A Literature Review of Data Ethics in Autonomous Vehicles

Joshua Chong

Received December 01, 2024
Accepted April 25, 2024
Electronic access May 15, 2024

The rapid pace of innovation in artificial intelligence and the resulting rise of autonomous vehicles (AVs) has left a trailing gap in ethics. Training a system as complex as a self-driving vehicle requires a substantial volume and diversity of data, raising concerns about the origin of said data. This paper examines the surrounding literature discussing data used in the training and implementation of AVs, the security and privacy of the gathered data, regulatory frameworks in existence, as well as their relation to modern day ethics. Data ethics in AVs is important because of the risk of cyberattacks, and subsequently, safety. Although there are a number of papers discussing ethics in AVs, most focus on moral dilemmas, such as the trolley problem, and fail to satisfactorily explore the data used. The information gathered in this literature review comes from multiple papers, including literature reviews and independent studies. This study found that while AVs have the potential to be very beneficial in the future through increased safety and accessibility, there are concerns regarding data privacy, cybersecurity, and transparency. This study also proposes a driver's education course for AVs that explains the data privacy risks associated with using an AV as a solution to these concerns.

Keywords: Autonomous vehicles, Self-driving vehicle, Artificial Intelligence, Big Data, Data privacy, Cybersecurity, Transparency

Introduction

With the world exceedingly focused on what the future will look like with AI, awareness is diverted from the less visible aspects, such as ethics. In 2022, the global artificial intelligence market size was valued at $136.55 billion, and is projected to expand at a compound annual growth rate of 37.3% from 2023 to 2030[1]. One major component this sector is comprised of is the category of autonomous vehicles, with the global autonomous vehicle market size estimated at $121.78 billion in 2022 and projected to grow at a compound annual growth rate of 35% from 2023 to 2032[2]. The rapid growth brings urgency to improving the safety of such vehicles, including ethical concerns like data privacy.

One major advantage of AVs is that they offer the promise of improved safety compared to human-driven vehicles. The World Health Organization reports that there are approximately 1.3 million fatalities each year from crashes related to road traffic[3]. However, AVs eliminate the human aspect of driving, leading to an increase in safety and efficiency[4]. The leading company in autonomous vehicle development, Alphabet-owned Waymo, has shown promising results through the deployment of their vehicles. A paper by Waymo researchers, who used 7.14 million miles of data from the National Highway Traffic Safety Administration's (NHTSA) Standing General Order, found that the any-injury crashed vehicle rate of the Waymo automated driving system was 85% less than the human benchmark[5]. Furthermore, AVs have the potential to increase traffic flow by 80% due to the ability to be interconnected with other AVs and technology[6].

The growth of autonomous vehicles is also supported by their potential to improve the modern world through an increase in accessibility and sustainability. With the average age of the population steadily increasing, the world requires constant adaptation. In the EU, the population of people aged 65 or older is projected to rise from 90.5 million at the start of 2019 to 129.8 million by 2050[7]. This increase in the elderly population in the EU coincides with increases in disability rates, with 48.5% of people with disabilities being aged 65 or older[8]. AVs can assist the aging population by granting the disabled or elderly access to quick and independent transportation without the need for them to physically drive. Ride-sharing and reduced costs of labor can also make taxi rides affordable to use on a daily basis, with estimates that the cost per mile of an autonomous taxi could be just 20 percent higher than that of a private car[9].

Yet, while the future of AVs appears promising, a cautious approach to implementation is essential. At the heart of all AI lies big data, with AVs relying on an estimated 104 TB of data for training, a volume that increases with model complexity[10]. There are a lot of ethical concerns surrounding this collection and storage of data, meaning that laws are needed that address cybersecurity, transparency, and accountability in order to protect this private data.

This paper conducts a comprehensive review of multiple papers, including both independent studies and literature reviews. While there are a number of papers discussing ethics in AVs[11],

there is a large focus on the moral dilemmas such as the trolley problem rather than the ethics in the data used[11–13]. Based on this review, it is concluded that education and transparency of data privacy to the consumer is necessary for data ethics to coexist with the advancement of AVs. This paper proposes that companies delay commercializing the technology until the technology is mature enough, and instead focus on the safety of data in AVs. Overall, the potential benefits of AVs outweigh the risks, and over time, this technology will improve until it becomes normalized like current-day technology.

The first section of this literature review will go over what data is used to train autonomous vehicles and the ethical issues surrounding this data. The second section discusses what laws exist concerning data privacy, including specific examples of incidents, as well as consider what areas lack regulation. The discussion section will go over what must be done to address data privacy ethical concerns and the ways to safely implement AVs into society.

Methods

This paper is a literature review, meaning it required a review of many research papers that discussed data ethics and autonomous vehicles. The papers reviewed in this paper were found by searching using key phrases like "data ethics in autonomous vehicles", "data privacy in autonomous vehicles", and "cybersecurity in autonomous vehicles." Some of the papers this research found were literature reviews, while others were studies on new advancements in the area of data security of AVs. This paper reviews papers that are more recent to get an accurate understanding of where research currently stands. The oldest paper is from 2017, and the majority are from 2021 or later. The main goal was to understand the importance of data ethics in AVs, and the regulations that exist or are missing regarding data and AVs.

Understanding Data Ethics in Autonomous Vehicles

Data with respect to autonomous vehicles is used for both research and commercial purposes. It is needed to train the AI models in AVs, and once trained, they capture surrounding data in real-time to make decisions. This data includes nearby obstacles, such as humans, other vehicles, and buildings. It also includes in-cabin data, such as the appearance of the passengers, which might help the AV know whether the passenger is capable of driving or if they need medical assistance. On top of this, interconnection of data between different AVs and other surrounding technology helps travel be more efficient. However, the collection of private data contains the possibility of it becoming public, which can be used maliciously in the wrong hands.

Data Privacy and Personalization

Data comes from many sources, including CCTV and vehicle cameras, sensors on AVs, and GPS. These can be exploited in malign attempts if not kept private. Identifying features such as faces, license plates, and location tracking can allow a hacker to track a vehicle. Such concerns bring up the dubiety around which data capturing is truly considered ethical. For example, CCTV cameras were initially not intended for data collection purposes, but instead for recording and monitoring. Would it be ethical to use the video-tapes of recorded subjects without their permission? There are solutions for more obvious issues like face recognition, such as blurring. This is not perfect however, as blurring happens after a picture is taken, meaning this data can be traced back to its original[14]. Other solutions include more advanced technology like LiDAR, which uses short light pulses that deflect off surrounding features to determine the shape of the surrounding, and can keep anonymization by removing the need for full color pictures[15]. At the same time, there are some less obvious and more ubiquitous areas of ethical concern. For example, wifi networks of AVs can be hacked into, allowing hackers to have access to all collected data and connected devices. Additionally, there is sometimes a log of user data that is kept to improve experience. For example, Google Maps tracks one's typical movement around the city and makes suggestions of places if not disabled. Even though Google deletes location history after 18 months, the data stored can still be used maliciously before then[16]. AVs might become a hotbed for recommendation algorithms like this in the future, parallel to how cell phones are now. Legal measures and their limitations are discussed in a later section.

Safety

Safety is one of the most crucial factors in the construction of AVs. It is critical that autonomous vehicles are tested thoroughly before being put into use. In order for an AV system to be created and tested accurately, while at the same time not risking the harm of bystanders, simulations are commonly used. A lot of the development on AV algorithms relies on fake data, as real data is not only sensitive but also extremely expensive to collect. However, parameters in simulations often differ from reality, and simulations have become unreliable due to over-optimization, creating a sim-to-real gap[17]. GANs and similar technologies try to bridge the sim-to-real gap as much as possible but there is always some distance from the truth. In such a safety critical application this holds the potential to be incredibly problematic.

