Mandatory Policy for Road Safety and Security

Introduction

Can you imagine a time when seat belts were not required to be fitted in cars by manufacturers? Only 50 years ago, in 1968, the United States mandated that all vehicles be fitted with seat belts [1]. According to the Journal of Economics, "mandatory seatbelt laws significantly reduced traffic fatalities and serious injuries resulting from fatal crashes by 8 and 9%, respectively" [2]. As we can see from this example, government intervention through mandatory policy saves countless lives. The seat belt however only kicks in after an accident happens. When it comes to driver safety, there are much more elegant solutions now that can prevent an accident from happening in the first place. However, these features are what seatbelts were in the past - unregulated and not required.

What causes these accidents is well explained by the old joke that “the most dangerous component in a car is the nut behind the wheel" [3]. It is however no joke when about 90 percent of the car accidents are caused at least in part by driver error [4]. Currently we are striving to eliminate the role of that most dangerous part of the car (driver) by relying more on technologies such as Artificial Intelligence (AI) and Internet of Things (IoT) [4]. Such an AI system is much more reliable as it is not affected by alcohol or distracted by texts. However, it does have its own set of challenges in building it which is why it isn’t completely commercially available yet. Challenges arise because the technology itself isn’t mature yet, is vulnerable to security breaches, there is lack of policy regulation and uncertainty about acceptance. If the United States government wants to address and mitigate impending security threats from self driving
cars, action must be taken. This action must happen on three pillars, technology, industry, and policy.

**Supporting Detail**

Between a manual transmission seat belt car to the fully autonomous self-driving car exist several more levels of car autonomy [5]. Even though the fully autonomous car remains a relatively distant dream, we will continue to see more and more byproducts of this autonomous car dream get into production.

Most in-use systems today can warn you of a non-ideal driving scenario. Examples like blind-spot alert in the side mirrors, lane departure warning, forward collision warning, etc. are available today and even in the non-luxury car segment [6] [7]. As technology matures, we will see these systems take over control of the car if it is in danger (e.g. driver sleeps behind the wheel) rather than simply warning the driver. There is no doubt that these systems are useful and well accepted when it comes to driver safety. But, because of the potential of these life saving technologies, it is easy to see why these future systems will become the seat belt equivalent today - mandatory. However, once the people are not given a choice in adopting a technology, the full extent of that policy must be discussed. A decision of making the seat belt mandatory required thinking about the economical implications, industrial readiness, political lobbying, etc. However, technologies that enable the modern safety features are not as straightforward as the seat belt. The additional concern is that they continuously consume and process data, are mostly probabilistic (as opposed to a mechanical instrument) and shockingly, bound to be hacked and used against its purpose of safety. These concerns are valid as we constantly see industry leaders falter in the ways their tools are being used.

AI and the connected world are relatively new tools for humanity, and the full implications of it we still do not have a good grasp of. Things that have gone wrong in the past with the then nascent technology, like the internet and websites, demonstrate that being concerned about its safety is warranted and warn us about things that could
go wrong with AI, and specifically autonomous cars, the today’s nascent. For example, it was probably unforeseen that a website meant to connect people socially would cause deaths in Mynmar [8]. Or, that a company meant to distribute credit in the USA in a systematic way would be hacked to access personal information of the general public [9]. These are two examples of an “unforeseen misuse” and “foreseen but not effectively prevented misuse” respectively. They are both related to the category of concerns about the use/misuse of technology.

A second category of concerns comes with the technology itself being imperfect in the way it is built. It wasn’t until recently that researchers began to notice that most of AI are biased in several ways. A recent article showing how a darker skin person is more likely to be hit by an autonomous car stands as an example to that [10].

To complicate things further, technology is built in a compounded way i.e. different imperfect pieces rely heavily on each other and the fall of one may cause a domino effect leading to a disaster. For example, in a world where cars see and talk to other cars to decide the best driving strategies, the reliability and integrity of the underlying communication network is critical.

A step further in that direction would be the power grid that underlies all of these systems as it too has been vulnerable to attacks [11]. AI safety features in cars are optional for use today. When signing up for them, the user is expected to accept the possibility of these risk and then decide if they still want to sign up for it. However, once the use of these technologies are mandated the users have no choice and have to use it even if they are not okay with the risk. While agreeing that mandating sophisticated safety systems in cars would make driving much more safer, we explore the considerations that one must make before doing so.

**Regulations**

The technical progress of self driving cars is growing exponentially, but the regulation that governs and rules the technology that will transform urban mobility is hardly progressing linearly. While companies are constantly testing their self driving
system in their private settings, in order to learn the system behavior in real life, testings must be done among public traffic where various actual transportation scenarios happen. Thorough regulations that run through the entire lifecycle of the self driving cars from their developing stage until they’re deployed on the road needs to be established. Among the states, Nevada was the first state to authorize the operation of autonomous vehicles in 2011. Since then, 21 other states have passed legislation related to autonomous vehicles. Governors in Arizona, Delaware, Hawaii, Idaho, Maine, Massachusetts, Minnesota, Ohio, Washington and Wisconsin have issued executive orders related to autonomous vehicles.[12] However, there are several issues still in need to be addressed.

