Private Autonomous Vehicles

The compatibility of privacy regulation and innovation in autonomous vehicles

Student Name: Maximilian C. Mathysen Gerst
Student Number: 365958

Supervisor: Dr. Payal Arora

Master Media Studies - Media & Business
Erasmus School of History, Culture and Communication
Erasmus University Rotterdam

Master's Thesis

Private Autonomous Vehicles

ABSTRACT

Due to the ever increasing interconnected and data collecting world the modern consumer is presented with, the notion of privacy is a topic that is often discussed within current academic research about media studies. The argument often made in academia that the notion of privacy is presented as a trade-off with innovation in the modern technological world and is seen as a limitation to the furthering if the technological progress that modern society is pursuing. As a means of addressing the current concerns within the topic of privacy and a digital world, the European Union has introduced new regulations to enforce more control over what data is collected, stored and process in and effort to ensure privacy of the user of these technologies is not only improved upon but restored with the European Economic zone through the implementation of the General Data Protection Regulation (GDPR).

The main research question driving this thesis thereby is: To what degree is privacy, through GDPR, compatible with innovation in AV's? This leading research question seeks to create an understanding of how both technology and privacy regulations could be introduced within a modern technology filled life and designed to create a far more secure and inclusive society. GDPR, a set of regulations enforced by the European Commission, is a regulatory measure developed to control the processing by and individual, a company or an organization or personal data, relating to individuals within the EU. By using the AV sector as a lens, this thesis hopes to contribute to the current understanding of how autonomous vehicles remain pioneering while at the same time continue to develop the technology, ensuring at the same time, privacy is maintained. A qualitative content analysis, based on online material published by five primary stakeholders, was conducted to seek a middle ground, and through it this thesis identified four main patterns in the compatibility between AV technology, privacy and how the GDPR could complement both. The first pattern involved the concept of trust. Trust is a vital pattern that the stakeholders have identified and is a reoccurring pattern as a result of this study of online content. The second pattern identified with regards to consent, which echoed the theoretical background, and where in which GDPR plays a vital component as it explicitly requires the consent of the user. Thirdly, transparency and public information was identified in answering the research question. Data collection must be transparent and finally, the fourth pattern revolves around ethical dilemmas, which shows that contrary to contemporary academic debates, ethical dilemmas, or so-called 'trolley cases,' are not required for AVs.

KEYWORDS: Privacy, Innovation, GDPR, Autonomous Vehicles, *Technology*

Table of Contents

1. Introduction

1.1 Background

For thousands of years, humans have been seeking to develop means of transportation over land to allow humans to travel quickly and safely over ever-increasing distances. Innovation in transportation has seen several major shifts historically. Previous major shifts include the domestication of animals allowing them to be used as means of transport in combination with the development of the wheel, carriages and wagons. Later on, transportation methods shifted to rely on steam and coal powered transportation devices which provided major enhancements in the speeds of mobility and transportation bringing a new dimension of efficiency to the industry. Fossils fuels shifted the industry once again as they provided advancements in speeds and efficiency.

Currently, society is at the forefront of the latest, major shift in the industry where the advances in communications technology and Internet of Things (IoT) applications will allow the future of transportation to extend beyond human control for the first time, as current developments are shifting towards a world where one could hand over control to a computer presenting a new perspective on transportation. “I’m so done with driving,” was what a car owner stated to a prominent newspaper which reported the responses of people watching a steering wheel turn by itself as a person sits idly behind it (Rushe, 2018). For example, with the push of a button on a smartphone, a vehicle will find a place to park or drive other people around as a taxi service to cover the vehicle ownership costs. Features such as these are often described within mainstream media as a concept known as autonomous vehicles (AVs) and is far closer to reality than most consumers think (Litman, 2017). Some suggest that the real-world application of AV technology is distant, however recent studies imply that AVs could play a role in daily life and is merely one decade away (Davies & Marshall, 2019). Other experts predict experts predict that new automobiles will be capable of driving themselves and transition to AV’s under limited conditions in as soon as 5 to 10 years from today, and under most conditions within 10 to 20 years. (Wadud, MacKenzie, & Leiby, 2016). This indicates that the shift in the current understanding of mobility and transportation due to AV technology is soon to arrive within modern society.

Furthermore, many real-life examples of the applications of AV technology showcase more accurate representation of the capabilities and benefits of the technology, AVs are now considered one of the most significant areas of technological progress and development that could fundamentally alter transportation solutions known today (Fagnant, & Kockelman, 2015). AVs are central topics debated by stakeholder groups focused on automotive innovation, including legislators, watchdogs, manufacturers and others, by promising improvements in safety on public roads by deterring fatal crashes, offering critical mobility to new market segments such the disabled or elderly, increase road capacity, saving fuel, and lowering emissions (Fagnant, & Kockelman, 2015; Litman, 2017).

Unfortunately, the current representation of AV technology is currently facing challenges, particularly as some media representation and stories published on public opinion is generating skepticism (Litman, 2017). The fear brought by news stories of early versions of AV technology malfunctioning, or freak accidents presented in the mainstream media exhibits the public interest in the topic, however the media coverage of incidents involving AV's is currently constructing a dystopian narrative in the popular news media. For example, significant public debate and re-evaluation of the idea of AVs was sparked when an Uber car containing AV technology was involved in a fatal accident when the AV failed to recognize a pedestrian crossing the road in front of the vehicle (Kohli & Chadha, 2019). These events risk negatively affecting public opinion, hindering the speed of adoption of the technology, resulting in a risk of developmental slowdown of AV technology and implementation into day-to-day life. Many of these concerns and safety fears must be addressed with the introduction of this new technology before autonomous vehicles can become available to the general public (Litman, 2017).

One major aspect of the development of AVs concerns digital privacy and the collection of data of users of AV technology. This is a wider discussion that revolves around digital privacy and innovation in technology, of which AVs constitute a part of. Digital privacy has indeed become an addition to the modern concerns of users of innovation and to the modern world as we know it today. Within current modern society, and in many aspects of technological innovation, digital privacy has become a central to the development, design, and regulation of digital platforms. The notion of digital privacy itself has been debated in academic, policy, and public fora, including on the implications of the impacts it has on daily life and the continued development of technology. For example, a crucial business and policy dilemma worldwide concerns the notion of "big data," which are extensive data sets generated by the content and information shared by technology in a broad range of industries, including AVs (Lari, Douma, & Onyiah, 2015). Big data relies on the analysis and storage to gain knowledge. However, the innovation of gathering "big data" seems to come at a cost, namely through the privacy of users of these new technologies.

1.2 Aims & Relevance of the Thesis

Academic research has focused on this debate between the trade-off of privacy and the opportunities of innovation (Goldfarb & Tucker, 2012; Cohen, 2012). These debates have focused on how the furthering in innovation comes at the loss of privacy. Researchers have studied the effects of these the ever-present tradeoffs in innovation and privacy in forms such as IoT devices.

As a way to address the current concerns and debates on privacy and the digital world, the European Union (EU) introduced new regulation to enforce more control over what and how data is collected, stored and processed in an effort to ensure the privacy of the user is not only improved upon

but restored. The newly introduced General Data Protection Regulation (GDPR), developed and proposed by the European Commission, sets out to control one fundamental principle, namely to establish who has access to their data and what is done with this data, pursuing to bring control back to users' hands (GDPR, n.d.). The GDPR regulations, developed to normalize the processing by an individual, a company, or an organization, of personal data within the EU.

Thus, this thesis will seek to bridge the academic debates on privacy and innovation with regards to the newly created policy on GDPR. Specifically, it will focus on the current debate surrounding AV technology and privacy, and the adaptation of this technology into society alongside the implementation of the GDPR in an attempt to understand the application of privacy and innovation within the sector of AVs in the EU. The research question the thesis seeks to answer is: *To what extent can the GDPR create compatibility between privacy and innovation in autonomous vehicles?* This is relevant for AVs as they contain many sensors and computing, which enhances their data gathering capability and could result in ever more data collected and analyzed (Chui et al., 2010). The flow of information provided by AV's consequently creates an inherent privacy risk (Goldfarb & Tucker, 2012; Cohen, 2012; Litman, 2017; Chui et al., 2010). This thesis will aim to provide an understanding of the implementation of legislation such as GDPR as a way of establishing neutral ground and gaining insight into how both AV technology and privacy can both be enjoyed by users.

This is a particularly significant point of discussion since AVs will be capable of spawning a substantial amount of data on operators' travel habits, including information on GPS location, speed, traffic, weather conditions, and road conditions, as well as information about other road users (Litman, 2017; Lari, Douma, & Onyiah, 2015). Furthermore, in assessing the GDPR legislation, which aims to provide a legislative step into restoring privacy rights to users, the thesis will seek to address a research gap by showing different stakeholder perspectives on how privacy through the GDPR legislation can be compatible with innovation in AVs.

Furthermore, this thesis has wider implications, particularly within the debates of the notion of privacy in academic media studies in a world of increased innovation and data collection.. The thesis aspires to address how innovation and privacy can remain pioneering while continuing to ensure privacy remains upheld and the user remains protected. As Litman mentions, stakeholders seek to maximize both innovations as well as privacy and a balance must be obtained (Litman, 2017). Through the lens of AVs, the compatibility of innovation in technology and privacy regulation could be applied to multiple other technological sectors that revolve around interconnectivity and data collection. In addition, the use of AV technology as a lens in this research is due to is popularity in mainstream media and its dependence on gathering "big data" for its development and operation. Thus, the research aims to utilize media sources as a primary gathering tool in its assessment of the compatibility of privacy and innovation. As mentioned, AV technology is a useful case in highlighting the trade-off between

innovation and privacy associated with adoption of new technologies, and thus a beneficial point of assessment in how regulation such as the GDPR can impact it.

1.3 Structure of the Thesis

To address the main research question, the thesis will shine light on both conflicting elements discussed by addressing multiple sub-questions. Firstly, in order to gain insight into the nuances of what parts of the GDPR affect the AV sector, the research will aim to discuss *Which GDPR regulations are directly affecting innovation within the AV sector?* Secondly, to understand the social issues at play and to picture what the effects of the GDPR are on the AV sector, another sub-question is utilized: *Who are the stakeholders in the AV sector and how may they be impacted through these new regulations?* The third sub-question *What diverse perspectives are circulating around the globe regarding AV innovation and privacy concerns*? aims to bring to light the various concerns amongst different stakeholders and regions while attempting to understand the multiple AV stakeholder perspectives influenced by the introduction of GDPR. For AVs to be embraced, and a global, mass-market phenomenon, perceptions and worldviews of the full range of stakeholders and regions are involved in this process discussing the affordances and constraints of these technologies.

Following this introduction, the following theoretical background will provide detail insights into the main societal and academic debates at play. Including the main technological shifts, the field and gamechangers, as well as the main drivers for concern and threats while concluding with strategies to address those threats. The following session will detail the research methodology, including the reasoning for the qualitative research approach data, collection and analysis. Findings as well as conclusions and discussions will provide answers to the research question.

2. Theoretical Background

This chapter will discuss the theoretical background and the academic debates surrounding privacy and AVs. This discussion will serve as a backdrop in understanding the current available debates on innovation and privacy, but also provide a detailed understanding of AVs. This will allow the thesis to provide a backdrop on understanding the impact of regulation such as GDPR on AVs and provide a theoretical understanding of the debates surrounding the issues of the divergence or convergence of privacy and innovation.

It will first provide a backdrop of technological shifts in the automotive industry. It will then provide an overview of the evolution of IoT and AV technology, and discuss the current debates on AV technology, including the main concerns and drivers of AV technology. Finally, it will provide an overview of GDPR and the current available debates surrounding GDPR and AV from a policy perspective. This discussion will serve as a backdrop to demonstrating the main drivers for concern in the fields, followed by the negative effects of AV's and the strategies to address these negative effects.

2.1 Technological Shifts in the Automotive Industry

Human society has always been on the move. From the era of hunters and gatherers to colonization and globalization, humans have continuously had the urge to remain mobile and to find better habitats to live. In the past, there was a physical need to do so from a survival perspective, as humans traveled in order to find food and less harsh climates (Sterelny, 2003). In more modern times these primal problems of food and safety have been largely addressed through large scale agriculture and exporting industries. Modern society still has urges to seek for optimized mobility solutions, but in a slightly shifted manner where the pleasure of travel, or productivity gained through mobility is much more of a motivation.

In its motivations to increase mobility, society has also continuously been seeking to optimize transportation solutions that could cover larger distances, arrive somewhere in shorter time, consume fewer resources while always attempting to remain safe. One of the ways to overcome these challenges is through the implementation of smart technology which could allow vehicles to travel faster, safer, and more efficiently.

Since the conception of the automobile by Carl Benz in the early 1890's, the automotive industry has been characterized as a competitive industry. Thus, automotive brands have consistently looking to innovate and find new ways to distinguish themselves from the competition. Although most of the innovations of the automotive industry has been gradual, in recent years, the progress regarding AV technology and its development has been rapid (Anderson et al., 2016) resulting in a transformational

shift in the industry towards ever more optimized mobility solutions changing various elements that the traditional car models present.

In academic literature, AVs are mentioned using variations in wording, and multiple terms describe the concept, resulting in uncertainty regarding the definition. According to Reese (2016), self-driving, autonomous, driverless, automated, and semi-automated are some of the words that are used interchangeably in the literature. In addition, these words are merely more specific versions of the same principles regarding moving a vehicle by utilizing electronic systems (Reese, 2016). First emerging in the 1980s, the experimentation of AV technology is predicted to become the largest innovative jump in technological progress ever seen in the automotive industry (Anderson et al., 2016) and provides major economic implications to the market, such as saving trillions of dollars to the global economy as seen in Figure 1, and societal benefits such as accident evasion, reductions in traffic congestion, higher occupant productivity, and fuel savings (Morgan Stanley, 2013). Thus, the adoption of AV technology is accelerating at a far quicker pace than a natural demand-pull due to the social benefits and economic benefits (Morgan Stanley, 2013).

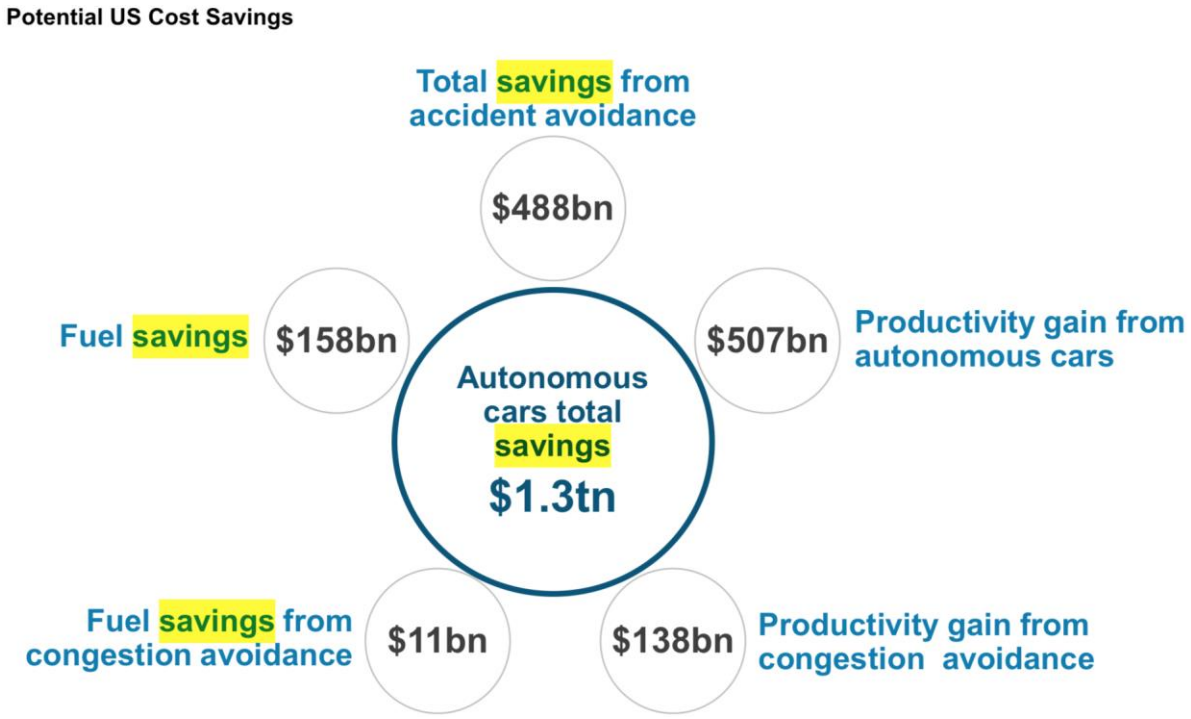

Figure 1: Potential US cost savings: Morgan Stanley research (2013)

As described by Fagnant and Kockelman (2015), AVs have the potential to alter transportation systems fundamentally as automobile manufacturers are using data in order to develop systems that can automate functionalities of automobiles. AV technologies are at the forefront of this development (Gogoll & Müller, 2017) and will take a primary role in the future of travel (Litman, 2017) by averting deadly crashes, providing critical mobility to the elderly and disabled, increasing road capacity, saving fuel, and lowering emissions. Furthermore, complementary trends (Litman, 2017) in shared rides and

vehicles may lead us from cars as an owned product to new ownership models like on-demand services and vehicle sharing. Infrastructure investments and operational improvements, travel choices and parking needs, land use patterns, and trucking and other activities may also be affected (Litman, 2017). Additionally, passenger compartments may be entirely reimagined. Where drivers previously had a cabin focused on vehicle control and driving, with AVs possibilities for entertainment and relaxation arise as watching movies, eating, or socializing can transform the vehicle cabins towards lounges or living rooms (Litman, 2017). Thus, the evolution of AVs constitutes a major technological and mobility shift for humankind.

2.2 The Field of IoT and AVs as Game-Changers

As devices become smarter, academics have initiated the development of theories to study the associated phenomena with these technological innovations, particularly with regards to data collection and the consequences of such. In today's world, data is consistently generated as part of our interconnected, internet-enabled, media- and information-rich lives (Lari et al., 2015). Automobiles are no exception in this regard, with traveling now being monitoring and inter-connected to allow mobility users to remain knowledgeable and updated on driving conditions, traffic, and vehicle maintenance.

The tenacity of enabling vehicles to be part of a connected society and continuously have the ability to share information is described under the term Internet of Things (IoT). The Internet of Things (IoT) has been defined in several different ways by scholars since the conception of the term. According to some scholars, the term describes the ability for technology to remain interconnected in distinctively recognizable and intelligent computing devices with an existing internet infrastructure (Holler et al., 2014). IoT has been central to many scientific debates and for other scholars is considered more of a general term describing the interconnectivity of smart devices connecting the digital and physical world (Ray, 2018). However, latest research finds a consensus that the IoT enables physical objects to be linked to the virtual world, ultimately constituting a global network (Mattern & Floerkemeier, 2010; Uckelmann et al., 2011; Vermesan et al., 2013) of interconnected devices.

AVs implement IoT technology in vehicles as elements of connectivity are often installed, including data collection capabilities and embedded internet connectivity. AVs are in essence systems that allow automobiles to function without the dependence on a driver and is one of the premier examples of IoT technological applications (Krasniqi & Hajrizi, 2016). Thus, AVs are capable of generating massive amounts of delicate, personal data on user travel habits, including data such as GPS location, speed, traffic, weather conditions, and road conditions, as well as information about other road users around the operator. AV systems today rely on technology to keep the vehicle occupants safe and the car on the road through a combination of sensors, cameras, radars and lasers that build up a representation of the vehicle surroundings resulting in the ability to act upon concurrent on-road

situations through the gathering and processing of the data collected by the vehicle (Litman, 2016). Sensor technology is a showcase of IoT as all of the sensors must interconnect and communicate, with one another, to facilitate the car to drive safely (Krasniqi & Hajrizi, 2016).

Furthermore, automotive original equipment manufacturers (OEM's), like BMW, Mercedecs, Toytota and others, are already implementing automated systems and IoT data into vehicles today and as a result, are collecting ever more data (Albrecht, 2016). Academic literature estimates a magnitude of growth in the world's data generation from about four zettabytes in 2019, to approximately 40 zettabytes in 2020 (Adshead, 2014). With such vast quantities of generated and stored data, new challenges arise regarding the protection of this data. Not only will new technologies and algorithms for processing and storing data be needed, but also standards for protecting this data. AV technologies are at the forecourt of this development (Gogoll & Müller, 2017) because of the benefits of AV's including, accident savings, fuel savings, congestion avoidance, productivity gains (Figure 1) and will take a primary role in the future of travel (Litman, 2017).

2.3 Main Drivers for Concern in IoT

The introduction of IoT technology into daily life creates challenges or specific obstacles that could threaten the potential of IoT. The majority of risks concern issues regarding security, privacy, standardization. Customers for new innovative technologies including IoT systems are most apprehensive, according to the current academic debate, about the main drivers of digital privacy concerns which are broadly categorized as: 'control' (control of the information after the initial transaction), 'consciousness' (of collection and use), and 'privacy' (protection of the data) (Bélanger & Crossler, 2011; Culnan, & Armstrong, 1999; Sheehan and Hoy, 2000; Malhotra et al., 2004). Another element that is a driver for concern in IoT technology revolves around the ethical implications of the data collection in IoT. The following subsections provide details on these concepts relating to the academic literature on IoT concerns.

2.3.1 Control

Most scholars address the issue of control in the field of IoT and summarize this issue as a user's fear of a loss of control of the information gathered about them. As a result of the data gathering capability through AV's, the tracking of all humans could be made possible, in what literature describes in terms of an opt-in or opt-out transaction (Gudymenko, Borcea-Pfitzmann & Tietze, 2011), where the user of the technology must express enough control in order to have the capability to opt-in or opt-out. For example, if a government would gain access to AV data, this could be used to limit the freedom of citizens by providing knowledge of real-time location information and well travel habits of all citizens. On the flip side, by opting in, a government could also use IoT data in order to develop infrastructures further, manage congestion or optimize city safety. However, the concern remains

whether this improvement in efficiency comes at the expense of human rights (Uckelmann et al., 2011) through the impact it has on a user's privacy. Further concerns arise where data falls into the hands of authoritarian or malicious states where opting out would be no longer possible and the use of this data as a method of surveillance (Van Kranenburg & Bassi, 2012) becomes apparent. The right to remain in control of personal information and the right to remain anonymous must be maintained, so a lack of control over data is a concern for users, but also for the general population and is a result of the omnipresent nature of IoT.

2.3.2 Consciousness

The knowledge for a user being explicitly aware of what and how information is collected on a subject is crucial to tackling the concerns associated with IoT. Users that are aware of the provision of data through the use of connected technology were found to be less concerned with the data collection taking place (Graeff & Harmon, 2002). With IoT ever more seamlessly integrating into households, consumers have begun to lose sight of the technology, and it is not often clear whether a product with IoT technology is collecting data, let alone what is done with this information. In categorizing the degree to which the user is conscious of data collection, Nowak and Phelps (1995) assessed users on a scale in which they were fully conscious of data collection and use to not conscious at all of data collection and use. The debate regarding conscious data collection is amplified when considering that some researchers argue that with regards to data, there is a 'right to be anonymous' (Goddard, 2017). Thus, there is a conflict regarding when users are unaware of the data collection and the use of the data in IoT that needs to be kept in mind, referring to the second and third categories of conscious data collection highlighted by Nowak and Phelps.

2.3.3 Privacy

According to academic consensus, privacy is likely the primary concern of consumers with regards to IoT technology (Park & Kim, 2016). This is due to the highly intimate, omnipresent, non-transparent data constantly collected, which results in the characteristics of fear for IoT systems. The main concern revolves around the protection of the data generated. Consumers are significantly more concerned regarding their privacy when data sharing involves personal information such as information that could be used by external parties, for example insurance companies. Where the concern of control is more focused on whether the consumer has a say in sharing data or not, the concern regarding privacy is more nuanced. The data collected and passed on to other parties beyond the original data collector is a concern. Once it has been established whether data has been collected, the degree to which the data reveals personal information and is shared on to other parties could become out of the control of the original user. Fagant and Kockelman (2015) highlight this issue in a case study on how insurance companies could use data in the applications within AVs. Through IoT, insurance companies have the potential to gain access to data collected directly in a vehicle, monitoring many parameters such as speed, location, and vehicle use. This potentially poses questions

regarding the driver, or vehicle owner's, freedom being affected by limiting driving behavior. This phenomenon is known as 'behavior rewarding', which consists of altering driving behavior to be considered favorable towards third parties, such as insurance parties in order to receive a reward, often in the form of lower insurance rate. Although lower insurance rate seems favorable to some, it comes at a significant cost, namely the loss of privacy and to what extent linking insurance rates to behavior could change behavior of users, for the sole purpose of satisfying a third-party surveyor, thus altering the representation of freedom traditionally associated with vehicles.

2.3.4 Ethical Dilemmas

Current academic debate also highlights concerns regarding more nuanced apprehensions, such as the ethical implications of the global abundance of sensors and connectivity within daily used products. Concerns include human tracking, digital trust, and the associated freedoms or impacted freedoms resulting from the IoT (Atzori et al., 2010; Uckelmann et al., 2011; Gubbi et al., 2013; Roman et al., 2013). The methods of moving collected data has also advanced through general progressions in connectivity, meaning that sizable amounts of data are collected and transmitted globally. This has resulted in data movements becoming more complicated due to the increased quantity of personal information being collected and transmitted on a global level. Furthermore, the tracking of individuals which is possible through IoT technology highlights a surrounding debate regarding the freedom and privacy with mobility. In some ways, it could be argued that vehicles would no longer offer the same sense of freedom they once did (Litman, 2017). Automobiles are mainly used for people as a mobility solution and as a way to gain independence and the possibility to move whenever needed. If each of these movements is perceived, recorded, and processed an ethical question arises, namely whether or not an automotive customer would still have to possibility to remain anonymous.

Furthermore, the performance of machine perception is another concern in the current literature. Specifically, as part of 'robotification,' users are becoming reliant on the proper functioning of hundreds of sensors, camera, and computers in order to properly use the AV systems; all these sensors and systems must be capable of functioning at all times and in all conditions and need to be continuously analyzed, while the consequences of failure must be anticipated (Lin, 2016).

As devices become further integrated into the daily lives of the average consumers, the user becomes less aware of the processes at play with the interaction happening with these devices. Due to automation, and the seamless integration of the devices in daily lives, consumers no longer take the time to understand the IoT devices' operation and function. This results in a disconnect between our understanding and participation with digital devices (Mikton, 2015). The current understanding of the newly introduced field of machine intelligence is resulting in a complex dynamic of new ethical implication which are beginning to challenge the moral constructs and relationships between machines

and humans (Mikton, 2015). For many, the frictionless experiences of automation out way the potential costs of giving up privacy to third parties and comes at the benefit and pleasure of a seamless experience. However, many of these interactions have become involuntary with IoT as devices are now so integrated in daily life.

For AVs, ethics are not limited at subconscious data collection, due to seamless integration into daily lives but rather, one must consider the complexity of driving behavior and road conditions. Only after AVs have proven successful with all kinds of ethics in decision making will self-driving vehicles be able to assert itself in practice (Lin, 2016). In current literature this is described in the so-called 'dilemma situations', in which AV technology must be pre-programmed and educated from an ethical standpoint. In the case of an unavoidable collision, what outcomes are favorable from a safety, as well as ethical standpoint? According to Lin (2016), an example of this could be to program AVs to cause the least possible harm to the humans involved, both inside and outside the vehicle in the case of unavoidable damage.

However, on the contrasting debate, there is the question on whether AVs safety demonstrations take away traditional ethical considerations. For example, according to a study by the ENO Center of Transportation, about 93 % of the 5.5 million crashes in the U.S. have been attributed to human error as the primary cause of the crash (Gogoll, & Müller, 2017) leading researchers to conclude that most scientific efforts result in AV technology having an overall positive impact on driver safety and AVs resulting in lower overall numbers of road accidents and deaths. The contribution of AV to increase safety on the road could dispel current traditional ethical dilemmas with regards to AVs.

However, in the discussion of ethical dilemmas and automation, the navigation of complex ethical scenarios should be done, according to what Litman (2017) describes as pre-programmed ethical dilemmas. These ethical dilemmas require research to be done and a consensus to be established on each individual ethical scenario presented on public roads. For example, if a car is advertised as being particularly safe, and the customer purchases this vehicle for the sole motivation of the superior safety, then in the case of an accident the complexity of the scenario becomes apparent: As the vehicle was purchased because of superior safety, it could be argued the car should attempt to maximize the safety of the driver, as the driver has paid for the above superior safety of the vehicle. Alternatively, the vehicle might be programmed to protect as many pedestrians or other road users as possible and therefore attempt to limit human deaths, perhaps at the expense of the driver. If both outcomes are mutually exclusive, where either the driver survives or pedestrians outside the vehicle survive, an ethical decision must be made. These types of dilemmas, referred to as "trolley cases" (Himmelreich, 2018) are building ethical discussions surrounding AV technology (Gogoll & Müller, 2017).

Another popular and often discussed example of a ‘trolley case’ is where the ethical dilemma is presented in multiple railway workman on one train track with an intersection with another train track containing only one worker on it (Gogoll & Müller, 2017) while the AV equipped car can control the switch between the two tracks, meaning it must decide between one of the two train tracks. If a train is coming down the track and is unable to slow down, the AV system is presented with a choice: send the train down one track, risking the life of one worker or send the train down another track risking a group of workers. This popular dilemma has been central to the debate about AV technology as it demonstrates a situational choice where there are no clear or "good" outcomes, questioning if the object in control. AVs for instance, are able to choose the best outcome by acting according to a moral code of human protection. This is a subset of the philosophical principle of utilitarianism, where the morally correct decision is the one that maximizes the well-being of the greatest number of people (Nyholm & Smids, 2016). The AV technology of the future must be able to judge these types of dilemmas, among others, and only when AV technology has proven successful with all kinds of ethics in decision making will self-driving vehicles be able to assert itself in practice (Lin, 2016).

Thus, the discussion surrounding automation and data collection through the IoT, particularly the use of AVs, raises many questions and debates central to societal topics discussed in mainstream media alongside technical, philosophical and academic perspectives. These challenges, particularly surrounding privacy, raises specific concerns and dilemmas that constitute the current debate and potential future consequences of both AVs and IoTs in general and are a significant part in understanding whether and how potential regulation such as the GDPR might mitigate some of these challenges, particularly regarding privacy.

2.4 Potential Negative Effects of AVs

Although fantasizing about traveling in vehicles more reminiscing of driving living rooms going to work while watching movies or having a meeting sounds impressive to most, there are some considerable downsides to the potential introduction of AV technology beyond the privacy and ethical considerations of automation and IoT. Although the goal of this thesis is to focus on the perception of privacy with the use of AVs, the possible other negative effects of AV technology are also considered as they could introduce new contexts into the current and balanced debates on the subject.

Firstly, with the introduction of new technology, the issue of transition is apparent. Development is considered when, at the same point in time, both traditional and new technologies are combined and able to work together (Todorovic, Simic, & Kumar, 2017). This presents a potential safety concern as human drivers might not be compatible with AV driving conditions and road interpretation. This transitional phase, where humans and AVs will mix on public roads, must be overcome before the technology can be fully embraced by all stakeholders and fully integrated into society.

Secondly, the use of AVs may have societal and psychological impacts. As highlighted earlier, the current scientific debate often explains the positive effect of the use of AV technology on society and often describes benefits when it comes to fuel savings, parking and driving infrastructure and better time management for the driver, allowing for entertainment or work to take place instead of driving. However, AVs may also have an adverse effect. While the inevitable development of AV systems seems high at first glance, it is clear that with the introduction of automated technology, there are some downsides for society. AV technology will become responsible for the replacement of various jobs of driving-related professions such as taxi drivers, chauffeurs, and bus drivers (Pettigrew et al., 2018). Furthermore, many consider an automobile as an item of substantial value and an item of pride. This status and pride of owning an automobile may no longer be achievable, due to the rising cost of ownership, and to the large-scale offerings of new ownership models, such as car sharing platforms. As Litman (2017) highlights, car ownership may change altogether with the possibility that automobiles may be more often shared, resulting in a decrease in vehicle ownership and a loss in the feelings of freedom and achievement. These challenges also demonstrate the crossroads surrounding AVs today and the changing automotive and mobility industry as a result of this.

2.5 Strategies in addressing challenges

In order to understand to what extent innovation in the field of AV technology and privacy can co-exist, one must first gain insight into the values that are being integrated within the development of AV systems. On the one hand, AV systems could change composition and traffic flow within cities, such as a reduction or shifting of parking-space requirements in inner cities and efficient use of road space in flowing traffic would be set against fresh suburbanization stemming from alleviated conditions on the urban fringe (Lin, 2016). On the other hand, however, fundamental concerns regarding privacy and ethics must be addressed prior to the global integration of AVs into the global automotive market. Indeed, in failing to address these concerns regarding privacy and data protection, autonomous vehicles could well meet “market resistance” from potential users who perceive autonomous vehicles as threats to their privacy and thus potentially decrease or halt the adoption of AV into society. Similarly, assuring respect for user privacy is one of the best ways to foster trust and confidence in new technologies such as autonomous vehicles (Glancy, 2012).

Although the focus of this thesis is surrounding how policy measures, particularly the implementation of GDPR can be a potential method in making AV technology and privacy complementary, the section will first highlight the strategy of privacy by design thinking into initial AV design as a potentiality before addressing policy implications and introducing the theoretical discussion of the GDPR.

2.5.1 Design Thinking

The field of design thinking, particularly focused on privacy by design (Weinberg et al., 2015) is at the center of academic debate as a value that can be integrated into AV design and is an essential consideration to account for within the primary design of AV systems. The foundation of privacy by design is a concept known as "design thinking," the concept of "design thinking" consists of "a methodology that imbues the full spectrum of innovation activities with a human-centered design ethos" (Brown, 2008). This notion was derived from design thinking methodologies long advocated by privacy theorists such as Helen Nissenbaum (Glancy, 2012). Privacy by design, and more generally "design thinking" is achieved by allowing the innovation to be powered by a thorough understanding and with direct observation of what people want, understanding what is desirable in the daily lives of the consumer, and the product under development. These are fundamentals to the development of products and integrated into the packaging, production, marketing, sales, and support (Brown, 2008). By using design as a collective understanding of what is needed, the approach can be far more effective in tackling concerns with new product types and better existing ones. It has been used to make products more desirable and has stimulated market growth in the past. The concept of privacy by design is described by Ann Cavoukian (ND) through the following principles:

1. Proactive, not Reactive; Preventative not Remedial
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy

Increasingly the concept of design thinking has been heavily associated with an innovative, creative and competitive business practice. This is due to the perspective of the world approached by the "design thinking" perspective, which is more holistic, interdisciplinary, integrative, innovative, and inspiring (Cavoukian, ND).

Design thinking can thus be utilized as a way to mitigate privacy concerns in the development and updating of AV technology. As discussed previously and as described by Glancy (2012), AVs could meet "market resistance" from potential users who perceive autonomous vehicles as threats to their privacy. Glance (2012) additionally describes that assuring respect for user privacy is one of the best ways to foster trust and confidence in new technologies. In AVs data privacy must be an integral component and priorities must be integrated into each protocol and process within AVs (Cavoukian, ND). By utilizing design thinking to build privacy protection into autonomous vehicles from the start, the potential for "market resistance" and a slowing in mainstream implementation could be avoided and could help maintain a proactive approach to privacy thereby strengthening user trust in AVs.

2.5.2 GDPR and Its Implications on Privacy

The GDPR was initiated on 25 May 2018 after a two-year conversion period in May 2016. GDPR directly impacts all organizations processing and controlling data of each individual within the European Union (EU). This has implications to all global organizations, as the GDPR applies to any entity that collects and processes personal data of subjects within the EU (GDPR, ND). As part of the GDPR, data processing activities done by any organization must be transparent and completed with a specific purpose. As data processing becomes complete, the data must be removed when that intent has been satisfied or the need for the data collection completed (GDPR, ND). Saving personal data is restricted, with the exception of the gathered personal data that is in the public or scientific interest (GDPR 5.1e). The personal data collected must be managed legitimately, including with either the consent of the data subject or for a legal obligation. Moreover, data must be processed lawfully (i.e., either with the consent of the data subject or for a legal obligation), whether the processing is done in an automated (e.g. 'profiling') or non-automated manner (GDPR 4). As part of the GDPR, data is processed lawfully when one of the following components are complied with:

- The data subject has given consent
- Processing data is necessary for the fulfillment of a contractual or legal obligation
- Processing data is necessary to protect the vital interests of the data subject
- Processing data is necessary for authorial tasks (EUGDPR, n.d.).

Although the initial publication of the GDP did not provide explicit reference to data controlling and processing with regards to robotic or autonomous applications, in 2017, the European Parliament provided classification within the applications of AVs and the further developing of this technology under the GDPR (Daly, 2017).

The newly introduced GDPR should place control of who has access to their data and what is done with it back into the users' hands (GDPR, n.d.). Goddard (2017) describes that although GDPR is a European regulation, the scaling of GDPR within Europe, as well as the globalization of current society and technology, will mean the regulations may have implications worldwide. Because the regulations set out to cover all personal data of EU residents, regardless of the location of the processing, thereby not limiting the impact of these regulations to EU borders.

Although scholars tend to agree that privacy is a concern, most scholars do not agree on the definition of personal data, which is key to building an understanding of the matters that are affected as a result of AV systems. For the purposes of this thesis, Article 4 of the GDPR provides an extensive definition of personal data which will be utilized as the definition by the thesis: "Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

identification number, location data, and online identifier or to ones or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person." (GDPR, n.d.). A concern arises with regards to the requirement that saving personal data is restricted, apart from the exception that is in the public or scientific interest along with the notion that the current regulations merely require compliance with one of the four listed elements. It can be argued that in assessing the improvements in road safety, reduction in traffic congestion, and emissions is in the public or scientific interest, collected data could be free of limitations according to the GDPR. In any case, the user is allowed to have the data removed if they wish, enabling more control in the access to their data. However, all in all, these privacy regulations are widely referred to as the single most important impact on data privacy regulations in over 20 years (EUGDPR, n.d.).

In summary, this section provided the theoretical backdrop underpinning the public and academic debates surrounding AVs and more generally the IoTs. The section focused primarily on the technological shifts in mobility throughout history, and how the introduction of AVs creates optimistic changes as well as significant challenges not only in its implementation and development, but in public perception surrounding AVs. This stems around primarily the concerns of privacy, which the section provided an analysis of current academic debates on, particularly with regards to challenges of maintaining privacy in today's world of increasing data collection. Finally, the chapter introduced the commencement of GDPR in the European Union in order to provide background into the regulation used in the analysis.

3. Methodology

The aim of this thesis is to create a more nuanced understanding of the two main topics of this paper, namely that of innovation, more specifically AV technology and privacy regulations in finding a middle ground where both notions co-exist. As highlighted earlier, to limit the scope of this paper to a manageable and yet insightful degree, the focus of this paper is on European privacy regulations, particularly the GDPR. The compatibility of both privacy and innovation is necessary in the modern interconnected world fueled by IoT and internet exposure and thus an analysis of a combinations of perceptions and worldviews of the full range of stakeholders involved in this process regarding the affordances and constraints of these technologies is crucial to understanding whether the GDPR can provide a relevant framework for the public perception of privacy and innovation in AVs to be complementary. This section will first discuss the reasoning in choosing a qualitative content analysis and the data collection utilized for the analysis.

3.1 Qualitative Approach

Given the nature of the research question, a qualitative content analysis method was selected for this study. According to the academic consensus, a qualitative approach is considered "any kind of research that produces findings not arrived by means of statistical procedures or other means of quantification" (Corbin & Strauss, 1990). Qualitative research is beneficial in the exploration of meaning and how meaning is formed. Essentially, the researcher seeks to uncover insights in the form of implicit and explicit meanings when conducting qualitative research. Therefore, it is suited to this study, as this thesis seeks to explore the compatibility of both privacy and innovation, which is a matter of perceptions and worldviews of the full range of stakeholders involved in this process regarding the affordances and constraints of new technologies. Furthermore, according to Malhotra & Birks (2007), qualitative content analysis denotes a procedure that seeks to organize data into sets of themes and codes. By doing this, the qualitative units of analysis can be assigned labels or codes of which the researcher can identify patterns through meaningful categorization of the labels and codes (Malhotra & Birks, 2007). The use of labels allows researchers to provide meaning to the data collected and ensure the reliability of the data through the categorization of these labels. In addition, Schreier (2012) portrays a key characteristic in conducting a qualitative content analysis which requires the researcher to set out to use interpretation and be reflexive (Schreier, 2012).

To sum, this thesis follows the criteria of a qualitative content analysis in the following ways. Firstly, the thesis will analysis and interpret symbolic content through the interpretation of how media publications, done by stakeholders, represent AV technology, and to what extent privacy regulations are taken into account. The aim is to attempt to broaden the understanding of how the compatibility of privacy regulations within AV's technology is represented in the main debates and public perception

on AVs. The thesis seeks to uncover the compatibility of both elements as in order for AVs to be embraced as a global, mass-market phenomenon, the perceptions and worldviews of the full range of stakeholders are crucial in the perception on the affordances and constraints of these technologies. Secondly, this research design supports the creation of social meaning as the themes of privacy and innovation are represented in the articles written and the construction of patterns about the topics described in the research question (Schreier, 2012).

3.2 Data Collection

In order to fulfill the methodological guidelines of the Master's thesis, the analysis will utilize approximately 10 sources per stakeholder category, as discussed below, to ensure that the research question of this paper can be answered with a fair interpretation of the concepts of this paper. Through the utilization of different stakeholders, the research will ensure equal and balanced representation of each stakeholder's perspective, which will, in turn, result in a fair and balanced exploration of the meaning created surrounding the topics at hand. Indeed, as Schreier (2012) describes, content analysis is about systematically describing the meanings of the data through a qualitative approach and goes beyond merely counting words by classifying meaning to categories that represent similar meanings (Weber, 1990).

Multiple sources of data are also vital to the representation of patterns identified by "the different sources or methods of data must necessarily converge or be aggregated to reveal the truth" (Schwandt, 2014). Thus, the thesis will attempt to triangulate different sources, as it, as described by Yin, (1984) underwrites the reliability of the entire database of the content constructed. Triangulation is described as the use of numerous data collection approaches or sources that certifies the establishment of stronger substantiation of constructs (Eisenhardt, 1989). The thesis thus opted to select relevant online content, including publicly available reports and press releases, from each stakeholder perspective published within the past 24 months of the initial writing of this thesis. Limiting data collection to only the most recent sources was done with the aim to avoid a lack of relevance, which in turn supports the validity of this study, particularly given the novelty of the subject at hand as well as the rapid development of the technology itself and the industry.

As the research hopes to gain an insight into the multiple perspectives of privacy on the AV sector, it is crucial that the thesis utilizes multiple stakeholders. Thus, in choosing the stakeholders, an identification of the important stakeholders in the AV sector were conducted and the following stakeholders will be the focus of the analysis: (1) Government and Policymakers, (2) Original Equipment Manufacturers (OEM's), (3) Watchdogs, (4) Automotive Customers, and (5) Public Transportation. These stakeholders were selected from research conducted from EY's (2014) report on AVs, and each were chosen for this research due to their varying perspectives and exposure to privacy regulation and AVs. Firstly, as AVs are very much ground-breaking technologies sought to be

implemented to the general public, they are very heavily reliant on the approval of local governments and policymakers. Governments and policymakers would add insights on how AV technology would be permitted on the public roads, through the eyes of regulators, particularly with regards to compliance to GDPR. The second identified stakeholder, OEMs, are another perspective used for this study, as the research hopes to include insights into the development of AV technology from car manufacturers themselves. Furthermore, due to the nature of the research design, insights into what aspects of AV technology and data collection OEMs find important, and how they navigate marketing their product and using GDPR regulations in AV design. Thirdly, watchdogs will add an independent perspective on the regulatory and security developments within AV. Fourthly, automotive consumers will add a significant perspective, as to which elements of AV and privacy regulations are compatible from a consumer perspective, and whether the GDPR is able to curb consumer concerns. Finally, public transportation provides a different application of AV technology and the perspectives of a non-automotive form of AV technology. The following table shows the data sources gathered for each stakeholder category:

Stakeholders	Sources
Automotive customers	Capgemini. (2019). *The Autonomous Car Report*; *Consumer excitement for autonomous vehicles soars but barriers remain.* Ericson. (2018). *The Self-driving Future* Here. (2017). *Consumer Acceptance of autonomous Vehicles; 3 key insights for the automotive industry*
Government Policymakers	ACEA. (2016). *Auto industry develops articulated pedestrian dummy.* ACEA. (2018). *Focus on vehicle safety measures with most tangible results, auto industry says.* ACEA. (2019). *Auto industry to raise awareness of safety technology, as new EU data on road fatalities is released.* ACEA. (2019). *New vehicle safety rules: auto industry reacts to European Parliament vote.* ACEA. (2019). *Vehicle safety: auto makers call for rapid adoption of new EU requirements.*

	European Commission. (2019). *Connected and automated mobility in Europe.* European Parliament. (2019). *Parliament closes legal loopholes to protect victims of road accidents.* European Parliament. (2019). *Self-driving cars in the EU: from science fiction to reality*. European Parliament. (2019). *A More proactive approach needed on autonomous mobility, Transport MEPs say.* European Parliament. (2019). *MEPs call for safety and liability rules for driverless cars.* European Parliament. (2019). *Car insurance: new EU rules to better protect victims of road accidents*
OEMs	BMW Group (2018). *When the driver becomes the passenger.* BMW Group (2019). *The Future of Driving is Autonomous.* BMW Group (2019). *The new BMW Group High Performance D3 platform.* Daimler (2018). *Successful autonomous driving*. Daimler (2018). *Going with the autonomous flow*. Daimler (2019). *A vehicle doesn't have an ego*. Honda (2018). *Honda Joins with Cruise and General Motors to Build New Autonomous Vehicle.* Honda (2018). *"Honda Autonomous Work Vehicle" Makes Off-Road Work Easier, Safer and More Efficient.* Tesla (2019). *Tesla To host autonomy investor day.* Toyota (2019). *Toyota Research Institute Bets Big In Vegas On "Toyota Guardian" Autonomy.* Toyota (2019). *PAVE coalition launches broad-based public education campaign on automated vehicles.*
Public transportation	Intelligent Transport (2018). *Autonomous vehicles to 'see' around corners in new project.* Intelligent Transport (2018). *Electric autonomous vehicles set for Gatwick airfield trial.*

	Intelligent Transport (2016). *Public testing of autonomous vehicles takes place in UK for the first time.* Intelligent Transport (2016). *Autonomous vehicles operate as temporary bus service at Dutch university.* UITP (2019). *UITP arrives at new milestone on road to SPACE.* UITP (2019). *Geospatial technologies: moving people ahead.* UITP (2018). *UITP takes an active lead in the autonomous revolution.*
Watchdogs	CAD (2017). *UK is to be a world leader in autonomous vehicle technology.* CAD (2018). *Europe opts for the development of connected vehicles.* CAD (2019). *More autonomous cars – less car ownership?* CAD (2019). *The Netherlands Ranked First in KPMG Autonomous Vehicles Readiness Index (AVRI).* Consumer Watchdog (2018). *Industry Deal Threatens To Undo CA's Robot Car and Privacy Standards.* Consumer Watchdog (2019). *Self-Driving Cars Have Miles To Go Before They Reach Full Autonomy, Says Watchdog.* ICDPPC (2017). *39th International Conference of Data Protection and Privacy Commissioners Hong Kong, 25-29 September 2017.* NHTSA (2012). *Remarks Delivered by David Strickland, Administrator National Highway Traffic Safety Administration Autonomous Vehicle Seminar.* NHTSA (2019). *Preparing for the future of transportation: Automated vehicles 3.0.* NHTSA (2019). *Automated vehicle for safety.* NHTSA (2019). *Vehicle-to-Vehicle Communication.*

As this thesis is relevant to Media Studies, the aim is to understand the meanings captured from the context on privacy concerns and AV technology from the aforementioned stakeholders, and to assess if GDPR is able to make those two issues complementary to each other. As such, the data provided is mostly from stakeholder publicly released information, such as press releases and media reports and articles. This allows for meanings to be constructed for an analysis into the research question using a media-focused data gathering and analysis method. For the government and policymaker stakeholder perspective, due to the European focus on this paper, sources were gathered from the European Commission publicly available documents and press releases. For OEMs stakeholder perspective, data was collected by analyzing the most recent annual reports of these OEMs, such as BMW, Daimler, Toyota, Honda and Tesla. The data on watchdogs was analyzed in the most recent press releases by these watchdog organizations released in the past 24 months. In order to satisfy data from automotive customers, the research utilized publicly released reports from the past 24 months by major credible automotive customer research institutions, including Capgemini, Here, and Ericsson. Lastly, online content through press releases and available online articles were gathered to gain insight into public transportation stakeholder perspectives. The data used however, could lead to some online publications favoring messages that are in beneficial to the presentation of the organization's investors, media or customers, which in turn, could impact the online publications resulting in possible influences in the data sets. However, through this method, the findings gained new insights as well as answers to the research questions while preserving a valid and reproducible research methodology.

3.3 Data Analysis Methods

To answer the research question, the researcher focused on the terminology and conceptualizations related to AV technology and privacy, as defined in the literature section of this thesis, as well as terms relating to GDPR. The research sought to answer the research question by identifying patterns through the information provided by the different stakeholder data and comparing it to the others. As described in the previous section, each stakeholder perspective was analyzed by searching for key terms related to the various elements of AV and privacy described in current literature. These, for example, included terms related to automation, ethics and morals, and values by design. After identifying the main themes and categorizing the data units into each respective category, each data unit was further analyzed to determine themes throughout the data. Indeed, the ways in which stakeholders report on the various topics within AV and GDPR may impact the public opinion on the subject, and as this paper seeks to identify compatibility between these issues, the phenomena at play must be identifiable. Thus, for each stakeholder perspective, the findings have identified patterns between stakeholders that result in a compatibility on each element of AV and GDPR. As stakeholders both seek innovation as well as privacy in an ideal world, identifying areas where stakeholders agree and disagree on the subjects at play could be used to adjust policy, social norms, and potentially new business opportunities.

The identification of patterns and themes was conducted through the creation of a coding (Appendix 1) to assist in answering the research question. Within qualitative methods, the coding frame is the heart of the methodology (Schreier, 2012). Through open coding, the identified hidden meanings within data resulting in patterns have been identified through categories and subcategories. Firstly, the thesis will categorize elements of the research identified, and group the data into initial larger themes allowing for a more general sense of the topics at hand. Secondly, the thesis to provide subcategories to gain insight into what is being debated about the elements of the research question, where established (See Appendix). In dividing the categories and grouping the data into themes, the thesis will attempt to ensure inconsistencies and repetitive categories do not arise, in order to ensure the focus and answer the research questions at hand. Following the establishing of dimensions, the researcher looked to specify what was being discussed about each dimension and within each category and subcategory. The categories provided a deeper meaning that assisted in answering the research question, through a deductive, and concept-driven approach. Building on previous understandings of media and stakeholder viewpoints, the coding frames were used as a filter for insightful data that can be used for the research question. It is adjusted throughout the process of gathering data and is built by the researcher individually. This was done to result in a deeper understanding of the topics at hand and seek to reduce the personal bias of the researcher.

Validity is ensured due to the use of a coding frame by collecting data and collecting themes represented within the data. This allows for a global overview of what themes are discussed and therefore allows of the further categorization and grouping of larger more general themes into smaller, more specific subthemes. Repeatability of the finding of this thesis is vital to the reliability of the findings. To ensure reliability within the research design, themes in both the larger, more general themes as well as subthemes are built through keywords that are described in previously published literature on the subject with the aim of using a basis of consensual knowledge and redetermined keywords to describe these novel topics at play.

4. Findings and Analysis

In this section, the findings of the research will be analyzed and discussed. As mentioned, the goal of this thesis is to answer the main research question: *To what degree is privacy, through the GDPR, compatible with innovation in AVs*? This will be conducted through qualitative research analysis that in which an identification of patterns from a coded data gathered from online public media publications by various stakeholders. As described in the previous section, stakeholder perspectives were used and analyzed by searching for key terms related to the various elements of AV described in media publications and providing insights into the themes through a deeper analysis of the patterns.

As a result of the research question, four main themes (or patterns) were highlighted that will be discussed in detail in this section. The first pattern involves the notion of trust, as it is a vital pattern

that was identified and is a recurring theme. The second pattern concerns consent, and echoes what the theoretical section of this thesis highlighted as a vital component of GDPR. This particularly concerns the debate on whether consumers understand the gathering of data that is currently being accumulated in customer vehicles. The third pattern concerns transparency and the need for public available information. Finally, the last pattern concerns the ethical dilemmas highlighted in Section 2, in which the research found that there was actually no need for the ethical dilemmas focusing on 'trolley cases', due to the ability of AV technology to gain knowledge through data gathering, challenging the current academic consensus. These findings will be analyzed in detail in order to provide a platform for discussion and the concluding remarks in the next section.

4.1 Trust in AVs is indispensable

Handing over control of a vehicle at high speed on a highway to a computer could seem like an unnerving and futuristic idea. As AV technology seems to no longer require drivers to be behind the wheel, this will require a certain degree of confidence in the systems inboard. These include confidence in aspects of the car such as the quality of the sensors used in the vehicle to the programming of the driving software. Central to this idea is the notion of trust, which is a vital pattern that multiple stakeholders have identified and is a reoccurring pattern as a result of the data gathering of this study. According to the findings of this study, various stakeholders share differing views on the concept of trust. However, as the media has recently covered stories regarding the misuse or abuse of data and technology, most stakeholders have consistently naming trust as an issue surrounding AV innovation. Although trust in itself is not directly linked to GDPR, it can provide a framework in identifying how principles, acknowledged in this thesis such as "design thinking", can be implemented to ensuring GDPR creates compatibility between innovation and privacy in AV's.

Stakeholders indicate trust as being the main concern with AVs, while also holding differing notions of the concept of trust. The data collection found that trust is identified by all the stakeholders to be established with regards to AVs in the following three central ways:

1. Proven track record in safety, both physical and digital safety
2. Bridging a transitional period through the democratization of safety
3. Implementation of design thinking principles

From the standpoint of government entities and policymakers, the pattern of trust is founded from a safety concern. According to the European Commission, trust is gained through the proven safety of AV systems with two core aspects that were identified guiding trust in AV systems, "physical" and "digital" safety. Physical safety required AVs to be proven as safe for occupants within the vehicles as well as for pedestrians and other road users, while digital safety referred to governments trusting that the digital services provided by AVs are traceable. This particularly refers to the compulsory use of data recorders to ensure that the data collected is traceable and ensures improved accident investigation as well as limiting liability concerns (European Commission, 2019). Essential in

compliance with privacy regulations and therefore GDPR is that regulations can help to ensure that the data recorders are utilized in a manner that ensures personal privacy. GDPR can set a framework that facilitates trust in the safe and private gathering of data. However, the concept of trust with regards to innovation is nothing new, as policymakers and government entities want to trust in the safety standards of AVs before allowing them on the public roads (ACEA, 2019). Thus, from the perspective of the European Commission, the safety improvements must be measurable, indicating that most AVs can safely navigate the public streets.

Furthermore, with the introduction of any new technology, there comes a phase of transition, where new and older forms of technology must be able to converge safely on the public roads. With AVs this means that a period of transition where the human driver, as well as the AV's, must be able to function together safely and beneficially to society and the general population. OEMs address this concern by reaffirming the building of trust and supporting of the driver (BMW, 2019). For example, Toyota developed a system called "Guardian" which helps support the driver in the operation of AVs (Toyota, 2019). Furthermore, Dr. Levant Ekiz, a developer of autonomous driving at the BMW Group, likened trust in the AV system to driving school:

> "It's like the first day of driving school, where we have to learn to trust the car and its functions – the brakes, the gears, our ability to steer it. It's no different with an autonomous vehicle. It's our job as an innovation leader to build this trust level by level." (BMW, 2019)

The above quotation, as well as Toyota's "Guardian" system, describe an attempt by OEMs to conduct an initial phase of integration with AV systems through the gaining of trust by experience, enjoyment, and trial and error. As the academic literature mentioned, the perception of machine performance and the reliance of the proper functioning of the hundreds of sensors, camera, and computers to properly use the AV systems must be capable of functioning well in every condition, and these conditions need to be analyzed, and the consequences of failure must be anticipated (Lin, 2016). In the case of OEMs, this is where the uncertainty lies. Thus, OEMs are in a position of uncertainty, as they need to ensure that in this phase of transition where AV technology may populate the public roads, trust is what will ensure that the stakeholder feels confident enough to use AV systems.

Moreover, trust according to OEMs is about the concept of 'democratization of safety', a philosophy Toyota and Lexus pioneered, by building trust and supporting the driver with the operation of the vehicles through a system. By the providing of automatic emergency braking as standard equipment in nearly every model and trim level sold in the US (Toyota, 2019). This is linked to the concept of design thinking highlighted in Section 2, as the need for safety was taken into account in the basic design of the vehicle, as demonstrated by Toyota and Lexus by in providing the automatic emergency braking system. Indeed, a Capgemini (2019) report echoed that "automotive companies

would do well to understand consumer expectations and bake them into the design process itself." On the contrary to what the literature suggests, where the market in which OEMs operate is highly competitive (Baily et al., 2005), OEMs will refrain from demonstrating transparency regarding the data collected, which in turn, results in a newly found trust concern with the consumer. Data confirms this, as for trust to be established, rather than engaging with the customer regarding the sourcing of customer data as the literature suggests, by putting the data collected through AV systems at the heart of its operations, companies can increase automation and control. As will be highlighted in the subsequent subsection on transparency, the GDPR enables the action of trust through the requirement of entities to be transparent on the use of data collected and processed.

From the watchdogs' perspective, the benefits of AV, through the interconnectivity of vehicles and the infrastructure, results in data are continuously being shared with the environment and other vehicles, infrastructure, and third parties (ICDPPC, 2017). This is done in order to ease traffic or to improve safety or efficiency, build trust, and demonstrate how AVs can be implemented and can be used as game-changers. One of the ways in which watchdogs highlight the issue of trust is in their assessment of over-reliance on these technologies, particularly in the early stages. Interestingly, as devices become safer, accident rates tend to increase initially (Ackerman, 2017). This is due to a so-called 'over-trusting' phenomenon where the user is placed in a safer environment compared to what that user might be used to, resulting in increased risk-taking. This is also referred to as "offsetting behavior" or "risk compensation" (Litman, 2017). With regards to AVs, this can occur due to what was earlier highlighted in Section 2 regarding consumers depicting cars as living rooms without drivers attending to the control of vehicles. As a result of this perception, passengers could then not be adequately secured with seatbelts and over-trusting the technology (Ackerman, 2017). As is so simply stated:

"Trust is not given, but earned," (Here, 2018)

One of the automotive customer studies highlighted that only 19% of customers stated with certainty that they would likely use autonomous vehicles (Here, 2019). Thus, the earning of trust is essential to increasing the likely daily use of AV technology for customers. This can also be said about GDPR and privacy regulations. Regulations are not a given and must be central to the development of each system, in a every more interconnected world. Although trust does not directly link to GDPR, regulations can provide an indirect platform alongside other processes such as "design thinking" to enable trust in the adoption of this new technology.

Another theme identified through the data analysis of the notion of trust concerns the status and pleasure that owning a vehicle provides consumers. Not only is vehicle ownership imbedded within society as a symbol of status and accomplishment, but the physical pleasure and enjoyment provided

by owning a personal vehicle available is essential to car ownership. This was also a pattern found in many of the data sources, as various stakeholders including OEMs, governments, and customers highlighted the use of a vehicle as a form of pleasure and a "symbol of freedom" (Ericsson, 2018). While OEMs such as BMW attempt to assure customers that the so-called 'Ultimate Driving Machine" (BMW, 2019) will remain fun to drive no matter what or who is controlling the vehicle, automotive customers seem to be concerned. Customers highlight that the automobile is more than simply a transportation method to travel from A to B, but rather it is a possession that creates enjoyment, emotion, and status (Ericsson, 2018). Whether cars change from personal transportation device or source of pleasure and enjoyment, to a shared, utility device where transportation is provided as a service, GDPR must ensure the newly shared data, previously stored within a personal car, complies with regulations. Customers are providing more personal data to third party transportation providers through this shift from personal to utilitarian transportation.

This notion is amplified as a result of the identification of the AV movement as a mobility service more than a car service. Through the further development of AV technologies, the data suggests that further development of secondary industries will likely capitalize of this new technology in creating vehicles more towards customers of the transportation industry who rely on public transport rather than more suitably the leisure industry. Consequently, consumers may start to view automobiles and other transportation methods affected by AV technology as a transportation solution rather a provision of pleasure and enjoyment. This can raise consequences towards regulators, as the classification of AVs may move from personally owned vehicles to a shared, connected mobility platform. This in turn can raise privacy concerns on the collected data and where GDPR must play a central role, as it is no longer seen as a personally owned product, but one that is shared. Trust that the newly generated and store data from these services are within the GDPR will ensure compatibility. However, this may be a Eurocentric perspective, as data on Chinese customers shows that they have fewer reservations towards data security and data use due to their affinity to technology, and their openness to sharing services regardless of the data collection concerns due to the limited resources (Mercedes-Benz, 2019). This is significant to take into perspective, as it shows that the analysis of data concerns with regards to shared mobility may be limited to the European region.

In short, the data collected indicates that trust is an evident pattern across all AV stakeholders. This is particularly concerning the trust of the vehicle providing physical safety, the building of trust trying the transitional period when both old and new technologies converge, the over-reliance of new technologies that are not yet fully ready, and concerns on the privacy of data collection. This raises complications with regards to privacy regulations, particularly when observing the shift of AVs as a personal good to a shared mobility tool. Thus, trust in the regulations governing the AV system, as well as incorporating trust into the design process of AVs seem to be crucial components of enhancing trust between AVs and privacy issues.

4.2 Consent Must be Explicit

As identified by the previous sections in this thesis, consent is a vital component of GDPR and as the data shows, consent is found to be a central pattern in AV technology, and is identifiable in various forms that vary with differing stakeholder perspectives. The data gathered shows that most stakeholders have a consensus in that with the integration of AV technology into society, data is gathered at an increasingly high rate (Mercedes-Benz, 2019). What stakeholders do not seem to agree upon is whether consumers comprehend and are able to provide consent to the gathering of data that is currently being accumulated in customer vehicles.

An AV enabled vehicle must collect data points both while driving and while under development. Most OEMs indicate that in order to build a database of road conditions, traffic behavior, driving vehicles equipped with AV systems must be exposed to a significant amount of various conditions in order to allow the systems to learn, adjust and to become capable of safe operation (BMW, 2019). The data indicates that customers do not entirely understand what data is being collected and are not provide explicit authorization of gathering of this data Capgemini (2019). Furthermore, as mentioned earlier in Section 2, due to automation, and the seamless integration of technology through the devices in daily lives, consumers no longer take the time to understand the IoT devices' operation and function resulting in a disconnect between our understanding and participation with digital devices (Mikton, 2015). However, the GDPR aims to resolve this issue by requiring consumers to provide explicit consent to their data being used (GDPR, ND). In requiring consumers to provide explicit consent to the AV gathering data, consumers might be more willing to be less disconnected in their understanding of the data gathered from their devices, while OEMs are fulfilling their GDPR obligations in order to lawfully collect data.

However, while the GDPR provides a platform in requiring explicit consent from the consumer for data to be used, there are certain limitations. One such way is due to the complexity of the systems within an AV, resulting in consumers needing to have substantial technical knowledge in order to meaningfully understand the data collection processes, and provide mindful consent to the data collection
(ICDPPC, 2019), resulting in in responsibility significant burden of responsibility on the auto company to be candid about the capabilities of the vehicle (Capgemini, 2019). As a result, questions are raised as to whether the GDPR is able to bridge this gap, as its mere requirement of explicit consent does not fully allow for a capable understanding by the consumer of the data collection by the AV technology. Indeed, the reports provided by the OEMs are unclear on the sources and understanding of the data collected to develop the AV technologies as can be seen in data gathered from BMW stating that a database of 5 million kilometers of driving data is needed to make a substantial base for AI to be able

to autonomously navigate the roads using the gathered data (BMW, 2019) but fail to specify how data sourcing is done.

Furthermore, as mentioned in Section 2, questions are often raised on where the data is going, and whether it could be utilized by insurance companies, manufacturers, advertisers, and law enforcement for instance. This was echoed in the data where multiple both OEMs, public transport and watchdogs mention the use of AV data by other parties. Thus, it is important for automotive companies to be "candid about the capabilities of the vehicle and avoid any risk of misrepresentation" (Capgemini, 2019). Although GDPR regulations should protect the user when it comes to personal data that is collected and processed by one entity from transferring the data to another, one could question whether the consent of an AV user's data is clear, and therefore whether it is consensual and legal under the GDPR. This also ties back to Section 2's focus on consciousness with regards to the user's awareness of their data collection.

Another challenge that emerges as a limitation to the GDPR was described in Section 2 when highlighting the exclusion of the restriction of data that is in the public or scientific interest (GDPR 5.1e). In the research conducted, it was found that most stakeholders underscored the AVs benefit towards the public interest, by highlighting improvements in road safety, reduction in traffic congestion. Furthermore, the demand for data is quite significant, as BMW estimates that a database of 5 million kilometers of driving data will be needed to make a substantial base of knowledge, including data on road conditions, driving behavior, and traffic conditions (BMW). Thus, this potentially raises the question of whether data from AVs would be free from the GDPR's requirements, due to its public interest arguments, leading to more unambiguously defined data collection procedures.

These challenges of the notion of consent return to the academic debate regarding the notion of consciousness, as identified in the literature section of this paper. Consciousness refers to the explicit knowledge of the user that data is collected on and as highlighted in Section 2, is a primary debate regarding the application of IoT technology. As identified by the data, GDPR provides a platform in which users can ensure that they must consent prior to their data being used. However, even with the GDPR regulations, concerns arise regarding the technical understanding when consenting, the utilization of the data by third parties, and the loophole provided by the GDPR itself in which data can be unrestrictingly used in the public interest. Thus, in establishing the GDPR as a mechanism to make AVs and privacy more compatible, it is a useful starting point but there are still areas lacking with regards to ensuring consent is made in a manner that complements the theoretical notion of consciousness.

4.3 Transparent Data Collection and Public Information

The third pattern identified in the data collection of multiple stakeholders revolved around the issues of transparency, both on the usage of the data alongside the reasons behind the data collection. Indeed, if customers are made aware of the benefits of AVs, new markets can be penetrated. As a report by Mercedes Benz (2019) highlights, "autonomous vehicles make older people who need assistance, as well as people without a driver's license, more mobile" which could reduce the number of traffic deaths. The data especially shows that younger generations and millennials are identified as the customer segment with the most significant interest in AVs. Indeed, one report highlights that young people and users of local public transportation are also among the target groups that are more open to the idea of autonomously driving vehicles (Mercedes-Benz, 2019). However, "despite the surge in positive consumer sentiment, excitement and anticipation, barriers to adoption remain" as a watchdog survey conducted shows "respondents saying that purchase or adoption of a driverless vehicle is dependent on vehicle security (73%) and system security (72%)." (Capgemini, 2019).

Thus, it is imperative for OEMs and AV manufacturers to make data surrounding AV technology available publicly, in order to address concerns by consumers, both regarding issues with security, but also specially to highlight where the data collected is being utilized. By making data surrounding the AV technology available publicly and being transparent, these concerns can be addressed. By providing data on issues such as the functionality of the systems, the data on the proven safety record of the technology and addressing vehicle safety and privacy concerns, this can not only assist in satisfying watchdogs and policymakers, but also consumers. It will also fulfill GDPR requirements in enabling transparency on the rights in relation to the processing of the data being collected as well as exactly what data is being processed (GDPR, 13 & 14).

However, one challenge will likely come from the resistance of automotive OEMs to be transparent due to the competitive nature of the automotive industry as previously described. As the potential for a successful and quick introduction of AV technology can provide a huge competitive advantage, OEMs may resist in being fully transparent regarding their data collection methods. The potential for a first-mover advantage within the automotive industry provides an edge over a competitor, especially if OEMs can utilize GDPR 5.1e (on gathering data for public or scientific research) to negate their obligations to be transparent.

Thus, the research has shown that transparency offers many advantages in introducing new markets and curbing concerns on privacy. The GDPR regulation, particularly Articles 13 & 14 make it obligatory for organizations to be transparent on their usage of data, enabling consumers to feel more at ease. This shows the complementary nature of the GDPR regulation in allowing for consumers to have their rights of their data and privacy, while at the same time enable the AV market to gain from

the benefits that transparency has, although many OEMs may see it as going against the competitive nature of the automotive industry.

4.4 No Need for "Trolley-Case" Ethical Dilemmas

As demonstrated in the literature section, trolley cases have been traditionally used in debates in the subject of AV technology to demonstrate ethical dilemmas and the complex nature of the consequences of poor addressing of safety protocols in AV development. This discussion is significant as although it was not directly related to privacy, it was an emerging pattern from different stakeholder sources, and indirectly impacted privacy as many of the ethical dilemmas revolved around the collection and processing of data, of which the GDPR focuses on.

In contrast to the academic and media debate revolving around the ethical dilemmas that AVs face, particularly in dilemmas relating to "trolley cases", the stakeholder consensus contradicts the current academic debate, in which it was argued that for AVs to be trusted as safe products that are beneficial to modern contemporary society, AVs must be able to handle complex ethical dilemmas, or so-called 'trolley cases' (Lin, 2016). These dilemmas are considered central to the debate on the subject of AV technology as they demonstrate a situational choice where there are no clear or "good" outcome, questioning if the object in control, AVs for instance, are able to choose for the best outcome by acting according to a moral code of human protection. This is a subset of the philosophical principle of utilitarianism, where the morally correct decision is the one that maximizes the well-being of the greatest number of people (Nyholm & Smids, 2016).

What is noteworthy is that the data suggests that this is not required. OEMs such as Mercedes-Benz (2019) state that like other emerging technologies, there is a cultural shift and an evolution in the way humans behave once they get used to the new technology. BMW (2019) also highlights this by explaining that the substantial amount of data collected will be able to eliminate the need to pre-program or educate AV systems regarding ethical dilemmas and "trolley cases". Concluding that with the arrival of a new technology, human behavior will adapt to support this technology. This means that human will adapt to the machine. Trolley cases, contrary to the literature and academic consensus may play a far less central role in the development of AV's.

These findings echo the introduction of new technologies which come with questions and challenges that need to be addressed, but in which the pattern of adaptation and then adoption is a recurring one. One notable example is the introduction of the internet, in which the shift from knowledge in written form (published by scholars) to user-generated content on the web turned the consumer from a target audience to a participant (Lefebvre, 2007). The same might be said about the introduction of AV technology, where the newly introduced technology will shift how we view automotive manufacturers and mobility in general. Furthermore, as can be seen with the introduction of the internet, the new did not purely replace the old. As adaptation and further developments are

time-consuming and do not happen overnight, both traditional mobility solutions must work hand-in-hand with AV technology. Some applications of the technology will be in the form of early adoption, and others with require further development and slow integration into society. This, for example, includes how to reconcile privacy concerns in new technology which involves AV. Indeed, as previously highlighted by BMW, the data collected could eliminate the need for AV systems to enter the ethical dilemmas debate. However, for this to be the case, privacy issues relating to this data collected needs to be reconciled, which allows the GDPR to do this. This shows that alongside the way the GDPR plays a role in the previous patterns identified, it also by extension plays a role in mitigating ethical dilemmas, as one of the solutions to ethical dilemmas involves the use of massive data collection.

Thus, the findings of the stakeholder reports have shown four key patterns that have been highlighted by all stakeholders: trust, consent, transparency, and ethics. These issues are all of vital importance in highlighting the debate between the continuing innovation of AV technology and ensuring consumers' right to the privacy of their data. Although the GDPR has shown to be a complementary method to enhancing the right of privacy while ensuring that innovation does not lack in the process, other practical challenges emerged in the findings with regards to the implementation of GDPR as a complementary method to bridge both privacy and innovation. As will be discussed in the concluding section, the findings match some of the theories represented in Section 2, and open the floor to future debates and research.

5. Discussion and Conclusion

The data collected for this thesis has shown that AV technology is truly a game-changer in automotive technology, resulting in an active debate and conflicts coming to light regarding both privacy and innovations in technology. AV technology has enabled a shift within the automotive industry, moving control physically away from human drivers improving safety, congestion, comfort, emissions, and more. These benefits of AV technology are vital to the successful adaptation and integration of AV technology into society and the full acceptance of the technology to the general public. As can be seen in the current representation of media narratives surrounding AV technology, the general public must be assured about the benefits and improvements of the technology.

In looking to answer the main research question this thesis identified four main patterns in the compatibility between AV technology, privacy and how the GDPR could complement both. The first pattern involved the concept of trust. Trust is a vital pattern that the stakeholders have identified and is a reoccurring pattern as a result of this study of online content by showing where GDPR can create compatibility between innovation and privacy through principles such as "design thinking". The second pattern identified with regards to consent, which echoed the theoretical background, and where in which GDPR plays a vital component as it explicitly requires the consent of the user. Thirdly, transparency and public information was identified in answering the research question. Lastly, the research found that there is a possibility that no need was identified for so-called 'trolley cases' due to the ability for AV technology to gain knowledge through data gathering. This section will conclude the research provided by first highlighting a discussion into the patterns mentioned in the research, tying it back to the theoretical contributions, alongside providing the prospects of future research on this subject.

5.1 Discussion

In tying back the findings and analysis to the theoretical and literature review, many of the challenges highlighted by the academic debate are echoed in the findings, yet some are also deemed of less importance. This, as will be discussed, has implications in terms of how the current academic debate is bridged with the media and general stakeholder perceptions of AVs, alongside creating new prospects for further debates and research studies.

The notion of trust, identified as the first key finding in the data collection, was also one highlighted in the literature. Indeed, trust was mentioned throughout the literature, particularly with regards to ensuring control over their data, but also with regards to the large amount of data collection capabilities and embedded internet connectivity involved in the innovation of AV technology. The data from stakeholders also was central to the compatibility of technology and privacy, as many stakeholders identified trust as primarily grounded from safety concerns. For example, from the

stakeholder perspective of governments and policymakers, the compatibility of AVs into modern society needs to be physically and digitally safe, addressing a need for congruence privacy concerns with GDPR. (GDPR, ND). Furthermore, the arrival of AV technology has resulted in a shift away from a utilization purpose, resulting in ambiguity regarding the privacy of data collection. New challenges presented in the forms of shared mobility, physical, and digital trust mean that new clashes will be presented regarding the compatibility with GDPR. Also providing opportunity through the utilization of principles like "design thinking" to highlight compatibility shortcomings and to ensure innovation and privacy can both take place. As demonstrated in the literature section of this thesis when failing to address these concerns regarding privacy and data protection, autonomous vehicles could well meet "market resistance" from potential users who perceive autonomous vehicles as threats to their privacy and thus potentially decrease or halt the adoption of AV into society. Similarly, assuring respect for user privacy is one of the best ways to foster trust and confidence in new technologies such as autonomous vehicles (Glancy, 2012). In this manner, the GDPR provides a platform in which organizations are obligated to ensure their respect for user privacy, fostering this sense of trust and confidence in AVs.

Secondly, as identified by the previous sections in this thesis, consent is a pattern that not only emerged in the data findings, but has been a central driver of concern, as it transcends both the 'control' and 'consciousness' category. Indeed, as the literature highlighted, central to the debate are the user's fear of a loss of control over their information, alongside the user's awareness of what information is being collected. The GDPR helps reconcile this by requiring organizations to seek the explicit consent of users' prior to collecting and processing their data. The GDPR can also provide a space to solve the challenge mentioned by academics in which the user often has a lack of understanding of the exact working of the technology, as the GDPR requires that the information provided to the user be provided in a readable and user-friendly manner presenting manufacturers with the responsibility to inform users effectively.

However, although a key step forward, even with the implementation of the GDPR, some of the challenges highlighted in the literature are still evident in the key findings, particularly with regards to control. This is because under the GDPR, organizations are allowed to collect data without a user's consent if it is in the public interest, and the data has shown that OEMs have, in many ways, provided statements that echo that the data collection is in the public interest, hence not reconciling the control issues evident in users' privacy concerns. This data collection method is also echoed as a challenge in the literature, in which the literature highlights that data collected outside the consumer's control could be passed on to other parties, such as insurance companies, to utilize (Fagant and Kockelman, 2015). Thus, although the GDPR enables a platform for consent, it is also not a perfect platform, as there are still limitations that provide complications in ensuring consent in AV technology, as echoed by the literature available.

However, in order to enhance users' trust and ensure the general public's acceptance of AVs, manufacturers such as BMW should comply with the GDPR's requirement of users being kept aware of how their data is being collected and processed and requiring their consent. If the consent needed is fairly and clearly communicated and is made explicit knowledge to the user that data is collected, this can allow people to not only increase their trust in the technology, but to gain from the advantages of the innovation of AVs under the auspice of their data being collected in a legal and secure manner.

Thirdly, as the data from this thesis shows, the need for transparency regarding data collection is evident. This is also highlighted in the GDPR, in which Articles 13 & 14 state the importance of providing information about the data collection and processing. Transparency allows for consumers to understand the benefits of AVs, feeling more confident in the use of the new technology. Indeed, as mentioned in academic literature, AV technologies are at the forefront of new development and can avert deadly crashes, provide mobility to the elderly, and lower emissions amongst other benefits (Litman, 2017). This can allow new markets to enter the AV sector, such as the elderly or those seeking more environmentally friendly options. Thus, in establishing the GDPR to require organizations to be transparent about their data collection and processing techniques, this can actually be beneficial for the AV sector. However, as shown by the data from OEMs, automotive manufacturers are unlikely to view it in this case due to the competitive nature of the automotive industry.

Interestingly however, although current academic debates highlight many of the concerns regarding privacy and its limitation on users' ability to use AV technology, it also highlights the Euro-centric view in these concerns, as the data has shown that other societies, such as in China, have low concern for data privacy in order to enhance the technology and mobility standards in their society. Although the focus of this thesis is indeed on the GDPR, which is limited to the European view, it is imperative to highlight whether more technological-accepting societies have less concerns on privacy, and whether, as mentioned earlier, the understanding and transparency of the benefits that AVs provide might allow for people to be less concerned about their privacy in lieu of AV innovation. Could the education systems used today in combination with government awareness programs of data usage and the importance of data privacy be another potential path forward? If users are educated from a young age about the effects or possible effects of data processing and collections, as well as the power of IoT integrated technologies and the applications of this technology, less initial fear and hesitation by stakeholders could be a result. Allowing for developers to further accelerate the new technologies and resulting in a more meaningful integration into the daily lives of consumers, while at the same time avoiding further reluctance of the latest technology. Furthermore, as mentioned earlier with regards to consent, complying with the GDPR with regards to providing information in a transparent and public manner could allow society to understand the benefits of AVs while ensuring they are kept aware of how their data is being processed and the use of their data.

Finally, the final pattern highlighted was focusing on the ethical dilemmas challenge highlighted in the literature. Indeed, the academic debate questioned the ability for AV technology to negotiate complex ethical scenarios in the form of 'trolley cases.' However, according to the findings of this paper, stakeholders found that AVs evidently do not require a detailed understanding of ethical scenarios but rather require merely background knowledge of road and driving situations. This notion was established by data collected from OEMs currently developing AV technology who have a significant interest in the presentation of AV technology as safe and trustworthy. As findings were collected from data was sourced from online publications, OEMs must present the developments in AV technology in a transparent, user-friendly manner that could also be presented to the academic world in order to provide a perspective in the debate on ethics and AVs. According to the data provided by OEMs, using the theory that trolley cases demonstrate ethical issues, however, is not required in order to create a meaningful improvement in safety. Although it is important to study various ethical debates related to AV technology, these debates become less relevant if AV technology is proven to be more capable than its human car driving equivalent. Including the practical data from OEMs into the academic debate could provide a major step forward in bridging that gap on ethical dilemmas and allowing more acceptance of AVs from the community.

However, it should be noted that if AV technology is presented in an unfinished stage to the public as safe, and not all aspect of safety, outlined previously, secure, the trust in AV technology may be hugely impacted. This also includes trust in the data collection and processing methods by AV technologies that ensure the respect for privacy. This is hence why the GDPR plays a role here, as the regulation and respect for privacy issues will allow for data collection to be done in a way that respects the users' privacy while ensuring that AVs are able to function in a way that removes the ethical dilemma angle from the debate on AVs.

In conclusion, although the GDPR has its challenges with regards to the implementation of AV technology, and some challenges can result in some degree of incompatibility between AVs and privacy, the GDPR is a major starting point in ensuring the compatibility between AV technology and innovation with privacy. Notwithstanding the GDPR's limitations, having the GDPR in place and ensuring that all stakeholders respect its obligations allows for trust to be placed in AV technology, the consent and transparency to be provided by OEMs and allow for user's to understand and gain from the benefits provided by the data used in AV innovation, as well as ensure that by following the GDPR, that users can consent to the data collection, thereby ensuring that OEMs can collect enough data to mitigate ethical dilemmas with regards to AVs. In an ever more interconnected world, users can lose sight of the processing power and capability of electronic devices. To avoid a loss in digital trust or the many advantages presented by innovations in AV technology, it is vital that users are consciously and explicitly giving consent.

5.2 Conclusion and Suggestions for Future Research

The research conducted for this thesis has provided substantial and valuable insights into the innovations in AV technology and the compatibility of privacy. It has shown how regulation can be a tool to bridge the gap and concerns that emerge between the two issues. However, there are areas in which more research can be provided in order to better understand how regulation can be a method of compatibility between innovation and privacy in general, and also more limited to AV technology.

Firstly, further research needs to be done at a comparative level, between different national and regional systems, and how they are being affected by privacy regulations and the coming of AV technology. This paper has taken GDPR, a European regulation, as a lens; however, due to the ever more globalized economy, the intersection of these two subjects will require a global academic debate. Research should also consider how other regions, such as the Global South, might view the intersection between privacy and innovation. This is highlighted in the data findings, in which it was shown that China had less concern for privacy in order to produce more AV innovation. In ensuring the success of AVs, providing vast improvements in vehicle safety and a reduction in road accidents, the study of both privacy and AV technology needs to be conducted on a global scale, and ensuring the study of this in developing countries particularly.

Secondly, the data collected for this thesis are permissible for a limited time. Due to the rapid development of the industry and rapid transitions taking place towards an ever more interconnected world, the findings of this thesis need to be updated and re-evaluated in the future. Moreover, it would be beneficial to include more stakeholders to provide more extensive and more detailed perspectives. As AV technology develops, analyzing the perspectives of more OEMs will further provide more detailed insights on the topics at hand as there are so many manufacturers working on so many new applications of technology. As all major OEMs are currently researching and developing the concept of AVs and the application of the technology is not yet fully clear, addressing more than 5 OEMs would be beneficial to the narrowing of the research gap in this field.

In an ideal world, an altered methodology would be beneficial to answering comparable research questions. Although care was taken within the boundaries of the methodological research guidelines of an MA Master's thesis to seek the most in-depth findings and to answer the research question, the use of in-depth interviews could have provided a more detailed in-depth understanding of the precise compatibility between AV and GDPR. For example, interviews with both executives from the leading stakeholders in the AV field, as well as the leading developers of GDPR, might provide an additional layer of analysis.

The broad approach to this research topic does provide an overview of the topics at play, which provides benefits in a novel subject such as the ones of this thesis. It raises concerns and connects topics that had not previously been brought to discussion, alongside bridging the theoretical debate into real practical findings from stakeholders. One such example focuses on the ethical dilemmas in AVs. Although the academic debate raised a major concern regarding AVs ability in ethical dilemmas, the findings of this paper concluded that ethically fueled 'trolley cases,' as explained in the previous sections of this thesis, are no longer needed. Furthermore, the research on AV innovation and privacy may gain interesting developing by subcategorizing AV technology to gain further depth to the understanding of the compatibility of privacy with AV technology. For example, the assessment of AV technology in airports to resupply and refuel aircrafts might provide different analyses from the application of AV technology of a personal vehicle on public roads.

In conclusion, to address the components of AV innovation and privacy, the thesis sought to shine light on both conflicting elements by gaining insights into the nuances of what parts of the GDPR affect innovation within the AV sector, answering the research question *To what degree is privacy, through the GDPR, compatible with innovation in AVs*? For this reason, through the analysis of the data findings, the following sub-questions were indirectly referred to in the data collection and analysis:

- Which GDPR regulations affected innovation within the AV sector?
- Who are the stakeholders in the AV sector and how may they be impacted through these regulations?
- What diverse perspectives are circulating on this debate around the globe?

The goal of the main research question, alongside the various sub-questions, was to bring to light the various concerns amongst different stakeholders while attempting to understand the multiple perspectives influenced by the introduction of GDPR. For AVs to be embraced into a global, mass-market phenomenon, perceptions and worldviews of the full range of stakeholders and regions have to be involved in the process regarding affordances and constraints of these technologies. Innovation must be shaped in a way that will create a more secure and inclusive society where the technology, as well as the privacy of the user, is maintained. Due to the recent European introduction of the GDPR, this thesis focused on the nuances of privacy that arise in Europe, and how the GDPR can be utilized as a tool to curb privacy concerns with regards to AV innovation. As the findings and analysis showed, although the GDPR still has many challenges in ensuring a comprehensive standard in users' privacy with regards to AV technology and data collection, it is a useful starting point in bridging the gap created between AV innovation and privacy. Furthermore, the GDPR is a comprehensive tool that can be applied to other markets, since not only is the GDPR applicable to any worldwide firm operating in Europe, but it can provide an understanding of how a regulation standard for privacy can be applied to curb global and regional concerns on AV technology (and IoT innovation in general) with privacy

concerns. This thesis has thus aimed to provide a basis of understanding of how the GDPR can be utilized as a tool in order to gain insight on bridging the gap and creating a complementary way for both innovation and privacy to go hand in hand.

6. References

Ackerman, E. (2017). Toyota's Gill Pratt on self-driving cars and the reality of full autonomy. *IEEE Spectrum*, *23*.

Albrecht, J. P. (2016). How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, *2*, 287.

Anderson, J. M., Kalra, N., Stanley, K. D., Sorensen, P., Samaras, C., & Oluwatola, A. O. (2016). *Autonomous Vehicles Technology*. Santa Monica, Calif.: RAND Corporation.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.

Baily, M. N., Farrell, D., Greenberg, E., Henrich, J. D., Jinjo, N., Jolles, M., & Remes, J. (2005). Increasing global competition and labor productivity: Lessons from the US automotive industry. *McKensie Global Institute, November*, *7*.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 35(4), 1017-1042.

Boeglin, J. (2015). The costs of self-driving cars: reconciling freedom and privacy with tort liability in autonomous vehicle regulation. *Yale JL & Tech.*, *17*, 171.

Brown, Tim. "Design thinking." *Harvard business review* 86.6 (2008): 84.

Cavoukian, A. (ND). Foundational principles of privacy by design. Information & Privacy Commissioner, Ontario, Canada.

Cheng, X., Hu, X., Yang, L., Husain, I., Inoue, K., Krein, P., ... & Wang, F. Y. (2014). Electrified vehicles and the smart grid: The ITS perspective. *IEEE Transactions on Intelligent Transportation Systems*, *15*(4), 1388-1404.

Chui, M., Löffler, M., & Roberts, R. (2010). The internet of things. *McKinsey Quarterly*, 2(2010), 1-9.

Cohen, J. E. (2012). What privacy is for. *Harv. L. Rev.*, *126*, 1904.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

Davies, A., & Marshall, A. (2019). Are We There Yet? A Reality Check on Self-Driving Cars. Retrieved from: https://www.wired.com/story/future-of-transportation-self-driving-cars-reality-check/.

Ernst & Young. (2014). *Deploying autonomous vehicles: commercial considerations and urban mobility scenarios.* Retrieved from: https://www.ey.com/Publication/vwLUAssets/EY-Deploying-autonomous-vehicles-30May14/%24File/EY-Deploying-autonomous-vehicles-30May14.pdf.

Fagnant, D. J., & Kockelman, K. (2015). Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice*, *77*, 167-181.

GDPR (n.d.) General Data Protection Regulation. Retrieved from: https://gdpr-info.eu/.

Glancy, D. J. (2012). Privacy in autonomous vehicles. *Santa Clara L. Rev.*, *52*, 1171.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703-705.

Goldfarb, A., & Tucker, C. (2012). Privacy and innovation. *Innovation policy and the economy*, *12*(1), 65-90.

F, J., & Müller, J. F. (2017). Autonomous cars: in favor of a mandatory ethics setting. *Science and engineering ethics*, *23*(3), 681-700.

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of consumer marketing*, 19(4), 302-318.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

Gudymenko, I., Borcea-Pfitzmann, K., & Tietze, K. (2011). Privacy implications of the internet of things. In *International Joint Conference on Ambient Intelligence* (pp. 280-286). Springer, Berlin, Heidelberg.

Holler, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., & Boyle, D. (2014). *Internet of Things*. Academic Press.

Nikken, P., & Jansz, J. (2006). Parental mediation of children's videogame playing: A comparison of the reports by parents and children. *Learning, media and technology*, *31*(2), 181-202.

Krasniqi, X., & Hajrizi, E. (2016). Use of IoT technology to drive the automotive industry from connected to full autonomous vehicles. *IFAC-PapersOnLine*, *49*(29), 269-274.

Krystlik, J. (2017). With GDPR, preparation is everything. *Computer Fraud & Security*, 2017(6), 5-8.

Lari, A., Douma, F., & Onyiah, I. (2015). Self-driving vehicles and policy implications: current status of autonomous vehicle development and minnesota policy implications. *Minn. JL Sci. & Tech.*, *16*, 735.

Lefebvre, R. C. (2007). The new technology: the consumer as participant rather than target audience. *Social Marketing Quarterly*, *13*(3), 31-42.

Lin, P. (2016). Why ethics matters for autonomous cars. In Autonomous driving (pp. 69-85). Springer, Berlin, Heidelberg.

Litman, T. (2017). *Autonomous vehicle implementation predictions* (p. 28). Victoria, Canada: *Victoria Transport Policy Institute.*

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2004). Beyond concern: a privacy–trust– behavioral intention model of electronic commerce. *Information & Management*, 42(1), 127- 142.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), 336-355.

Mattern, F. and Floerkemeier, C. (2010) From the Internet of Computers to the Internet of Things, *From Active Data Management To Event-Based Systems And More*, pp. 242-259.

Mikton, J. (2015). The Internet of Things: ethics of our connectivity. *The International Schools Journal*, *35*(1), 56.

Morgan Stanley (2013) 'Autonomous Cars: Self-Driving the New Auto Industry Paradigm', *Morgan Stanley Blueprint 2013*, pp. 1.

Nyholm, S., & Smids, J. (2016). The ethics of accident-algorithms for self-driving cars: an applied trolley problem?. *Ethical theory and moral practice*, *19*(5), 1275-1289.

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing*, 9(3), 46-60.

Pinto, C. (2012). How autonomous vehicle policy in California and Nevada addresses technological and non-technological liabilities. *Intersect: The Stanford Journal of Science, Technology, and Society*, *5*.

Ray, P.P. (2018). A survey on Internet of Things architectures. Journal of King Saud University, 30(3), 291-319

Reese, H. (2016). Autonomous driving levels 0 to 5: Understanding the differences. *Tech Republic*, *14*.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266-2279.

Rushe, D. (2019). 'I'm so done with driving': Is the robot car revolution finally near? Retrieved from: https://www.theguardian.com/cities/2019/mar/09/im-so-done-with-driving-is-the-robot-car-revolution-finally-near-waymo.

Schreier, M. (2012). *Qualitative content analysis in practice*. Sage Publications.

Schwandt, T. A. (2014). *The Sage dictionary of qualitative inquiry*. Sage Publications.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, 19(1), 62-73.

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology*, *13*(1), 3-21.

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer law & security review*, 34(3), 436-449.

Wadud, Z., MacKenzie, D., & Leiby, P. (2016). Help or hindrance? The travel, energy and carbon impacts of highly automated vehicles. *Transportation Research Part A: Policy and Practice*, 86, 1-18.

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons*, 58(6), 615-624.

Uckelmann, D., Harrison, M. and Michahelles, F. (2011) An architectural approach towards the future Internet of Things, *Architecting the Internet of Things*, pp. 1-24.

Van Kranenburg, R., & Bassi, A. (2012). IoT challenges. *Communications in Mobile Computing*, *1*(1), 9.

Vermesan, O., Friess, P. Guillemin, P., Sundmaeker, H., Eisenhauer, M., Moessner, K., Le Gall, F. and Cousin, P. (2013) Internet of Things Strategic Research and Innovation Agenda, *River Publishers Series in Communications.*

Yin, R. K. (1984). Applied social research methods series Case study research: Design and methods.

Zarsky, T. Z. (2016). Incompatible: the GDPR in the age of big data. *Seton Hall L. Rev*., 47, 995.

7. Appendix

Coding scheme Including Primary and Secondary (sub)Themes

Primary Themes (Categories)	Secondary Themes
Trust	- Trust is grounded from a safety concern (SH: G&P) - Physical and digital safety (SH: G&P) - Lack trust in the mixture of both AVs and traditional, human operated vehicles (SH: OEM) - Democratization of safety - "Hands-on-the-wheel and eyes-on-the-road is first-and- foremost about safety. But it is not all about safety. It is also about how a driver feels behind the wheel; safe and secure to enjoy the drive, instead of the ride. "It's all about how much trust we are willing to place in the car," (SH: OEM) - "It's like the first day of driving school, where we have to learn to trust the car and its functions – the brakes, the gears, our ability to steer it. It's no different with an autonomous vehicle. It's our job as an innovation leader to build this trust level by level." (BMW, 2019). (SH: OEM) - Automotive companies would do well to understand consumer expectations and bake them into the design process itself (SH: OEM) - where the notion of trust is described as the need for a feeling, in terms of comfort towards the technology, of trust to be created, rather than engaging with the customer regarding the sourcing of customer data as the literature suggests (SH: OEM) - Trust does present an inherent danger when relied upon and stakeholders demonstrate that trust must remains nuanced. With devices becoming safer, interestingly accident rates tend to initially increase (SH: Watchdogs) - over-trusting (SH: Watchdogs) - "Trust is not given, but earned," (Here, 2018) as stated in the data collected, where only 19 % of customers stated with certainty that they would be likely to use an autonomous vehicle meaning that clearly that trust has not yet been earned with customers. (SH: Watchdogs) - Driving pleasure: "symbol of freedom" (Ericsson, 2018) (Consumers) - "a sense of freedom and a love of driving are often closely connected to car ownership" (Ericsson, 2018) - Chinese people have a high affinity to technology, but are already used to sharing services due to densely populated cities and the presence of third generation households meaning they have fewer reservations towards data security and data use (Mercedes-Benz, 2019). (OEMS)
Consent	- Consciousness - users have not explicitly provided consent, which is to be expected through the integration of technology in

	modern society, however, does present a concern. Consent must be expressed in the category: full of conscious data collection and use, as the confirmed by the literature. - the seamless integration of the devices in daily lives, consumers no longer take the time to understand the IoT devices' operation and function resulting in a disconnect between our understanding and participation with digital devices - significant burden of responsibility on the auto company to be candid about the capabilities of the vehicle and avoid any risk of misrepresentation" (Capgemini, 2019) - BMW stated that a database of 5 million kilometers of driving data is needed to make a substantial base for AI to be able to autonomously navigate the roads using the gathered data. it is unclear where this data is gathered. BMW stated they do this through a testing program but do not specifically note that the data is exclusively gathered through this program (OEMS)
Transparent Data Collection	- made aware of the benefits of AVs - "Autonomous vehicles make older people who need assistance, as well as people without a driver's license, more mobile. And according to all the forecasts, the number of traffic deaths will be significantly reduced." (Mercedes Benz, 2019) (OEM) - Millenials greatest interest, least fear - Young people and users of local public transportation are also among the target groups that are more open to the idea of autonomously driving vehicles and better prepared to pay for them" (Mercedes-Benz, 2019) (OEM) - Barrier to adoption - "despite the surge in positive consumer sentiment, excitement and anticipation, barriers to adoption remain with respondents saying that purchase or adoption of a driverless vehicle is dependent on vehicle security (73%) and system security (72%)." (Capgemini, 2019)
No Trolley-cases	- Cultural shift - Like with any other emerging technology whenever new things become possible, the culture shifts around it." (OEM) - Humans will adapt to the situation of living with AV as opposed to having to teach the AV's all required cases making their movements more obvious like that way humans talk differently to primitive voice assistants - stating that a database of 5 million kilometers of driving data is needed to make a substantial base for AI to be able to autonomously navigate the roads using the

	gathered data. (BMW) (OEM) -