There have been recent improvements to the collection of simulation data concerning the sim-to real gap. SurfelGAN,

created by researchers at Waymo, is able to generate realistic scenario sensor data with only a limited amount of liDAR and camera data collected by an AV[18]. They do this by using a generative adversarial network (GAN), which is a deep learning AI that can generate realistic images based on sample data. This makes it both faster to obtain data, as well as more private, since much of the data is generated from a smaller batch of data. Another recent proposal by Trinh et al. (2023) is the use of PP4AV, a benchmarking dataset for privacy-preserving autonomous driving. This dataset is a collection of data from the public domain that can be used to test anonymization of private data, such as faces and license plates[19]. Augmented autonomous driving simulation (AADS) is an updated type proposed by Li et al. (2019)[20]. On top of augmenting the data collected from liDAR and cameras, AADS also generates simulated traffic flow to increase the realism of the simulation. The more accurate the simulation is, the safer the autonomous vehicle will be when finished training.

Cybersecurity

Another way AVs can be more efficient and safe is through connected and automated vehicle (CAV) technology. This is when vehicles are connected to other vehicles, as well as transportation infrastructure. For example, AVs can obtain data from traffic lights to know when each light will turn green, or obtain data from CCTV cameras to get a better view of the surroundings and detect collision threats. Researchers estimated that CAVs can reduce traffic conflicts by 90%[21]. However, CAVs are susceptible to malicious attacks because the transmission of data makes it a lot easier for them to be intercepted. These attacks can be very dangerous to a vehicle that makes decisions solely based on the data it receives. Kim et al. (2021) classifies cyberattacks into the three categories of autonomous control system, autonomous driving systems components, and vehicle-to-everything communications, and classifies defenses into the three categories of security architecture, intrusion detection, and anomaly detection[22]. As a defense, Wang et al. (2021) suggests using real-time anomaly detection to detect abnormal data points that can be caused by a malicious attack[23]. Having a program like the one suggested in this paper adds another line of defense to the privacy and safety of data. This doesn't solve all the concerns though. In his paper, Wang mentions that they only use the data from the single leading vehicle, when data from multiple connected vehicles and other infrastructure components can have an impact on anomaly detection. For example, vehicles can be attached to their user's personal information such as contacts, home address, license plate, drivers license, financial information and can even be connected to other user accounts. Furthermore, if one is able to identify each vehicle and consistently track it, they can also learn user behaviors, which puts the users at risk of a robbery for instance. These examples show that if data is not properly protected, users can be at risk of both physical attacks and cyberattacks.

The Legal Facet of Data Privacy in Autonomous Vehicles

There have been numerous laws and regulations passed concerning autonomous vehicles, including ones on data privacy. In the United States, it is mainly up to the states to create their own legislation around autonomous vehicles. For example, in California, it is required for companies to inform passengers or owners of autonomous vehicles what data that is not a necessity for safety is being collected from them. If the consumer decides not to give approval to this collection of data, the companies have to anonymize the data[24]. Other than these laws, there isn't much else regarding the privacy of data. This could leave gaps in the law, such as companies being allowed to collect data that is necessary for safety without the consumers permission, something that is very subjective. An example of this is how San Francisco police have requested camera footage from Waymo autonomous vehicles to help gain evidence for crimes[25]. While this is obviously helpful to the police, the average consumer may find this a breach of data privacy.

In the European Union, there are more laws concerning autonomous vehicles when compared to the US. The EU includes a requirement for a closed-loop system in recording event data, meaning that the data gets constantly overwritten. It is definitely more thought out than the US regulations, as it even references connectivity risks between vehicles[26]. However, it still lacks specificity and a focus on the capture of outside data. Furthermore, the EU is not immune to cyber attacks and breaches of data, as proven by previous incidents. Tesla had a 100GB data leak due to an internal abuse of access[27]. This brings up the question of how safe a consumer's data is, even when they are guaranteed privacy. While there has been a lot of focus on accountability in terms of vehicle crashes, there hasn't been much focus on accountability of breaches in data privacy.

As shown in the case of California, there is a basis of laws concerning transparency of data privacy. However, this transparency may not reach the average bystander. While the consumer has to be given the option of sharing their data or not, data collected from the surroundings does not need such permission. Even though faces and identifying features can be blurred, it is not completely accurate at hiding information. Li et al. (2017) found a very high identification success rate of almost 70% when only the face is blurred[28]. In the example of Waymo, this information is not guaranteed to be hidden, and a bystander would not be aware of the use of their data due to the lack of transparency.

In terms of accountability, Andraško et al. (2021), in an analysis of the EU law, found that it is very important to establish the liable entity in matters relating to the processing of personal

data, especially in regards to CAVs. While data processing is especially important for the development and use of CAVs, there are many different entities that have control over the flow of data. Their paper argues that the regulations surrounding CAVs are not definitive[29].

Globally, there has been some international standardization of regulations. In 2016, the Vienna Convention on Road Traffic opened the possibility of automated features in vehicles, but even this only includes 86 countries[30]. More recently, during the World Forum for Harmonization of Vehicle Regulations in 2019, representatives of China, European Union, Japan and the United States of America met to create a revised framework document on automated/autonomous vehicles, with the goal to harmonize vehicle regulations[31]. However, the category on cybersecurity is broad and there is nothing on data privacy. This means that it is up to each country to make regulations concerning autonomous vehicles, especially in regards to data privacy and safety.

Discussion

AVs and CAVs are helpful and necessary in terms of safety and efficiency, especially with growing population numbers in the future. They can provide accessibility to the disabled or elderly and remove human error from the equation. Yet because of their complex algorithms and models, AVs cannot be perfect and bring many ethical issues to the table. The most researched one is the classic trolley problem, which considers the moral dilemmas that an AV might occasionally face. Many scholars have generalized this example to more plausible cases, such as what happens when there are multiple options that are all bad in some way. For example, what to do in a scenario where an AV has to decide whether to avoid a car crash and risk hitting a pedestrian[32]. Another concern is the loss of jobs from the implementation of AVs, a common issue with the use of AI. A study by The Center for Global Policy Solutions found that up to 4 million jobs could be lost in the United States, most having a driving occupation. However, they argue that proper policy making can minimize the harm of this shift to autonomous vehicles, such as making higher education more affordable so that other jobs like engineers can be created[33]. The highlight of this paper, though, are the non-physical ethical concerns like cybersecurity and the handling of data. A study by Vrščaj et al. (2020) found that 84.5% of people viewed data collection negatively[34]. Examples of areas where improvement is necessary before widespread implementation are anonymization and cybersecurity, especially in CAVs. It is important for companies to acknowledge that improving the safety of data in autonomous vehicles is more necessary than improving the user experience. Vrščaj's survey found that 54.9% of people viewed AI and recommender systems negatively. This becomes even more important when considering ride-sharing because a public transport that is used by many people could hold a large amount of sensitive data. Things like recommendations have to be only an option, as all consumers have to have the right of data privacy. Based on a survey by Bloom et al. (2017), 54% of the participants were okay with spending more than five minutes using an online system to opt out of identifiable data collection[35]. Transparency is important so that people can understand how an AV is different from a normal vehicle, as well as the physical and privacy risks of using AVs. The government should also take an active part dictating the level of transparency through more specific laws.

It is possible, however, that even if legislation is in place, a company or owner of an AV can still tiptoe the line of what is legal and what is not, such as including things in the fine print. Even in these cases, empowerment lies in education and transparency of the consumer. Because of the rapid advancement of AI, there is an increasing gap between the improvement of AVs and the knowledge the average person has on AVs. This means it is necessary to reshape the education surrounding driving with AVs.

My proposal is to have a driver's course for AVs, where instead of having to physically take action and drive, consumers and users of AVs will be required to understand the data privacy risks with using an AV. This online course would explain what data is being collected, how it is being used, and what options the passenger has concerning the data. An AV course would only be a few hours at most–much shorter than the average driver's education, which in the US is around 45 hours of lessons and 20 hours of practice[36]. Additionally it would be much cheaper and accessible, as it would be fully online compared to the in-person driver's education and test. Since 85.8% of people above the age of 16 in the United States were willing to get a driver's license, an AV course and test would not deter many people[37]. Driver education for self-driving vehicles has been recently suggested to the UK Parliament to help the public understand the capabilities of self-driving technology[38]. Driver education is easier said than done, and research has found a lack of evidence that current driver education is an effective approach to reducing crashes or injuries[39]. The proposal of education for drivers of autonomous vehicles has only recently been mentioned, and more research would have to be done on the benefits of education and the creation of such courses.

There are moral philosophies that justify the use of AVs. The theory of utilitarianism defines morally good as whatever brings the greatest happiness to the greatest number of people. Through evaluating survey data, Karnouskos (2021), found that utilitarianism plays a role in people's acceptance of AVs in society[40]. The benefits of AVs are clear; they can be used as public transport, sharable rides, and taxis, which would reduce the costs of travel and increase accessibility. Therefore, even though there are some risks concerning safety and privacy, the many benefits of AVs make it morally acceptable to implement them as long as they create more good than harm. Additionally, the view of

longterminism, which proposes that positivity influencing the future is the moral priority, counters the argument that AVs can be dangerous with their potential to improve society[41]. Lives may be lost in the near future, but in the long term, lives will be saved through an increase in safety. The same thing follows for jobs, as jobs such as taxi and public transportation drivers will be lost, but jobs such as engineers and programmers will naturally be created in the long term.

Conclusion

AVs have the potential to be very beneficial in the future. However, there are many ethical concerns that come with its creation and implementation. Anonymization is still not perfected, and there is a lack of specific laws concerning collected data. Additionally, CAVs, while more efficient, open up a greater possibility of data being used maliciously if improperly obtained. Previous incidents have shown the vulnerability in the use of data in AVs. As this technology advances, not only is it important to improve the cybersecurity aspect, but also important to educate consumers of the risks of using their data, as well as for big companies to maintain transparency. A large amount of research has been done on the trolley problem and safety of AVs, but there is a lack of research on other ethical dilemmas, including data privacy in autonomous vehicles. Additional research should also be done on the effectiveness of education of drivers on the dangers of autonomous driving, including data privacy, and the possibility of its implementation before the integration of AVs into society.

Acknowledgments

I would like to thank Dimitra Tsakona (Imperial College London) and the Lumiere Research Program for their guidance in the creation of this research paper.

References

1 A. I. M. Size and Share, *Growth Report 2030*, Grand View Research.

2 *Autonomous Vehicle Market Size to Hit USD 2,353.93 BN by 2032*, Precedence Research.

3 W. H. Organization, *Road traffic injuries*.

4 *National Highway Traffic Safety Administration. Automated Vehicles for Safety*, `https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety`.

5 K. Kusanoa, J. Scanlona, Y. Chena, T. McMurrya, R. Chena, T. Godea and T. Victora, Comparison of Waymo Rider-Only Crash Data to Human Benchmarks at 7.1 Million Miles. arXiv:2312.12675 (2023).

6 B. Friedrich, *Autonomous Driving*, Springer, Berlin, Heidelberg.

7 *Ageing Europe: Looking at the Lives of Older People in the EU : 2020 Edition*, ed. L. Corselli-Nordblad and H. Strandell, Publications Office of the European Union.

8 W. Organization, *World Report on Disability*, World Health Organization.

9 *McKinsey*.

10 A. Grzywaczewski, *Training AI for Self-Driving Vehicles: the Challenge of Scale*, NVIDIA. NVIDIA Developer.

11 M. Alawadhi, J. Almazrouie, M. Kamil and K. Khalil, *Int J Syst Assur Eng Manag*, **11**, 1065–1082.

12 S. Hansson, M. Belin and B. Lundgren, *Philos. Technol*, **34**, 1383–1408.

13 C. Xie, Z. Cao, Y. Long, D. Yang, D. Zhao and B. Li, *Protection Methods, and Future Directions*, **2209**, year.

14 A. Mishra, J. Cha and S. Kim, *Computational Intelligence and Neuroscience*.

15 T. Raj, F. Hashim, A. Huddin, M. Ibrahim and A. Hussain, *Electronics*, **9**, 741.

16 *Google will automatically delete location history by default*, CNBC.

17 J. García and F. Fernández, *Journal of Machine Learning Research*, **16**, 1437–1480.

18 Z. Yang, Y. Chai, D. Anguelov, Y. Zhou, P. Sun, D. Erhan, R. S. and H. Kretzschmar, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, p. 11118–11127.

19 L. Trinh, P. Pham, H. Trinh, N. Bach, D. Nguyen, G. Nguyen and H. Nguyen, Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, p. 1206–1215.

20 W. Li, C. Pan, R. Zhang, J. Ren, Y. Ma, J. Fang, F. Yan, Q. Geng, X. Huang, H. Gong, W. Xu, G. Wang, D. Manocha and R. Yang, *Science Robotics*, **4**, year.

21 A. Papadoulis, M. Quddus and M. Imprialou, *Accident Analysis Prevention*, **124**, 12–22.

22 K. Kim, J. Kim, S. Jeong, J. Park and H. Kim, *Computers Security*, **103**, 102150.

23 Y. Wang, N. Masoud and A. Khojandi, *IEEE Transactions on Intelligent Transportation Systems*, **22**, 1411–1421.

24 *Deployment of Autonomous Vehicles, Ca*, `https://www.dmv.ca.gov/portal/file/adopted-regulatory-text-pdf/`,, § 228.24,.

25 J. Love, *Police Are Requesting Self-Driving Car Footage for Video Evidence*, Bloomberg.

26 Regulation, *Regulation (EU) No 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users*, `http://data.europa.eu/eli/reg/2019/2144/oj`.

27 S. Ikeda, *CPO Magazine*.

28 Y. Li, N. Vishwamitra, H. Hu, B. Knijnenburg and K. Caine, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, **61**, 803–807.

29 J. Andraško, O. Hamuľák, M. Mesarčík, T. Kerikmäe and A. Kajander, *Sustainability*, **13**, 10610.

30 *UNECE paves the way for automated driving by updating UN international convention*, UNECE.

31 *Revised Framework document on automated/autonomous vehicles. World Forum for Harmonization of Vehicle Regulations*.

32 A. Martinho, N. Herber, M. Kroesen and C. Chorus, *Transport Reviews*, **41**, 556–577.

33 A. Austin, C. Bucknor, K. Cashman and M. Rockeymoore, *Stick Shift: Autonomous Vehicles, Driving Jobs, and the Future of Work*, Center for Global Policy Solutions (2017).

34 D. Vrščaj, S. Nyholm and G. Verbong, *AI society*, **35**, 1033–1046.

35 C. Bloom, J. Tan, J. Ramjohn and L. Bauer, *Thirteenth Symposium on Usable Privacy and Security*, **357-375**, year.

36 D. Hawley, *J.D. Power*.

37 *Highway Statistics Series Highway Statistics 2021 Table DL-20*, Federal Highway Administration.

38 Connected, *Automated Mobility 2025: Realising the benefits of self-driving vehicles in the UK. Centre for Connected and Autonomous Vehicles*.

39 M. Akbari, K. Lankarani, S. Heydari, S. Motevalian, R. Tabrizi and M. J.M.Sullman, *J Inj Violence Res*, **13**, 69–80.

40 S. Karnouskos, *Cogn Tech Work*, **23**, 659–667.

41 B. Przybylska-Czajkowska, *Silesian University of Technology Organization and Management*, **183**, year.