Autonomous Driving Technology and Privacy Issues

Peng Yu, 46635884

Data7002 Individual Essay

Introduction

The continuous improvement of human productivity is inseparable from the full application of tools. From horse-drawn carriages to steam engines to automobiles is the liberation of human mobility. It is precise because of the unremitting efforts of human beings to pursue the liberation of mobility, autonomous driving technology has begun to be widely used and developed. But the ensuing problems are also unavoidable, that is, data security and privacy security. The autonomous driving system is more like artificial intelligence. The system will collect the driver’s personal information to learn driving habits and record the starting and ending points of the trip. At the same time, the high-resolution video will be captured while driving. Imagine that when autonomous driving technology is fully applied, massive amounts of data will be generated every second. How to ensure that these data are safe and the protection based on user privacy has become a problem that must be faced. This article will discuss the privacy issues of autonomous driving from the moral, legal, and technical levels. And to assist with relevant examples to prove our argument, describe how to do reasonable and legal data use, avoid illegal data disclosure and improper data use.

Keywords: Autonomous driving technology, artificial intelligence, big data, privacy protection, data security.

Moral level:

First of all, I hope to discuss this issue from the moral level.

At present, the autonomous driving technology we know mainly collects the personal information of the driver, such as name, gender, age, occupation, home address, company address, and phone number. Secondly, it will collect all the starting and ending points of the driver's journey, the reason is to plan the route reasonably. The reason for recording the surrounding environment during driving is to better train the autonomous driving model by learning the surrounding environment. So at this time, the question is, does the driver know that his information has been collected? Who collected it? Where is it stored? Has the data been misused? Unfortunately, most users know nothing about it. The collection and use of unknown data is itself an ethical dilemma. The autonomous driving system collects massive amounts of information every second, with the purpose of making the system "smarter" through the collection of data. The ultimate goal is to provide customers with better services. However, in the process of collection, users' private information may be unintentionally collected. Should the collection of data be stopped? Obviously not, the existence of this kind of conflict, in the final analysis, is that the system does not have the ability to filter and collect data.

Another ethical dilemma of autonomous driving technology is that autonomous driving will only follow the rules it has learned to drive. For example, a pedestrian is running a red light to cross the road. If it is a human driver, he will not choose to hit it, but AI The choice may be to drive according to the traffic rules. Who should be responsible after a car accident in autonomous driving? The universal adaptation pursued at the moral level often hopes to obtain the most idealized result. It seems to be the mistake of pedestrians but morally tends towards the weak. In other words, ethics cannot solve such problems, because ethics cannot quantify accident liability.

Since morality itself is produced by humans, whether it is data collection or driving rules learning, AI is behaviour without any tendency. When ethics cannot be imposed on AI, the ambiguity of responsibilities will make the whole event very complicated. In my opinion, morality cannot be used as a criterion to define right and wrong, because morality itself does not speak right and wrong, and only has a corresponding position for specific things. For example, the collection of data does not infringe on privacy, and AI is morally believed to be correct. Once the data collected by AI involves sensitive user information, AI will be morally condemned. This is actually unfair. Or in other words, when a pedestrian runs a red light, it is the pedestrian who made the mistake, and the accident that the vehicle hits will be morally condemned. In order to avoid this situation, some autopilot companies choose to let AI perform emergency braking in this situation, or make emergency avoidance. This may put the driver in danger, and morality will still condemn such behaviour. Morality is perceptual, while AI is rational. These are two things that are incompatible with each other. Neither can be imposed on each other, but both are actually serving one goal, so seeking a balance between ethics and AI has become a hot topic. Only AI that can work well while taking into account ethics is the technology that humans really need. The so-called moral dilemma stems from the lack of technology and the flaws of the law. When the law quantifies right and wrong, and technology guarantees that the basic morality will not collapse, it is a mature project that can be put into use. This is why it will be mentioned later that Australian law has always been cautious about autonomous driving.

To sum up, the ethical dilemma of autonomous driving technology comes from a problem, that is, autonomous driving technology cannot quantify responsibilities morally, and ethics cannot provide a solution to this dilemma. This is what I am going to talk about next, legal tools and technical tools.

Legal aspect:

Based on the two ethical dilemmas mentioned above, I will give a legal solution and possible solutions from a legal perspective. Law, as a tool that can quantify right and wrong, must be implemented under the premise of ensuring fairness and justice. This is also the reason why problems that cannot be solved on the moral level can often be answered in the law.

The first is the first moral dilemma. Autonomous driving needs to collect massive amounts of data to train AI, and it will inevitably infringe on the privacy of users. I found some relevant regulations from the description of privacy principles in Australian law. First, Australia requires APP entities to manage personal information in an open and transparent manner. In other words, after autopilot operators collect user information, all data usage must be open and transparent. This regulation ensures that even if customer sensitive data is collected, there will be no data abuse. At the same time, the supplementary regulations also mention that entities must comply with the Australian Privacy Principles or inquiries and complaints of such codes. In other words, customers can complain about the abuse of their sensitive data to protect their data security. Secondly, the legal regulations also mentioned that APP entities must have clear privacy policies, and all users have the right to understand their privacy policies. In this way, before users use autonomous driving technology, they can read the information that the company claims will collect and the way in which the data will be used in the future. Only after agreeing to the company's privacy policy can the autonomous driving technology continue to be used. Finally, the legal regulations also mention the handling of sensitive information. If the APP entity is an organization, the entity may not collect personal information unless the information is reasonably necessary for one or more functions or activities of the entity. The regulations clearly state that entities shall not collect sensitive information from users for any reason other than training AI. This ensures that the user's data will not be misused or maliciously disclosed.

The second is the second moral dilemma, which is the division of responsibility for autonomous driving accidents at the legal level. Currently, South Australia has enacted laws that allow driverless vehicles to conduct road experiments. It can be seen that Australia is also very cautious about autonomous driving technology. All autonomous vehicles need to be tested on closed roads in accordance with experimental guidelines, and they need to request preliminary instructions from the exemption bill, law, or standard, and evaluate the road value based on the test results. Possibility. For vehicles that are evaluated as qualified, the first stipulated by the law is insurance measures. Drivers using unmanned driving need to pay valuable insurance for the vehicle and themselves. At the same time, there are strict restrictions on the exemption time for vehicles. In addition, for any accidents caused by the driver's use of autonomous driving during the exemption period, the driver shall bear the responsibility and impose a fine on it. If the circumstances are serious, the driver will also be prosecuted. In view of the fact that the current automatic driving is more assisted driving, that is to say, the driver has the ability to manually stop the accident before the accident, so the driver also has to bear legal responsibility. From this, we can find that Australia takes a conservative attitude towards the popularization of autonomous driving technology, and it is the car owner who is mainly responsible for the partially exempted experimental autonomous driving technology. However, I believe that with the maturity of autonomous driving technology, the law will also make adaptive changes. It is understandable that the current autonomous driving technology is not recognized and trusted by the law due to its uncertainty.

Next, I will start my technical discussion on these two issues. The main purpose is to give the possibility of dealing with moral dilemmas and legal restrictions from the technical level, so as to give more possibilities for the development of autonomous driving technology.

technical level

The current immaturity of autonomous driving technology has led to its severe moral and legal restrictions. I think the main reasons for the immature autopilot technology are the following. First, the autopilot technology AI is not smart enough, and the main task is to use a pattern recognition method to complete the work. The second is that the sensors of autonomous driving technology are often meaningless to collect data. As long as the car owner activates the system, the data will be collected continuously, but in fact, the collected data is often invalid. There is no training and learning for AI. The key role. The third is the interaction of current driverless technology with other cars during driving, which is unsafe. There is a risk of data leakage and attack. Below I will give an example and demonstrate each of these three points.

Regarding the first point, autonomous driving technology is not smart enough. I think it is mainly reflected in three points. First, the autonomous driving technology will only learn rules mechanized, rather than adapt to changes. For example, weather forecast data collected by autonomous driving shows that it will rain today, and the road needs to be slowed down when the road is wet and slippery. But in fact, it didn't rain today, and the slow driving of autopilot is meaningless at this time. A smarter AI should combine the collected information with the actual situation sensed by the current sensors, and jointly give the results of the analysis. If it is different, everything should be based on the real-time data collected by the display sensor. This can also solve the problem of pedestrians running through the red light mentioned earlier. When the sensor returns the result that there is a pedestrian, even though it is currently a green light, an emergency brake should be used to avoid the pedestrian. When the realization of such technology becomes possible, the full application of autonomous driving technology will be possible. The second autonomous driving technology does not know whether the data is sensitive data or collectable data. As mentioned earlier, the suppliers of autonomous driving technology have their own privacy policies, so the privacy policies based on satisfying legal requirements should also be learned by AI. The data should not be collected at all. For some sensitive information but need to be learned, the data can be temporarily stored, and the data can be completely deleted after a certain period of time. In this way, infringement of user privacy is avoided. The last manifestation of not being smart enough is that the current automatic driving has a set of incomplete auxiliary driving rules. When automatic driving is popularized and all vehicles are automatic driving, there needs to be an AI that can completely replace humans to drive.

For the second point, the sensor collects a lot of invalid information, wastes a lot of storage resources, and consumes a lot of invalid learning. Let me make an analogy. We learned the word "apple" today. We know the spelling of this word and its appearance. So do we have to repeat this study every time we meet Apple? The answer is obviously no. Only when we learn that apples are red, and one day we see yellow apples, do we need to do a second study. Autopilot is the same. Take traffic lights as an example. Usually, AI learns only to stop at a red light, go green, yellow light and so on. One day the signal light is out of power, but AI thinks there are lights here, so AI sensors are only needed at this time. Fully open, to conducting a comprehensive study of the situation without signal lights, to facilitate the future to deal with similar situations. The advantage of this is that a large amount of invalid information can be filtered out, which greatly saves the space for storing data and the time for invalid learning. The greater advantage is that to a certain extent, it also reduces the false collection of some unconsciously sensitive information.

