THE CHANGING MOBILITY ECOSYSTEM

OUR AUTONOMOUS FUTURE

DIGITAL FUTURES PROJECT

JULY 2018

ABSTRACT

In recent years, technology companies have demonstrated not just the capability of autonomous vehicles, but the actual feasibility of future production and rollout of this technology. Yet, most indications suggest that it may be several years, if not a decade before autonomous vehicles become mainstream in our roadway environment. What major hurdles remain? Are we as a society ready? This document provides a review of the current state of connectivity and security, the evolving vehicle and roadway landscape, regulatory hurdles, and convergence of autonomous vehicles with infrastructure and future urban planning. In the context of these developments, it is crucial that we keep an open mind, considering both long- and short-term priorities. To do so, education will be a critical component of creating a public that is ready to embrace these potentially transformative technologies.

Wilson Center

By Jeremy Spaulding, Emma Grossman, Aidan Reilly Giunta

Corresponding Author: Jeremy Spaulding, AutoNebula Group, jspaulding@autonebula.com

AUTOMOBILES HAVE COME A LONG WAY OVER PAST CENTURY

From the introduction of map-based navigation systems in 1981[1], to GPS-based navigation in 1990, to infotainment and the integration of portable media, to driver assist technologies such as blind spot warnings, adaptive cruise control and lane departure warnings, vehicles have come a long way. Automobiles are more efficient, reliable, and safer with each successive generation. Many of the technologies introduced into vehicles have the specific purpose of making the vehicles safer for drivers to operate, offer mitigations for driver limitations, or offer conveniences to make the driving experience better.

One envisioned technology on the horizon of development has been the autonomous vehicle; the car that drives itself. This futuristic technology has been envisioned since at least the 1960's, in the form of early conceptual designs, patent filings, and even some coverage by mainstream media. Through the decades the concept of the autonomous vehicle has gained increasing momentum: its frequent presence in movies and television have brought the autonomous vehicle to the forefront of our collective consciousness, while on the technological side, efforts such as closed-track research demonstrations, scale models, and concepts created by scientific researchers and technology and supplier companies, have brought these vehicles closer to full realization than ever before.

In recent years, technology companies have been able to demonstrate not just the capabilities of autonomous vehicles, but the actual feasibility of future production and rollout of this technology. Advancements in computing, algorithmic programming, and vision-based sensors, such as LiDAR, have made it possible for autonomous vehicles to become a reality. Moreover, this reality has been put into action by most major Original Equipment Manufacturers (OEMs), Tier-one suppliers, technology companies, and even startups looking to create a presence in the space. In fact, Autonomous vehicles are now emerging as a niche market in and of themselves, attracting significant financial investments that are only projected to increase even more in years to come.

Even though technological advancement has progressed to the point of realizing nearly or fully autonomous vehicles, we have yet to see autonomous vehicles on most roadways. It may even be several years or even a decade before autonomous vehicles become mainstream in our roadway environment. Why? What hurdles are we facing to roll out this technology? What are the hidden challenges that are holding back development? How long is it going to be before we actually trust a driverless car?

[1] Arlt, G. (November 22, 2016) Automotive Navigation Systems. Historic Vehicle Association. Retrieved July 14, 2018, from https://www.historicvehicle.org/automotive-navigation-systems/

CURRENT STATE OF CONNECTIVITY AND SECURITY

Today's cars are capable of sharing information with each other and have been for a number of years now. Some cars connect via cellular signals through telematics services, e.g. OnStar, serve as mobile hotspots for Wi-Fi, and some are even introducing media streaming and other services. Many of these services are separate from functioning vehicle subsystems. Taking into account the cautionary tales from other problems with networked vehicles, such as the hacker that claimed to have gained control of an airplane through its in-flight entertainment system, it is necessary to ensure that this segmentation remains sufficient and secure.

Despite the fact that current day vehicles, though not fully autonomous, are already essentially mobile computer systems, car manufacturers have been unable to adequately address the cybersecurity threats associated with this technology.

On average, there are 70 electronic control units (ECUs) that provide modern cars with advanced functionality, all of which communicate using the Controller Area Network (CAN).[2] CAN originally became the standard protocol in the 1980s. As the automobile industry has changed drastically over the years, however, CAN has not been able to keep up. At the time of its creation, the focus was on low cost and low network latency, with security not being considered.[3] Multiple weaknesses of CAN in the framework of modern vehicles have already been reported by security researchers.