While the U.S. Department of Transportation and NHTSA periodically update their guidelines for autonomous vehicles, individual states are already passing relevant laws. However, they differ on basics like the definition of “vehicle operator.” Tennessee SB 151 points to the autonomous driving system (ADS), while Texas SB 2205 designates a “natural person” riding in the vehicle. Meanwhile, Georgia SB 219 identifies the operator as the person who causes the ADS to engage, which might happen remotely in a vehicle fleet. These distinctions will affect how states license both human drivers and autonomous vehicles going forward.[13]

Similar issues will be brought up when it comes to decide the responsibility of an incident. Detailed regulations need to be made regarding who is responsible in every possible scenarios. Flaws of the manufacturer, the driver or the design of system are all potential causes of an incident. Failure to clearly identify whether the problem is manufacturer level or consumer level would make it harder to solve the issue and make compensations.

Possible suggestions for manufactures are to make mandatory patching system on all models on the market in a timely manner based on the existing comprehensive instruction and training process of the driving system. Users have to update their software in the most updated and secured version in order to operate.
On the other hand, self driving systems generate enormous amount of data throughout their lifecycle. The usage and storage of these data need to be regulated as well. Of the three aspects of the CIA triad, the priority of integrity and availability of data should be higher than the confidentiality. Though the privacy issue of the location and communication data of the vehicle needs to be addressed, the other two aspects that lead to safety problems requires immediate attention. State-of-the-art security and manufacture standards should be maintained with the collaboration between all involved parties. They need to ensure the integrity of the data couldn't be compromised and cause safety hazard, and they must only be accessed by verified stuff and personals. The vehicle inspection process must be overhauled to account for the fitness of these new technologies, which are a combination of complex sensors and actuators.

**Necessary Infrastructure**

The infrastructure to support this connected and autonomous system needs to be implemented on a broad scale. Technology, policy, and industry infrastructure must support these road safety regulations in order for them to be successful.

In an autonomous system, technology tries to keep passengers safe, one example is by not allowing cars to speed. However, new issues arise when that system is also connected. For example, if a system has a subpar security system, a malicious hacker can compromise the system and change the speed putting the passengers and others on the road at risk. This example is just one of many vulnerabilities in an autonomous and connected car system.

Does an adequate technological solution to keep drivers and passengers safe on roads with connected and autonomous vehicles exist? If not, additional security research needs to be prioritized to ensure safety on our roads. This technology needs to address the key issues with a connected and autonomous system including integrity and availability threats.

Once there exists a solution for these security issues, this solution needs to become the industry standard. Experts and leaders would need to collaborate to
recommend the most secure solution. Industry automobile makers would then need to adopt and standardize those recommendations to be used in manufacturing. Since security can always be improved, this process should be cyclic so the industry can consistently have the most secure system.

Policymakers need some way to regulate and enforce this. To regulate these security measures, a federal law needs to be in place. State laws would not be effective in dealing with this issue, because manufactures are nationally and even internationally based, and having dozens of varying guidelines would lead to confusion and lower-quality systems. Having a federal law will establish a standard for manufacturers and for the overall safety on the roads. After this strong, thoughtful legislation is in place, an existing federal government agency would enforce the legislation. Ideally, this agency would be the Federal Motor Vehicle Safety Standards (FMVSS). The FMVSS is already responsible for enforcing safety standards on the roads and in manufacturing. As the connected and autonomous car system becomes a reality, FMVSS's responsibilities should be expanded to address those safety concerns.

**Metrics of Success**

Clear and unanimous metrics to determine whether the current regulations are successful enough are unclear given the lack of maturity of this area, but could be considered from the following aspects. Since self driving cars are supposed to rise the safety level of public transportation, the trend of incidents rate on traffic report is able to indicate whether the regulations have made improvements. Death rates and injuries should also be taken into consideration and whether the relationship between the issuing of the policies and these rate are a correlated one or the policies is really the causation of declined injuries for example. Also, the number of records of violations of these regulations can be taken as a main indicator as more successful policies will prevent these violations.
Next Steps

- To mitigate the technological issues created by self driving cars, more security research should be pursued. Specifically, this research should address the integrity and availability threats and focus on road safety.
- To address the industry and policy issues, the federal government could organize a task force or special committee consisting of security experts, automotive industry experts, autonomous driving experts, and lawmakers interested in creating policy surrounding this issue. Ideally, this task force or committee will be bipartisan. In order to have a productive and effective group everyone involved should put aside their political differences and focus on keeping their constituents safe on the roads.
- To effectively enforce this policy, discussion around how the FVMSS could expand to accommodate the additional responsibilities created by autonomous and connected systems should also happen.

Conclusion

The report summarizes how technology has continually advanced to keep drivers safe on the road. This report argues that while such technology is useful and must be adopted, the pitfalls of it need to be considered first. In order to do that, we have outlined several solutions that could be summarized into three categories - increased investment in security research, collaboration within the industry, with the government and academic institutes.

In order for consumers to continue to be kept safe on the roads, just as mandatory seat belts have helped keep drivers and passengers safe, policy makers and industry experts need to start laying the groundwork for regulatory policy and infrastructure to support autonomous and connected vehicles. Action needs to be taken now, so the consequences of connected and autonomous cars are minimized, and citizens are kept safe.
References:


