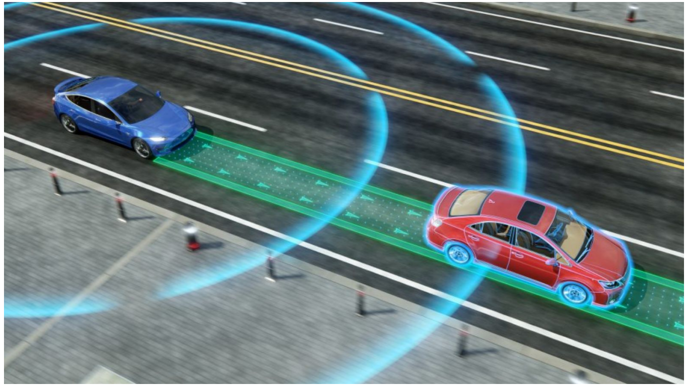
Security and ethics in driverless vehicles

Data Science Master
Cédric Prieels

Autonomous vehicles



- Machine Learning **breakthrough** over the last few years, leading to **automation** and to the development of driverless vehicles
- Estimated **market share** of 1.3 trillion of USD each year, just in the US [1]
- Could be additionally benefic in a number of ways:
  - Saving **lives** by reducing the number of accidents
  - Saving **fuel** and helping the environment
  - Reduce **congestion** and increase productivity
- However, there are still **debatable issues** related to this new technology, mostly:
  - **Privacy issues** with the data collected
  - **Safety issues**, regarding accidents, software flaws and hacking
  - **Ethical issues** due to the emergence of such new technology

Privacy issues

- These vehicles rely on the data gathered by tens of captors to drive safely
- Huge amount of data (~300Tb per year [2]) therefore generated by such vehicles
- Data typically sent to a global server and quite sensitive, since containing information about the position of any given car for example

- However, this debate is not new and customers are **already** (mostly) **protected** against such leaks of personal data
- Anonymization techniques do exist to lower the risks
- 7 privacy principles already published in this sense [3]

Safety issues

- Two main categories: **software flaws/misconceptions and hacking**
- Software flaws
  - Especially important at the beginning, when softwares have not been properly trained or when sensors might experience failures
  - Not much to be done, except **extensive testing**

- Hacking
  - Car-to-car/car-to-cloud communication system mostly **vulnerable**
  - Encrypting and securing the data is an option, but slows down the decision process
  - Road signs can also be hacked [4]
  - Integration of different softwares by different constructors is typically introducing weaknesses

Ethical issues and open questions

- Such cars being expansive, its benefits will be reserved to **richer people** first. Fair?

- Machine learning techniques need **training**. Should we train it mostly against everyday scenarios to avoid accident or teach it or to react in case of an accident?
- In case of accident, who should be saved in priority?
  - Greatest good for the greatest amount of people?
  - Or moral duty principle? The car was designed to keep its driver safe at all cost.

- Discussions already ongoing
  - Age, gender, physical and mental discrimination prohibited by the IEEE
  - Preliminary guidelines already put in place by countries such as Germany [5]

- Is the loss of jobs acceptable for the advantages of such driverless cars?

Conclusions

- Huge and evident benefits for the introduction of such autonomous cars
- However, many problems still need to be solved:
  - Privacy issues, already quite **advanced discussions**
  - Safety issues, **extensive training** absolutely needed
  - Many **ethical dilemma** that still need to be sorted out
  - Liability issues: should the constructor or the “driver” be responsible? Should laws be developed globally or by country?

- As with many innovant technologies, discussions and still needed before introducing these cars globally on the roads.
- Main question to answer: **Is it worth it?**

References

[1] C. Weiss, S. Gaenzle and M. Romer, ”How automakers can survive the self-driving era”

[2] A. Chaturvedi, ”Implications of data privacy once autonomous vehicles hit the roads”

[3] Autoalliance, ”Privacy Principles for Vehicle Technologies and Services”

[4] K. Eykholt et all., ”Robust Physical-World Attacks on Deep Learning Visual Classification”

[5] C. Lutge, ”The German Ethics Code for Automated and Connected Driving”