Prospectus

Evaluation of VDOT Safety Service Patrols
to Improve VDOT Response to Incidents and Crashes
(Technical Topic)

Privacy Concerns in the World of Autonomous Vehicles
(STS Topic)

By

Matthew Orlowsky

STS 4500-017

10/30/2019

Technical Project Team Members: Bunny Campbell, Emma Chamberlayne, Julie Gawrylowicz, Colin Hood, Allison Hudak, and Emilio Rivero

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.

Signed: Matthew Orlowsky

Approved: _____ Date 12/4/2019
Professor Rider Foley, Department of Engineering and Society

Approved: _____ Date 12/5/2019
Professor Michael Porter, Department of Engineering Systems and Environment

Introduction

The Virginia Department of Transportation (VDOT) funds Safety Service Patrol (SSP) Vehicles to assist in traffic control and general safety assistance. SSPs are "free of charge" vehicles that travel the Virginia interstates and provide emergency assistance to motorists (Virginia, 2019). The purpose of the SSP program is "to promote the efficient and effective flow of traffic through effective incident detection, verification, and notification to appropriate agencies to initiate rapid clearance of an incident" (Edara, 2006, p. 10). Unfortunately, The SSP vehicle program currently faces inefficiencies and constraints in their existing route selection and scheduling process due to the fact that these routes were created primarily using informal evidence and data that lacked scientific support. By using routes that are not optimized based on incident reports, VDOT has no guarantee that they are deploying SSPs to the areas that are most in need of assistance.

While their primary function is to assist traffic control and aid traveler's navigation through potentially unsafe areas, VDOT measures the performance of their program using metrics of how quickly they can arrive on the scene. Can these metrics be used to create an optimal VDOT SSP program schedule that will result in the fastest response time to the largest number of incidents? The new enhanced schedule is expected reduce congestion, disruptions, and secondary accidents. The hope is that this will help VDOT use their resources efficiently to keep Virginia moving.

For the STS Research Project, I will focus on a slightly different topic although it is still under the broad category of transportation technology. One of the most exciting innovations of today is the promise of autonomous vehicles. Autonomous vehicles (AVs) are expected to

occupy 25% of the global market by 2040 (Taeihagh, 2019). AVs have the potential for an abundance of benefits including improved safety, shorter commutes, less stress, fewer environment impacts, and freedom for immobile persons (Collingwood, 2017). The passenger is promised access to Wi-Fi, less risk of accidents, and avoiding traffic and road construction. However, these benefits can only be realized if the algorithms that navigate the autonomous vehicles are given vast amounts of data via GPS, voice-recognition, cameras, and other sensors. One thing that must be considered is what will happen with all of this information. The data includes not only locations and preferred routes, but also shopping habits, on-line activity, and even voice recordings. What if hackers were to get a hold of this data? Will robbers know when you are away from home? What possible things will the security agency be able to do with the collected data? My goal will be to examine the current vulnerabilities associated with autonomous vehicles and explore ways to mitigate the potential risks in privacy, security, and autonomy. Although autonomous vehicles promise many benefits, what are the potential privacy concerns and can actions be taken now to alleviate these risks? Elements to be considered include transparency, data minimization, security, access, and accountability (BCLP, 2018). The hope is that our privacy will be protected and that the car windows will be the only way that the outside world will be able to "see" us.

Technical Topic: **Evaluation of VDOT Safety Service Patrols**

The Interstate System today is plagued by constant congestion. The average driver loses 97 hours and $1,348 a year to congestion (INRIX, 2019). In addition to being costly, Zhang and Batterman (2014) report that "vehicle emissions have become the dominant source of air pollutants" (p. 307). According to Cambridge Systematics (2005), one of the major causes of congestion is traffic incidents (p. 14). Traffic incidents can block lanes from traffic flow, create backups by distracting drivers, and lead to secondary accidents. Virginia is uniquely impacted by congestion issues due to the several metropolitan areas across the state. To combat congestion, the Virginia Department of Transportation (VDOT) established the Safety Service Patrol (SSP) program in the late 1960s to assist drivers and quickly clear traffic incidents (Virginia Department of Transportation [VDOT], 2017). The goal of the program is "safe, quick clearance [of traffic incidents] to reduce secondary crashes, reduce[d] incident duration and improve[d] travel time reliability" (VDOT, 2017, slide 3). SSPs follow predetermined routes along highways in Virginia in search of traffic incidents. However, these routes were created using primarily anecdotal evidence and lack support from data. By using routes that are not optimized based on incident reports, VDOT has no guarantee that they are deploying SSPs to the areas that are most in need of assistance.