The last is the interaction between different autonomous driving AIs. During the driving of the autonomous car, the sensor will recognize nearby vehicles and collect and identify the other’s vehicles. For example, a narrow road can only At the same time, through two small cars or one large car, the autonomous driving AI needs to recognize whether the opposite vehicle is a large vehicle or a small vehicle, so as to make a judgment to continue driving or stop and avoid. If it is an ambulance or a police car that is going out of the police, it should be unconditional Judgment of avoidance. In the process of vehicle interaction, the sensor will inevitably collect some sensitive information about the opponent's vehicle. It's hard to say whether this is good or bad. For example, if the current AI recognizes that the opponent's vehicle is a small car, and we are currently driving a large vehicle, the opponent should avoid it, but if there is a pregnant woman in the opponent's car, what about giving birth? From a moral point of view, letting the other party go first may save two lives, but from the cold AI judgment, there is no morality. In this way, a moral dilemma that is difficult to reconcile appears again. It is not about the law, but it violates moral requirements. Another situation is that in the process of vehicle interaction, the sensor may shoot and transmit the high-definition photo of the other driver. According to Australian law, if the photo is not maliciously disclosed, the shooting by the sensor itself is not illegal. But what if the collected information is used maliciously? The disclosure of such sensitive information will become uncontrollable. From a technical perspective, at this time, autonomous driving companies often choose to use hypothesis verification methods to deal with. The so-called hypothesis verification is to make a hypothesis on the current situation, called H0. In the current situation, our hypothesis is that the sensor will not leak or abuse the collected sensitive information. After that, the company needs to apply statistical methods to sample from a large amount of data. Under normal circumstances, we think that a small probability event will not happen, but if information abuse or information leakage occurs during the sampling and detection process, it is considered that the sensitive information captured by the sensor will be leaked or abused.

To sum up, whether it is the moral dilemma or legal requirements, technology itself can solve these problems to the greatest extent, but there will be a priority for processing, that is, technology tends to give priority to solving legal requirements because This relates to whether autonomous driving technology can be used subsequently. On the ethical level, requirements are often difficult to judge. For example, when there is a traffic jam at work in the morning, we sometimes choose to let some cars pass courteously. The other party will also beckon to show gratitude. This customary habit is often not understood by AI. AI's processing logic is single, it will only follow instructions to complete the behaviour, and will ignore the moral rules between people. Therefore, only when the technology becomes intelligent enough, from the current pseudo artificial intelligence to real artificial intelligence, that is, when AI can have emotions and thinking abilities like humans, these moral problems can be solved.

Finally, I think the application of autonomous driving technology is inevitable. This is a double-edged sword. The unprecedented development of technology will inevitably bring controversy and contradictions. After the second industrial revolution, the widespread popularity of automobiles has also brought about a lot of moral and legal disputes. As the stability and safety of automobiles are comprehensively improved, new ethical standards will gradually be formed in ethics. The law will build a complete set of laws and regulations to protect human rights. When we are facing the third industrial revolution, it is now the information revolution. The main feature is the explosive growth of data, making various fields full of unknown possibilities. In my opinion, autonomous driving technology is a typical embodiment of the information revolution, not only the improvement of the technical level but also the continuous exploration and efforts of human beings for a better future. But we must also remain vigilant. More and more data problems have made modern people ‘naked’. In the face of big data, a person’s emotions, sorrows, sorrows, and relationships are all at a glance. Protecting data security and protecting human privacy are always the basic rights and interests that any technology must respect because any technology, ethics, or law ultimately serves people.

References

https://www.nature.com/articles/d41586-018-07135-0

https://www.theatlantic.com/technology/archive/2013/10/the-ethics-of-autonomous-cars/280360/

https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/

https://dpti.sa.gov.au/driverlessvehicles

https://www.legislation.sa.gov.au/LZ/V/A/2016/MOTOR%20VEHICLES%20(TRIALS%20OF%20NEW%20AUTOMOTIVE%20TECHNOLOGIES)%20AMENDMENT%20ACT%202016\_10/2016.10.UN.PDF

https://medium.com/hackernoon/autonomous-vehicles-and-the-end-of-privacy-9c3712f3494f

https://www.nature.com/articles/d41586-018-07135-0

https://www.theatlantic.com/technology/archive/2013/10/the-ethics-of-autonomous-cars/280360/

https://www.rand.org/pubs/research\_reports/RR443-2.html

https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety