehicles: The legal landscape of DSRC in the United Kingdom. https://www.nortonrosefulbright.com/en/knowledge/publications/85e2f81c/autonomous-vehicles-the-legal-landscape-of-dsrc-in-the-united-kingdom.

L. Schnabel, S. Matzka, M. Stellmacher, M. Pätzold, and E. Matthes. 2019. Impact of Anonymization on Vehicle Detector Performance. In *Second International Conference on Artificial Intelligence for Industries (AI4I).* 30–34.

European Data Protection Supervisor. 2019. EDPS TechDispatch on Connected Cars. https://data.europa.eu/doi/10.2804/70098.

Araz Taeihagh and Hazel Si Min Lim. 2019. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews* 39, 1 (2019), 103–128.

UK Parliament. 2017. *Vehicle Technology and Aviation Bill 2016-17.* Government Bill 143.

Shannon Vallor, Brian Green, and Irina Raicu. 2018. Conceptual Frameworks in Technology and Engineering Practice, Ethical Lenses to Look Through. Markkula Center for Applied Ethics.

Sandra Wachter, Brent Mittelstadt, and Luciano Floridi. 2017a. Transparent, explainable, and accountable AI for robotics. *Science Robotics* 2 (05 2017).

S Wachter, B Mittelstadt, and L Floridi. 2017b. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law* 7, 2 (2017), 76–99.

Bradley Wendel. 2018. Economic Rationality and Ethical Values in Design-Defect Analysis: The Trolley Problem and Autonomous Vehicles. *California Western Law Review* 55, 1 (2018).

Wojciech Wiewiórowski. September 7, 2020. Artificial Intelligence, data and our values – on the path to the EU's digital future. https://edps.europa.eu/press-publications/press-news/blog/artificial-intelligence-data-and-our-values-path-eus-digital_en.