This capstone seeks to create optimized routes for SSPs on I-95 and the connecting interstates. An optimal schedule will reduce incident duration and improve travel time reliability, leading to decreased congestion overall. Additionally, the team seeks to use the years of incident and response data collected by VDOT to evaluate the success of the SSP program. This could inspire lawmakers to further invest in the program and help it to better achieve the mission. VDOT is currently investigating expanding their SSP coverage along I-95 and support for the program's success could accelerate this process. The team will characterize incidents and response times in order to inform a model that will optimally place SSPs along I-95 in Virginia. Using incident data

from 2013 to 2018, the team will establish the probability of an incident for a segment of I-95. These probabilities will be established for both directions of the interstate by time of day and day of week. This will identify areas of high risk for incidents, therefore in critical need of SSP assistance. With this information, the team will also be able to identify areas that are currently underserved by the routes that the VDOT has established. The team will then estimate the time it will take SSPs to respond to an incident using historical data. By determining the maximum travel time for various segments on the road, the team will identify areas in most need of frequent coverage in order to decrease overall response times. Combining these two information sources, the team will build a model that will output a recommended route schedule for the SSPs. This schedule will allow VDOT to route SSPs to most effectively respond to traffic incidents on I-95.

Privacy Concerns of Autonomous Vehicles

Autonomous vehicles are promised to achieve the remarkable by transporting passengers safely and stress-free to their destinations with minimal human intervention. This technology cannot exist without abundant data transfer between the car, the infrastructure, and surrounding environment (Figure 1). Sensors such as radar, cameras, and even sonar will be required to calculate and derive the routes for the vehicles (LaFrance, 2016). The different designs of self-driving systems all create and maintain internal maps of their surrounding areas using sensors and radar (Union, 2018). Software will be used to plot efficient travel paths. In addition, the vehicle may use algorithms utilizing past user statistics gathered from EDRs (event data recorders). Artificial intelligence may aid in providing the "best" user experience. Some of the information will be used to create highly specialized maps and some companies will use the metrics for research to "better understand everyday driving scenarios that can be recreated in

simulation labs and test tracks" (Gardner, 2019, p. 1). All this data is necessary for successful operation of the autonomous vehicle.

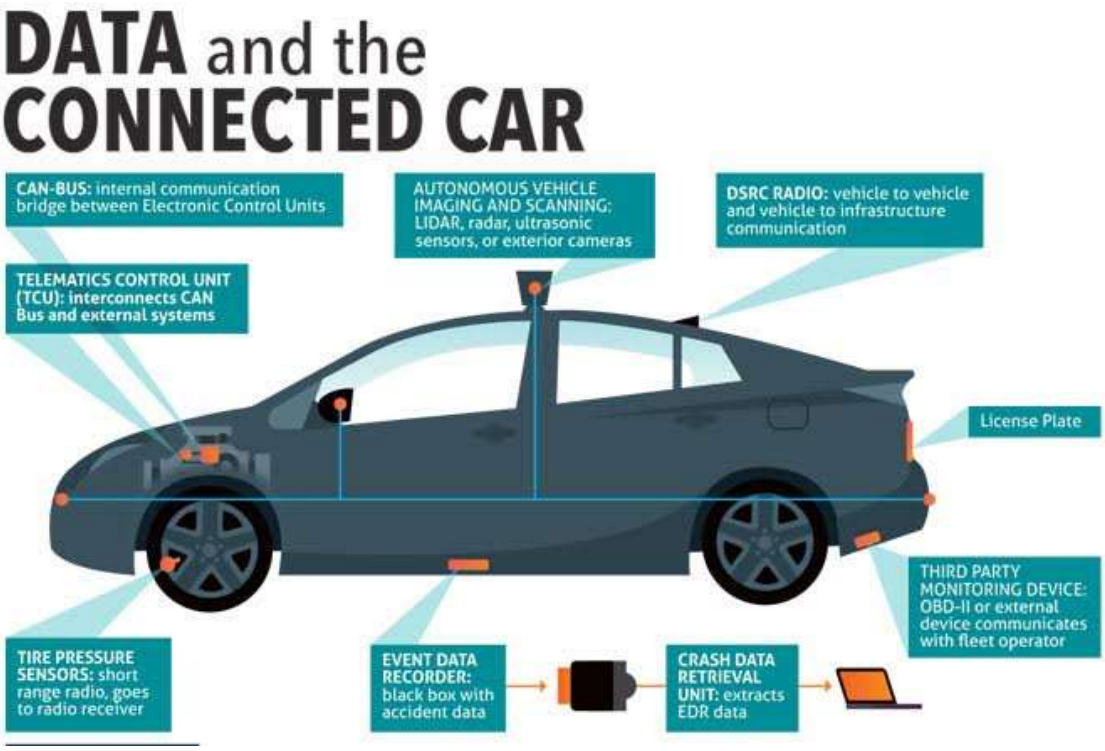

Figure 1. Data and the Connected Car (Image source: Future of Privacy Forum, 2017)

There are wide-spread human and social dimensions of autonomous vehicle technology. The technology may have enormous positive social impact for handicapped, young, and elderly people, who in the past were unable to operate a car and are promised greater freedom to travel. Although the possibilities are exciting, there is growing public concern regarding data privacy. In light of the July 2019 Capital One data breach where data from 106 million people was compromised, state and municipal legislature are considering new regulations regarding what data will be collected and how it will be used (Eliot, 2019). Additionally, consumer habits are

another area that can be potential affected. Will our purchasing behaviors alter due to vehicle advertisements suggesting shopping and dining options? How will this advertising be regulated? "Introducing the technology will potentially bring changes across the entire sphere of mobility, impacting many levels of society. At the same time, it could trigger a fundamental transformation in the way we get around" (Fraedrich, 2016, p. 622).

The sonar, radar, cameras, and wireless communication necessary for a safe and efficient ride come with numerous security dangers. User activity data has the potential to be used for manipulation and profiled advertising, and surveillance data could be used for legal and illegal tracking. The vehicle itself would be a repository of personal information that would be at risk for hacking, burglary, and misuse (Glancy, 2012). Imagine a scenario of a future of autonomous vehicles where the unsuspecting rider is manipulated by sponsored retailers and unseen persuasions due to data mining of personal travel history, emails, and shopping preferences (LaFrance, 2016). Some vehicle data remains anonymous, however, when information can be identified to an individual, then it becomes personal information, and must be protected. The moral obligations, the legal rights, and political considerations should ensure protection for individuals' civil liberties and freedoms (Glancy, 2012). Due to the social and human impacts, there must be emphasis on accountability of the roles, objectives and design approaches of the developers, including corporations, government, and researchers (Blyth et al., 2015).

Additionally, autonomous vehicle implementation requires that cities must be prepared for the changing role of the human inside and outside the vehicle, and the "consequent impacts, on sociotechnical structures and practices" (Blyth et al., 2015). Technology has grown rapidly and the regulatory environment has not grown proportionally (Collingwood, 2017). One

complexity is that neither privacy issues nor autonomous vehicles are clearly defined matters, so it is difficult to specify the interactions between them (Glancy, 2012).

The advances of autonomous vehicles can be understood with Thomas Hughes' framework of technical momentum. The development and expansion of the automobile is a conservative invention (Hughes, 1987). Automobile transportation in the United States (US) has been sustained for nearly a century. Such systems attain technological momentum when they "have a mass of technical and organizational components; they possess direction, or goals; and they display a rate of growth suggesting velocity" (Hughes, 1987, p.76). The components of the system of autonomous vehicles include all stakeholders with interests in the technology such as automobile manufacturers, technology firms, communications providers, federal and state regulatory groups, National Highway Traffic Safety Administration (NHTSA), state departments of transportation (DOTs), state departments of motor vehicles (DMVs), advertising agencies, and public commuters (Anderson et al., 2016). The evolution of large systems includes invention, development, innovation, transfer, and growth, competition, and consolidation. Theses phases are not always sequential and can overlap. Generally, during invention and development phases, inventor-entrepreneurs solve critical problems while engineers solve critical problems associated with growth and momentum. As systems grow, reverse salients develop. The technological advancements of autonomous vehicles necessitate data communication, transmission, and storage not previously required. This new functionality has now created a reverse salient due to the potential exposure of this data. The need for protection will lead to the alteration of other automobile components. This reverse salient must be addressed by the system builder, engineers, car manufactures and legislators. These problem solvers must construct centralized solutions for the privacy issues and enable coherence for future advancements (Hughes, 1987).

Issues that are identified up front during the design phase can be solutioned if the technology is still in development (Glancy, 2012). Security in automation vehicles is more important than traditional automobiles because in the case of an attack, the driver may not be available to recover the automobile. Techniques such as increased data redundancy are necessary because the redundancy will allow identification of conflicting data and allow proceeding to the recovery decision making process (Petit and Shladover, 2015). The very nature of the diverse radio communication required by the technology will require secure data collection and protection by means of data authentication, integrity, access control, encryption and sanitization techniques (Mahmood et al., 2019). Although privacy protections can be built into the architecture, to date, US state regulations have failed to address the extensive problems associated with collection, use, storage and dissemination of data generated by autonomous vehicles (Collingwood, 2017). Without clear privacy protections in place, autonomous vehicles could encounter public resistance from users who perceive them as a threat (Collingwood, 2017).

Research Questions and Methods

What are the current vulnerabilities associated with autonomous vehicles privacy, security, and personal autonomy and what are potential mitigations that can be put in place to protect the privacy of users? Can we identify current State and Federal legislature, and industry actions in the area of autonomous vehicle privacy and can we interpret if their support and participation is increasing in recent years, and if so, at what rate?

The methods that will be used for analysis will include surveys and prior literature, case law, and policy research. The communication, data transmission, and storage technology of the autonomous vehicle will be explored to understand the components associated with privacy

issues in three areas: personal information, personal autonomy, and surveillance. Vulnerabilities and the potential solutions will be identified. Content analysis will be used to evaluate each identified potential mitigation (i.e. encryption, anonymizing, data minimization, data destruction). They will be categorized according to the complexity, feasibility, and extent to which the problem is solved. This analysis will be tabulated in a chart to indicate technology and methods that can potentially ensure privacy. Car manufactures and other companies endorsing AV technology should employ "privacy by design" in order to ensure that the methods and regulations are defined up front during development (Glancy, 2012). This will establish consistency across the industry and eliminate the need for future modifications that may be difficult or impossible to put in place after the technology has advanced too far.

Researching historical data on past cases will also be completed since reporting on prior successes will bring validity to the ideas being proposed (Nash et al, 2017). Although this new technology will contain cyber dangers, many of these risks have been confronted before in other industries and if past lessons-learned can be applied to the autonomous vehicle industry, then these vulnerabilities may be contained. Successes were seen in the formation of Bluetooth Special Interest Group (SIG) which controls technological specifications, requires all members to certify their products are compliant, and performs audits to assure compliance (Nash et al, 2017).

Current and past legislative actions, hearings and testimony will be collected in order to elucidate discourse from federal, state, municipal, and auto industry participants on security and privacy. Currently only seventeen states have passed laws relating to the data retrieval from event data recorders (EDRs) (BCLP, 2018). This data will be analyzed using ranking and scoring to determine trends and statistics to see if policy and regulation implementation is increasing, and if so, at what rate.

Conclusion: Timeline and Expected Outcomes

Although autonomous vehicles promise numerous benefits, there are privacy vulnerabilities that need to be identified, understood, and mitigated in order to secure protections for users. If these issues are not addressed, consumers may become victims of personal information compromise, surveillance, and loss of autonomy. Identifying and solutioning the technology exposures should be done up-front while the technology is still in development. Unfortunately, there is no current standardization in regulations or policies. Government avoidance in putting strict regulations in place is most likely due to the desire to promote the emerging technology (Taeihagh, 2019). None the less, legislators need to act swiftly and decisively as these issues may impact the degree to which the technology is adopted, causing delays in implementation (Collingwood, 2017).

The research project on privacy issues of autonomous vehicles will involve surveying the general public through an internet based platform in December 2019 until February 1, 2020. The prior literature, case law, and policy research will have the same start and end dates. The research project deliverables will include the identification of autonomous vehicle privacy risks and mitigation proposals classified in terms of feasibility and forms of complexity. The status and trending of government and auto industry regulatory action will be presented as well as the public opinion concerning autonomous vehicle privacy and their willingness and trust of the technology. Once complete, this research can be used as guidelines or reference for future deliberations on privacy regulations of autonomous vehicles in hopes to minimize the risk of further privacy vulnerabilities.

Bibliography

Anderson, J. M., Kalra, N., Stanley, K. D., Sorensen, P., & Oluwatola, O. A. (2016). *Autonomous vehicle technology: a guide for policymakers*. Santa Monica, CA: Rand Corporation.

BCLP. (2018). Autonomous Vehicles – Data Privacy Issues. Retrieved October 9, 2019, from https://www.bclplaw.com/en-US/thought-leadership/autonomous-vehicles-data-privacy-issues.html.

Blyth, P., Mladenovic, M., Nardi, B., Su, N., Ekbia, H. (2015). Driving the self-driving vehicle: Expanding the technological design horizon. *2015 IEEE International Symposium on Technology and Society (ISTAS)*, 1-6.doi: 10.1109/ISTAS.2015.7439419.

Cambridge Systematics Inc. and Texas Transportation Institute. (2005). *Traffic Congestion and Reliability Final Report: Trends and Advanced Strategies for Congestion Mitigation: United States* (Report No. 05). Retrieved from https://ops.fhwa.dot.gov/congestion_report/congestion_report_05.pdf

Collingwood, Lisa (2017) Privacy implications and liability issues of autonomous vehicles. *Information & Communications Technology Law*, *26*(1), 32-45.

Eliot, L. (2019, August 15). Cloud Breaches Like Capital One Will Strike At Self-Driving Cars.*Forbes.* Retrieved from https://www.forbes.com/sites/lanceeliot/2019/08/15/cloud-breaches-like-capital-one-will-strike-at-self-driving-cars/#20b799cf3a49.

Fraedrich, E., & Lenz, B. (2016). Societal and Individual Acceptance of Autonomous Driving. *Autonomous Driving*, 621–640. doi: 10.1007/978-3-662-48847-8_29.

Edara, P. K., & Dougald, L. E. (2006). Identification of Core Functions and Development of a Deployment Planning Tool for Safety Service Patrols in Virginia. *Virginia Transportation Research Council*. 38.

Future of Privacy Forum. (2017, June 29). Retrieved from https://fpf.org/2017/06/29/ infographic-data-connected-car-version-1-0/

Gardner, G. (2019, September 17). Uber To Collect Mapping, Other Data For Possible Autonomous Service In Dallas. *Forbes.* Retrieved from https://www.forbes.com/sites/ Greggardner /2019/09/17/uber-to-collect-mapping-other-data-for-possible-autonomous-service-in-dallas/#4d2321d52aa4.

Glancy, D. (2012). Privacy In Autonomous Vehicles. *52 Santa Clara Law Review,* 1171, 1184.

Hughes, T.P. (1987) The Evolution of Large Technological Systems. In W.E. Bjiker, T.P. Hughes, and T. Pinch (Eds). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. MIT Press: Cambridge, MA. pp. 51-82.

INRIX research shows Americans lose 97 hours per year (2019). Retrieved from https://www.roadsbridges.com/inrix-research-shows-americans-lose-97-hours-year-congestion.

LaFrance, A. (2016, June 23). The Creepy Thing About Self-Driving Cars. Retrieved from https://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/.

Mahmood, A., Zen, H., & Hilles, S. M. S. (2019). Big Data and Privacy Issues for Connected Vehicles in Intelligent Transportation Systems. *Encyclopedia of Big Data Technologies*, 196–203. doi: 10.1007/978-3-319-77525-8_234

McCann, K. (2019, October 2). Personal Interview.

Nash, L., Boehmer, G., Hillaker, A., & Wireman, M. (2017). Securing the future of Mobility. *Deloitte Insights.* Retrieved October 14, 2019, from https://www2.deloitte .com/us/en/insights/focus/future-of-mobility/cybersecurity-challenges-connected-car-security.html.

Petit, J., & Shladover, S. (2015). Potential Cyberattacks on Automated Vehicles, *IEEE Transactions on Intelligent Transportation Systems*, *16*(2), 546-556. doi: 10.1109/TITS.2014.2342271.

Porter, M. (2019, October 2). Lecture.

Taeihagh, A., & Lim, H. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, 39(1), 103-128. DOI: 10.1080/01441647.2018.1494640.

Truitt, D. (2019, October 2). Personal Interview.

Union of Concerned Scientists. (2018). Self-Driving Cars Explained. Retrieved from https://www.ucsusa.org/clean-vehicles/how-self-driving-cars-work.

Virginia Department of Transportation. (2019). Safety Service Patrol - Travel. Retrieved from https://www.virginiadot.org/travel/safetypatrol.asp.

Zhang, K., & Batterman, S. (2013). Air pollution and health risks due to vehicle traffic. Science of The Total Environment, 450-451, 307–316. doi: 10.1016/j.scitotenv.2013.01.074