The Ethical Question of New Technology in Vehicles: Is It Worth the Trade-Off?

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Steven Peng

Spring 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

The Risks of Modern Automotive Technology

Every year, automotive manufacturers compete to be the first to design and develop innovative technologies and features to improve convenience, comfort, and safety, but manufacturers may also be increasing the risk of the vehicle being compromised while also jeopardizing the occupants privacy (SAE, 2018). One of the major drawbacks of implementing new "smart" features in vehicles is that more vulnerable endpoints are created, which allows malicious entities to compromise and potentially gain control of the vehicle (Sorokanich, 2015). These new "convenience" features can put both the occupants and the public in danger, as a vehicle that prioritizes the malicious entities inputs over the driver's input can cause major damages and injuries to everyone in and around the vehicle. The other major drawback relates to the privacy of the driver's data, as nearly all modern "smart" vehicles have a variety of sensors and data that is relayed back to the manufacturer for analytical purposes. From the manufacturer, however, a driver's personal driving habits can then be sold off to a third-party entity, such as an insurance company, to be used to calculating personalized insurance rates for the driver (State Farm). To fully understand the consequence of such new features in vehicles, the risk analysis framework along with the technological fix framework is utilized to answer the following question: what security and privacy tradeoffs do automotive manufacturers make when implementing new technology into their vehicles, and how do these decisions impact the general public?

Methodology

This research question is answered through a combination of political and discourse analysis. The political analysis determines how various countries regulate new technologies in

vehicles, as well as any data regulations that the manufacturers may be obligated to meet. For example, the United States Health Insurance Portability and Accountability Act protects the sharing of a patient's data without their consent within the healthcare industry (Health Insurance Portability and Accountability Act). Discourse analysis determines the public opinion of such technologies in vehicles, with a strong focus on public forums such as Twitter, YouTube, and Reddit from both general consumers and professional security researchers. Some examples of keywords that are used on these sites to find relevant posts and papers are "cybersecurity," "smart cars," "technology in cars," "smart car dangers," "vehicle vulnerabilities," and "data ethics." The information analyzed is organized based on the applicable STS framework and presented as separate examples.

The History of Automobiles

In 1885, the very first gas-powered automobile was introduced by Karl Benz, founder of Mercedes-Benz (Mercedes-Benz Group). The three-wheeled vehicle had a single-cylinder four stroke engine which produced 0.75 horsepower and could seat two passengers at a time (Mercedes-Benz Group). While these features of an automobile may not sound impressive in today's terms, this invention centuries ago would lead to the development of the multi trillion-dollar automotive industry today (IBISWorld, 2021). After the initial development of the automobile from Karl Benz, a wide assortment of new technologies that would improve the occupants' safety, comfort, and convenience were implemented from a variety of automotive manufacturers, such as three-point seatbelts in 1959 from Volvo, air conditioning in 1953 from Chrysler, and automatic parking in 2003 from Toyota (Jardine Motors Group).

Many of these features and innovations are only possible because of the advancement in technology which has allowed integrated circuits to become denser with transistors at an even cheaper cost than before. This observation is known as Moore's Law, which states that the density of transistors within an integrated circuit would double every two years, while the cost would decrease by the same rate (Moore, 2006). The reduced cost of complex circuits has allowed for manufactures to implement new features and technologies within their mass-produced vehicles, such as a combination of radars of various ranges, light detecting and ranging (LIDAR), and cameras to use for parking assists and front crash prevention (Insurance Institute for Highway Safety, 2021). The implementation of such features and sensors benefits the consumers by increasing their safety, convenience, and comfort at the cost of a slight premium, while the manufacturers would be able to collect data from the sensors to both improve their technologies and to sell off to third parties, which according to McKinsey & Company can become up to a 750-billion-dollar industry by 2030 (McKinsey, 2016). McKinsey & Company also reported that consumers were willing to share the data collected from their cars to the manufacturers if it would increase their safety, convenience, or save them time and money (McKinsey, 2016). While new safety features may seem like all positives for the consumers, there are some privacy and safety issues can arise from this massive amount of data collection and sharing.

To implement features such as automatic parking and adaptive cruise control into modern vehicles, it is required that the vehicle's engine control unit (ECU) can control and actuate all of the relevant mechanical components of the vehicle, such as the gas pedal, brake pedal, and the steering wheel. Adding this functionality of controlling mechanical aspects of the vehicle

electronically introduces a new attack vector for malicious entities to aim for, as they can now attempt to control mechanical aspects of the vehicle remotely, which can put both occupants and the public at risk. For example, in 2015 two security researchers, Charlie Miller and Chris Valasek, were able to hack a 2014 Jeep Cherokee remotely through a vulnerability in Stellantis' in-house infotainment system, Uconnect. This vulnerability allowed Miller and Valasek to gain access to the vehicle's control system, giving them the ability to remotely kill the engine, steer the vehicle in any direction, and enable or disable the braking system all remotely, which could compromise the driver's safety (Sorokanich, 2015). This vulnerability led to Stellantis recalling over 1.4 million impacted vehicles to update the software within the Uconnect infotainment system to patch the vulnerability (Fiat Chrysler Automobiles). As vehicles gain more innovative features to improve the safety of the occupants through a combination of hardware and software, the manufacturers may unintentionally be doing the opposite.

Risk Analysis, Technological Fix, and Modern Automotives

The Risk Analysis framework is used to determine the tradeoffs that automotive manufacturers make when implementing new technologies into vehicles, along with how they impact the consumers and the general population. According to Ulrich Beck, a German sociologist, risk can be described as "a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself" (Beck & Ritter, 1992). There are some debates on Beck's definition of risk, as Gabe Mythen, a professor of Criminology at the University of Liverpool, claims that "the abstract and sweeping nature of Beck's argument tramples indelicately over the idiosyncrasies and intricacies of lived cultural experiences" (Mythen, 2004). Mythen specifically points out that the argument Beck portrayed is purely theoretical and not

backed by any experience. That being said, there is a lot of inherent risks from emerging technologies in the automotive industry, especially in regard to the privacy of the users personal data. Along with that, there are some inherent risks with the operation of a motor vehicle that stem from operator error, which can also lead to technological solutions that would be considered a technological fix to a problem that requires either a solid social or political solution to properly solve.

The phrase "technological fix" was coined by nuclear physicist Alvin Weinberg and is defined as "a means for resolving a societal problem by adroit use of technology and with little or no alteration of social behavior" (Weinberg, 1978). Byron Newberry, a Mechanical Engineering Professor at Baylor University, also agrees with Weinberg that technological fixes are more of a "band-aid" fix to a constantly evolving problem that must be fixed through social or political means, to name a few (Newberry, 2005). In the automotive industry, there are many examples of technological fixes, such as a "driver awareness systems," that aims to solve the issue of drivers not having their full and undivided attention to the road. However, if the driver was falling asleep at the wheel, perhaps they have been working too many hours as a driver and regulations should be introduced to limit or reduce the cumulative time that drivers are on the road. The technological fix framework was used to analyze various technological solutions implemented within the automotive industry, and to determine their necessity as well as the pros and cons that they introduce.

Results and Discussion

To summarize, the customer's private data stored within new "smart" vehicles is commonly used to both improve features implemented by the automotive manufacturer and to

sell off to third party companies. If the sharing of data between the manufacturer and third parties is continued in the future, then it can lead to a dangerous future which may compromise democracy as a whole. Along with that, automotive manufacturers are not securing their vehicles enough from cybersecurity attacks and are introducing vulnerabilities at various points of the manufacturing and maintenance process. Automotive manufacturers are also implementing technological solutions to problems that may be better solved through the implementation of new policies and societal changes.

Starting with the Risk Analysis framework as the basis of analysis, there are many inherent security and privacy risks as vehicles become more and more complex with features. One major issue that spans multiple technological-based industries is the privacy of the user's data. With the addition of a variety of sensors that are advertised for use to implement convenience and safety features of the vehicle, the data that the sensors collect can be sent back to the manufacturer to be analyzed then either sold off or given to a third party for a monetary value. To the consumer, this data can both be used for both good and bad, as manufacturers can use the data collected to redesign components to make them more durable or safer, while third parties can use the data to target customers with ads, such as specialized insurance plans based on their driving habits, for example (State Farm, 2021). On a similar note, various insurance companies do offer systems for customers to willingly have their driving habits tracked and sent automatically to them to receive a discount on their policy, such as State Farm's Drive Safe & Save™ program, in which they provide a variable rate discount based on a variety of basic driving factors, such as rate of acceleration, hard braking events, sharp turning events, speeding, and phone usage (State Farm, 2021). At a glance, most of this data required can be obtained by

an accelerometer and would not require any other data sources, but State Farm does require the customer to provide their location data as well to help collect the aforementioned data. State Farm retains location data as a feature to the user to show their driving habits over the course of a trip, but the issue with requiring location data from the customer is if a malicious entity were to hack into State Farm's systems, then they would have access to the customers' past and present locations, which can pose as an extremely large safety risk, especially if the customer were a very important person. For example, if the malicious entity knew when the customer was out of the house, then they would be able to rob their house and get away well before the customer gets back home.

Another risk with smart vehicles is that the addition of new technologies would provide malicious entities more possible entry points to one of the vehicles' various modules, giving them control over the vehicle and potentially putting the occupants and any immediate bystanders at risk. For example, in 2015 security researchers Charlie Miller and Chris Valasek were able to hack into a 2014 Jeep Cherokee through a vulnerability in the vehicle's Wi-Fi hotspot that was built into the Uconnect infotainment system, allowing them to control nearly every aspect of the vehicle remotely, such as the engine, the steering wheel, and even the brakes, which caused Stellantis to recall over 1.4 million vehicles (Sorokanich, 2015). If this vulnerability were to fall in the hands of a malicious entity before a security patch could be applied to the impacted vehicles, then millions of people could have been injured or killed by forcing the vehicle to act recklessly and provoke a high-speed accident. The primary takeaway is that by adding a convenience feature such as Wi-Fi to the vehicle to improve the passenger's experience, a vulnerability was introduced that the manufacturer should have caught if the

system was fully tested before it was introduced into production. Unfortunately, there are many processes that manufacturers skip throughout the design and manufacturing process that would help catch vulnerabilities such as this one. A study titled “Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices” by the Ponemon Institute, a company dedicated to investigating and researching cybersecurity practices of various businesses and governments, found that over 41% of suppliers and ~18% of OEMs did not have a dedicated cybersecurity team, and that over half of the people interviewed believe that they do not have the necessary skills and resources to properly combat cybersecurity issues (SAE et al., 2018). As technology advances in the automotive industry, OEMs and suppliers must be willing and able to allocate more resources to combat cybersecurity risks throughout the entire manufacturing and supply chain, as any faults within the process can cause costly delays and negative public relations (PR) for the company, which would hurt the company in both value and trust from the customers.

To mitigate such risks, manufacturers and politicians alike must come together and enforce policies and regulations to ensure that modern vehicles are secured from such vulnerabilities from the entire design, manufacturing, and delivery process, including future support such as software and hardware updates for all manufactured vehicles to promote safety. In terms of public policy, many countries have started to implement or have already implemented automotive specific data policies that manufacturers must follow. For example, the Cyberspace Administration of China collaborated with other ministries to draft up the Provisions on Management of Automotive Data Security, which provides guidelines on the processing of automotive data (Wu et al., 2021). There are four guidelines provided: that all data be processed within the vehicles unless it is absolutely necessary to process it outside the vehicle; no data is

retained unless the driver consents to it; the specifications of the hardware to measure data must be specified according to the desired usage; and any data processed must be desensitized and anonymized during processing (Wu et al., 2021). These guidelines provided a solid foundation of guidelines that all OEMs, suppliers, and manufacturers should follow to protect the customers data from malicious usage from external entities. In the United States, legislation has also been introduced to Congress to enforce similar concepts to the Provisions, but with a stronger focus on informing the consumer of the risks and any cyber incidents that the vehicle they own are involved in. Named the "Security and Privacy in Your (SPY) Car Act of 2019," the bill introduces regulations that would require manufacturers to complete three tasks: implement systems that would defend against unauthorized access to the customer's driving data, the vehicles critical systems, and the vehicles electronic control system; adding a window sticker to vehicles being sold that would rank how well the vehicle defends the customers private data and resiliency against cybersecurity attacks; and a way to notify customers about the collection and usage of their personal data, requiring the customers consent to use their data for marketing purposes, and to allow the customer to opt out of any data collection (116th Congress, 2019). As a final example, the United Kingdom has also released a set of eight key cybersecurity principles for any and every party involved in the automotive industry to follow to ensure and maintain a secured process from the beginning of the design process to the end of the vehicle's life. The primary principles revolve around everyone involved in the process to collaborate and work together to validate and secure the vehicle throughout its usable lifetime, having appropriate incident response processes in place at every stage of the process, and designing the system around a "defense-in-depth" philosophy (HM Government, 2017). All of these processes are

being implemented by various countries governments to mitigate possible cybersecurity risks that come with the implementation of new technology in the automotive industry. Without these policies to follow, the automotive industry would be putting itself at risk for future incidents that could cause massive harm to the public, potentially recreating the scene from *The Fate of the Furious* where hundreds of vehicles were hacked and remotely controlled to chase down and immobilize a chosen target (Gray, 2017). All automotive manufacturers, especially those pushing the boundaries of new technologies and features, must consider and mitigate all of these risks from start to finish of the lifecycle of the car in order to maintain a safe society.

In one final scenario, automotive manufacturers must strongly weigh the benefits and risks that come with making their vehicles connected to the internet, as not only does it create an avenue for third party developers to come up with creative uses with the vehicles application programming interface (API), it would also create a large vulnerability point for malicious entities to take advantage of to control the vehicle and potentially steal any user data stored within the vehicle as well. For example, in late 2021 19-year-old German security researcher David Colombo noticed an exploit with TeslaMate, a self-hosted data logger for Tesla owners, which would allow external users to access the TeslaMate dashboard and view current and previous locations of the vehicle, previous navigation requests, current speed, and more (Colombo, 2022b). After Colombo poked around, he was able to find the API key used to connect to the Tesla stored without any form of encryption, which would allow him to send various commands to the Tesla, such as unlocking the doors, enable keyless driving, and more (Colombo, 2022b). The ability to unlock the door and enable keyless driving while also knowing the current location of the Tesla meant that malicious entities could target a vulnerable Tesla and

effectively steal it in broad daylight. During this process, Colombo attempted to get in contact with Tesla owners who were impacted with this vulnerability, but with little success Colombo went to Twitter and tweeted “So, I now have full remote control of over 20 Tesla’s in 10 countries and there seems to be no way to find the owners and report it to them…,” which went viral with nearly two thousand retweets and eight thousand likes (Colombo, 2022a). There were various reactions on Twitter, ranging from other security researchers inquiring about the technical details of the vulnerability to users suggesting that Colombo remotely destroy the Tesla to spare the owners from owning such a vehicle (Colombo, 2022a). While some reactions were helpful in trying to suggest how Colombo could contact the impacted parties, the reactions that attacked Tesla depicts some of the stigma around the concept of a smart car in favor for more traditional vehicles that are not internet connected. In the end, Colombo was able to get in touch with both Tesla and the maintainers of TeslaMate to implement a solution, which involved Tesla revoking thousands of impacted API keys and TeslaMate releasing a patch that would encrypt the API key within the database as well. This situation emphasizes the importance of securing the product that automotive manufacturers create from start to finish, as this situation could have been avoided if the API that Tesla provided had different scopes based on the situation, such as read-only access if the application only needs to pull data or limited write-access if the application only needs to use one specific feature. Another solution that could be implemented industry wide is a dedicated security team that would vet and test the usage of their APIs on popular products to prevent situations such as this one from happening again in the future, as this can lead to negative PR in the long run if developers continue to create insecure applications that can introduce risk to and potentially compromise the vehicle.

All of the possible risks that comes with new technology in automobiles can set forth a dangerous precedence if not properly addressed in a timely manner by both the manufacturers and the government. For example, if standard practice in the future allows for the user's data to be shared with third parties by the manufacturer, then it can lead to a system where various parts of society becomes linked together, similar to China's "Social Credit" system (Canales, 2021). Such a system will greatly reduce the amount of control one has over their own life and will allow either third parties or even the government more control over their lives. As the main reason third parties want the user's data is for targeted advertisements to increase their profits, then this would further lead society to one focused around personalized ads, in which companies are seeking to make even more of a profit. Once a company is large enough, then they can actively influence politics and legislation, similar to how Disney has kept extending the deadline for copyright laws to prevent Micky Mouse from entering the public domain (Tillay, 2021). Permitting a corporation to oversee and influence politics undermines the concept of democracy, in which people would not have a say for policies and laws that can impact them. As many of the risks that come to light from the introduction of new technology in vehicles can lead to an undesirable future, the question of whether the problem is best fixed with technology must also be investigated.

The technological fix framework is used to analyze the new features on vehicles to determine how necessary they may be, and whether there is a more appropriate solution to the problem at hand. For example, some new cars have a built-in "driver monitoring system" that can track the driver's awareness and control the vehicle if the driver is not paying attention to the road (Cvahte et al., 2019). While this technology may seem like a wonderful solution to drivers

who may be prone to falling asleep, it does not address the root of the problem, which is why are the drivers falling asleep at the wheel? Are the drivers truck drivers who are scheduled too many hours in a day and are unable to properly rest before their next shift? Some forms of the eye-tracking technology may require the data to be analyzed or shared with the manufacturer, which can lead to the risk of the data being sold to a third party for nefarious uses. The risk of user's data being sold off to third parties is increasing, as the automotive data industry is slated to become nearly a 750-billion-dollar industry according to a study from McKinsey and Company (McKinsey, 2016). The development of a "driver monitoring system" to reduce accidents was done in good faith but can be considered a technological fix as there are other, better ways to solve the root issue at hand.

In another attempt to solve the problem of distracted driving that came along with the invention of the smartphone, Apple and Google, the two primary smartphone developers, have implemented a "hands-free" infotainment system for the driver to interact with their phones through their vehicles navigation system, called CarPlay for the iOS ecosystem and Android Auto for the Android ecosystem. The primary benefit of this system is that drivers can access and view relevant content from their smartphone on their vehicle's larger navigation system, if installed. The driver can also interact with the infotainment system through voice commands or through either the infotainment system's touch screen or rotary dial, if so equipped. In theory, since the driver does not have to focus heavily on their relatively small smartphone screen to view driving directions but instead can quickly glance at their vehicle's navigation system, the driver's eyes will be more focused on the road. In reality, studies such as the one by a collaboration between IAM RoadSmart and Transport Research Laboratory Limited show that

drivers that use such infotainment systems have either just as slow or an even slower reaction time than drivers who are actively using their smartphone instead (Ramnath et al., 2022). In this study, drivers who used the touchscreen interface on the infotainment system had a much slower reaction time than drivers who either texted while driving or used voice controls to control the system (Ramnath et al., 2022). While many of the new features on vehicles either enhance the driver's comfort and safety or reduce the chance that the driver is distracted, some technological solutions are used as a temporary solution to a complex problem that would require either a social or political change to solve.

With the advancement in technology in vehicles to introduce new features, there has also been an increase in complexity to vehicles that eventually trickle down to additional costs to vehicle owners. For example, Jason Fenske from the YouTube channel Engineering Explained, explains that the cost to repair and maintain vehicles has increased as vehicles become more technologically complex since specialty tools that can communicate to the vehicle's various modules are required (Fenske, 2022). The requirement of specialty tools to work on the vehicle would prevent many do-it-yourselfers and local mom-and-pop shops from working on such vehicles, effectively requiring owners to go to the dealership to get their car maintained and repaired, which can at times cost an exorbitant amount of money, potentially even 2200% more than necessary as they are able to dictate the repair options knowing that the owner does not have any other options to repair the car as specialty shops for new vehicles with advanced technologies are very hard to come by (Benoit, 2021). Requiring specialty tools to work on new vehicles have become increasingly common in the automotive industry to dissuade owners from fixing their own vehicles at a lower cost, which can make the requirement appear as a

technological fix that is rooted for the manufacturers to make a profit from servicing their vehicles.

One final argument that showcases how modern vehicles are implementing technological fixes to solve societal issues is the increasing prevalence of autonomous vehicles. Autonomous vehicles are being developed so that the occupants of the vehicles can be transported from one location to another without actively controlling the vehicle, allowing them to focus on other tasks. One of the primary benefits with a fully autonomous fleet of vehicles on the road is that it should nearly fully negate the human error factor of accidents that come from distracted driving or poor driving abilities, making the roads much safer for both pedestrians and occupants of the vehicle. To successfully implement an autonomous vehicle, a lot of data must be processed by the vehicle to determine where it is relative to everything else, where it is able to drive, and where everything else is to avoid hitting other objects. This data can include both location data and camera data of everything around the vehicle, which could lead to the owner's location and driving trends to be sold off to a third-party company to target relevant ads based on the owner's frequent locations, as well as become a target for malicious entities to obtain as they would be able to know exactly when the owner is in and out of the house to determine the best time to rob the owner's house. While there are many technological solutions to the distracted driver issue, there may be a better solution that can be implemented both nationally and socially, such as an increased focus and expansion on affordable public transportation. A stronger focus on improving the public transportation system would allow people to be transported from point A to B without actively being engaged with the vehicle while also benefitting the ecosystem by reducing emissions from the decreased number of personal vehicles on the road. If one concern

is the lack of public transportation at certain times or inaccessibility of public transportation depending on the location, then companies that are able to expand permanent remote work for employees. There are many possible solutions available on both a political and social level that can be implemented to offset the risks introduced with new technologies on vehicles, and consumers should also be aware of all possible risks when buying and operating a smart vehicle.

Limitations and Future Work

Some limitations to this project include the availability of up-to-date survey data from both automotive manufacturers and the general public, as well as the availability and collection of public opinion from various sources in a condensed form. Another limitation is the lack of motifs for some of the public comments, and whether their opinions are biased because of personal experiences, political affiliation, or something else. In the future, a worldwide survey of both the general public and automotive manufacturers should be performed at set intervals to determine if there are any long-term trends to see if public perception changes based on the amount of risk that new technology in vehicles introduces from both a safety and security standpoint, and to see if automotive manufacturers are actively working towards reducing that amount of risk as well.

Conclusion

In conclusion, many automotive manufactures that implement new technologies in their vehicles are using the customer's private data to further advance their technology and to potentially sell off to third parties for a profit. Along with that, there is a chance that if a malicious entity is able to access such data then the customers safety will be put at risk, especially if life location data is included. If automotive manufacturers and politicians do not

work together to secure new and future vehicles from cybersecurity threats, then there is an increased risk of both personal and public property damage if the vehicles were to be remotely controlled from a malicious entity, as well as the customer's personal data being compromised. The cumulative risks of new technology, if left unchecked by both the government and manufacturers, will lead to a dangerous company and data-led society that may undermine democracy as a whole.

Work Cited

116th Congress (2019): *SPY Car Act of 2019*. (2019, July 18). https://www.congress.gov/bill/116th-congress/senate-bill/2182

Beck, U., & Ritter, M. (1992). *Risk society: Towards a new modernity*. Sage Publications.

Benoit, R. (2021). *Tesla wanted $16,000 to fix this NEW Model 3, we did it for $700! The importance of Right to REPAIR!* YouTube. https://www.youtube.com/watch?v=vVSw3KSevEc

Canales, K. (2021). *China's 'Social Credit' system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy*. Business Insider. Retrieved April 21, 2022, from https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

Colombo, D. (2022a). *So, I now have full remote control of over 20 Tesla's in 10 countries and there seems to be no way to find the owners and report it to them...* Twitter. https://twitter.com/david_colombo_/status/1480632304045330433

Colombo, D. (2022b). *How I got access to 25+ Tesla's around the world. By accident. And curiosity.* Medium. https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028

Cvahte Ojstersek, T., & Topolsek, D. (2019). *Eye tracking use in researching driver distraction: A scientometric and qualitative literature review approach*. Journal of eye movement research. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7880134.

Fenske, J. (2022). *Are Modern Cars Too Complicated? What The Future Entails*. YouTube. https://www.youtube.com/watch?v=yTXsg0bUKUI

Fiat Chrysler Automobiles. (2015). *Safety recall R40 / NHTSA 15V-461 Radio Security vulnerability*. National Highway Traffic Safety Administration. https://static.nhtsa.gov/odi/rcl/2015/RCRIT-15V461-4869.pdf

Gray, F. (Director). (2017). *The Fate of the Furious.* [Film]. Universal Pictures.

Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, § 262, 110 Stat.1177.

HM Government. (2017). *The key principles of vehicle cyber security for connected and Automated Vehicles*. Gov.UK. https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/

IBISWorld, (2021). *Global Car & Automobile Sales—Market Size 2005–2027*. IBISWorld. https://www.ibisworld.com/global/market-size/global-car-automobile-sales/

Insurance Institute for Highway Safety, (2021). *Advanced driver assistance*. IIHS-HLDI Crash Testing and Highway Safety. https://www.iihs.org/topics/advanced-driver-assistance

Jardine Motors Group. *The History of Car Technology*. Jardine Motors Group. https://news.jardinemotors.co.uk/lifestyle/the-history-of-car-technology

McKinsey. (2016). *Monetizing car data*. McKinsey & Company. https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing%20Car%20Data.ashx

Mercedes-Benz Group. *Benz Patent Motor Car: The first automobile (1885–1886)*. Mercedes-Benz Group. https://group.mercedes-benz.com/company/tradition/company-history/1885-1886.html

Moore, G. E. (2006). Cramming more components onto integrated circuits, reprinted from Electronics, volume 38, number 8, April 19, 1965, pp.114 ff. *IEEE Solid-State Circuits Society Newsletter*, *11*(3), 33–35. https://doi.org/10.1109/n-ssc.2006.4785860

Mythen, G. (2004). Defining Risk. *Ulrich Beck: A Critical Introduction to the Risk Society*. (pp. 53-73). London, England. Sterling, Virginia. Pluto Press.

Newberry, B. (2005). Technological Fix. In C. Mitcham (Ed.) *Encyclopedia of Science, Technology and Ethics*. (Volume 4., pp. 1901-1903). New York, New York. Macmillan Reference USA.

Ramnath, R., Hyatt, T., Chowdhury, S., & Kinnear, N. (2022). *Interacting with Android Auto and Apple CarPlay when driving: The effect on driver performance*. IAM RoadSmart. https://www.iamroadsmart.com/campaign-pages/end-customer-campaigns/infotainment

SAE, Synopsys. (2018). *Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices.* Ponemon Institute, from https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf

Sorokanich, B. (2015). *Why you still shouldn't panic about car hacking*. Road & Track. https://www.roadandtrack.com/new-cars/car-technology/a26144/why-you-still-shouldnt-panic-about-car-hacking/.

State Farm. (2021). *Drive Safe & Save™ Mobile - State Farm®*. State Farm. https://www.statefarm.com/customer-care/download-mobile-apps/drive-safe-and-save-mobile.

Tillay, M., 17, P. J., & Meganne Tillay Reporter. (2021, June 17). *The fight to continue Mickey Mouse's copyright*. The Courtroom. Retrieved April 21, 2022, from https://thecourtroom.org/the-fight-to-continue-mickey-mouses-copyright/

Weinberg, A. (1978). *Beyond the Technological Fix*. Internal Institute for Energy Analysis report. Oak Ridge Associated Universities.

Wu, S., Yan, P., Zhu, S., Sun, T., Xie, Z., & Yu, F. (2021). *Continued Development of Data Security and Protection in China – All You Need to Know about China's Latest Data Implementation Rules and the New Data Guidance for the Automotive Industry*. Paul Hastings. https://www.paulhastings.com/insights/client-alerts/continued-development-of-data-security-and-protection-in-china-all-you-need