One of the main issues is that external threats may present themselves wirelessly through external networks connected to CAN.[4] This would give hackers access to all of the on-board technology in the car, from safety systems to parking sensors. With such access, a number of different attack scenarios are possible including disabling brakes, turning off headlights, and taking over steering.[5] Risk of automotive attacks also increases with the use of Bluetooth, which connects smartphones and other devices to the vehicles.

In recent years, there have been several secure in-vehicle protocols developed, though each still comes with a certain amount of risk. The ID Anonymization for CAN (IA-CAN) protocol looks to prevent denial of service (DoS) attacks through sender authorization and message filtering, as well as a three-step

[2] Alert (ICS-ALERT-17-209-01). (2017, July 28). Retrieved July 10, 2018, from https://ics-cert.us- cert.gov/alerts/ICS-ALERT-17-209-01

[3] Han, K., Weimerskirch, A., & Shin, K. G. (n.d.). Automotive Cybersecurity for In-Vehicle Communication. Retrieved July 10, 2018, from http://www.iqpc.com/media/1001748/37529.pdf

[4] Kirkland, G. (2018, March 12). The Current State of Connected Cars: Can we be Secure? Retrieved July 10, 2018, from https://www.tripwire.com/state-of-security/featured/state-connected-cars-secure/

[5] Han, Weimerskirch, A., & Shin, K. G. (n.d.). Automotive Cybersecurity for In-Vehicle Communication. Retrieved July 10, 2018, from http://www.iqpc.com/media/1001748/37529.pdf

authentication protocol which allows for secure integration of external devices with the vehicle's electronics.[6]

> "Despite the fact that current day vehicles, though not fully autonomous, are already essentially mobile computer systems, car manufacturers have been unable to adequately address the cybersecurity threats associated with this technology.

The National Highway Traffic Safety Administration (NHTSA) is currently promoting a multi-layered approach to vehicle cybersecurity, focusing on both wireless and wired vehicle entry points that are vulnerable to cyberattacks. NHTSA is also conducting the following research projects dealing with vehicle cybersecurity[7]:

- Anomaly-based intrusion detection systems research: Researching metrics and objective test methods to assess effectiveness of such solutions.
- Cybersecurity of firmware updates: Researching cybersecurity of automotive electronics update mechanisms through physical and over-the-air means
- Cybersecurity considerations for heavy vehicles: Researching similarities and differences between passenger cars and larger vehicles from a cybersecurity considerations standpoint
- Research on reference parser development for V2V communication interfaces: Developing a formally verified and mathematically proven message parser
- In-house cybersecurity research at the Vehicle Research and Test Center (VRTC) in East Liberty, Ohio: Exploring the cybersecurity risks of today's vehicle electronic architectures establishing principles and guidance to improve the cybersecurity posture of passenger vehicles through applied research

With the growing ubiquity of connected vehicles and the rise of autonomous ones on the horizon, there are a host of questions regarding cybersecurity we must address. The next steps towards an autonomous future include the need to take on these issues and work on securing both our vehicles and our personal data.

[6] Han, K., Weimerskirch, A., & Shin, K. G. (n.d.). Automotive Cybersecurity for In-Vehicle Communication. Retrieved July 10, 2018, from http://www.iqpc.com/media/1001748/37529.pdf

[7] Vehicle Cybersecurity. (2018, April 13). Retrieved July 10, 2018, from https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

SECURING THE VEHICLES OF TOMORROW

NHTSA has been developing different approaches to securing the autonomous vehicles by focusing on the vehicle's "entry points". At this moment, NHTSA is only in the theoretical and planning phase, not in the implementation phase. They have developed a "layered approach" to their cybersecurity method with four layers:

1) A risk-based prioritized identification and protection process for safety-critical vehicle control systems
2) Timely detection and rapid response to potential vehicle cybersecurity incidents on America's roads
3) Architecture, methods, and measures that design-in cyber resiliency and facilitate rapid recovery from incidents when they occur
4) Methods for effective intelligence and information sharing across the industry to facilitate quick adoption of industry-wide lesson learned

NHTSA encouraged the formation of Auto-ISAC, an industry environment emphasizing cybersecurity awareness and collaboration across the automotive industry.[8]

The University of Michigan has been researching their own method called the Mcity Threat Identification Model. This model will provide a frame work for considering various factors, like:

1) The motivation and capabilities of the attacker
2) The vulnerability of the vehicle's systems
3) The various ways an attack could be achieved
4) The repercussions of a successful attack, whether in terms of safety, privacy, or financial loss[9]

These key components will help further develop the technology needed to keep the vehicles and the users secure and safe.

The University of Michigan's Mcity Research Center discusses how the threats to the vehicles can come through any of the vehicle's sensors, communication applications, processors, and control systems, as well as inputs from other vehicles, roadways, infrastructure and GPS.[10] To successfully protect the user from those threats, each of those systems will need to have their own specific threat prevention system implemented. Mcity has begun combining efforts with the NHTSA and the European Commission's E-

[8] Yoder, J. (2018, April 13). Vehicle Cybersecurity. Retrieved July 10, 2018, from https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

[9] Weimerskirch, A., & Dominic, D. (2018). Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles. *University of Michigan,*1-10. Retrieved July 10, 2018, from https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf

[10] Ibid.

safety Vehicle Intrusion Protected Applications (EVITA). These three institutions have been expanding their models while working together, so that all these threat models can be designed and implemented swiftly to protect the future of the automotive industry. The University of Michigan goes on to say that "The existing models by the NHTSA and EVITA are good, comprehensive examinations that look at automotive applications and their vulnerabilities but omit considerations about specific sources and actors behind security threats, their motivations, and how they weigh the risks involved in considering an attack".[11]

As technology becomes more advanced and more autonomous, the cybersecurity that is needed to keep it secure becomes more difficult and intricate. When a new component is implemented into the system, all the other systems' security features need to be reevaluated to make sure that the newly implemented system works with its current security. If it does not, then the entire security system needs to be redesigned to make sure that all the systems are continually kept secure from outside intrusions.

> "As technology becomes more advanced and more autonomous, the cybersecurity that is needed to keep it secure becomes more difficult

There's no way to know how many ways there are to hack a system. There are too many hackable components and too many different manufacturers to protect against every possible hack. The industry is also not mature enough to have an industry standard system. Every manufacturer is trying to develop their own system to be the industry leader, which creates both pros and cons from a security perspective.

Having every manufacturer design their own autonomous system means that a given threat will probably only work on the specific system it is penetrating at that moment. For example, if a hacker successfully penetrates the autonomous system in BMW's vehicle, that does not mean that the hack will work on Toyota's vehicles as well. As the autonomous industry grows and becomes more mature, however, a more generic, industry standard system used between all vehicles is likely to arise. The coalescence of various systems into an industry standard will allow for more productive information sharing across the sector and the construction of more robust defenses. At the same time, however, homogeneity of systems could also mean that any successful hacker who manages to penetrate the networks of a single system, could potentially work their way into most, if not all, linked systems.

THE EVOLVING VEHICLE AND ROADWAY LANDSCAPE

While the obsolescence of human-drivers is not yet close, we are on the precipice of an era of widespread adaptation of fully autonomous vehicles. Today, there already exist vehicles on our roads that offer varying degrees of this promised autonomy.

[11] Ibid.

The first such implemented autonomous vehicle that was sold to the general public was Tesla's 2014 Model S. The Model S was equipped with Tesla's "Hardware 1" autopilot system. That first generation of autonomy only included the feature for the vehicle to have some semi-autonomous driving and self-parking. In 2015, Tesla released "Autopilot version 7.0" which included the full autonomy while driving down the highway, but was quickly replaced by version 7.1, to remove some features that would encourage drivers to not pay attention to the road because of said autonomy. Version 7.1 also added the "summon" feature, which would allow the car to self-drive to your location with the press of a button on your key fob.

Vehicles using Tesla's Autopilot system have been involved in numerous incidents, some that were fatal to the user. Tesla has attempted to remedy these imperfections in the system and have installed fail-safes, such as insisting that the driver of the car must touch the steering wheel every couple of minutes to tell the system that they are still present and paying attention to the road while the car is in Autopilot.

Technology like this requires a lot of trial and error, but whether or not it should be released until those errors are sorted out remains a critical question that will remain at the center of our societal dialogue about these emerging technologies.

Designing integrated systems, in part via industrial internet of things (IIoT), involves interoperability which in turn requires both a degree of standardization and that the entire infrastructure is established in a common and interchangeable way. In the Tesla example, this could be one of the biggest hurdles. The infrastructure in the United States is still accepting this new form of transportation and the roadways need development. PricewaterhouseCoopers (PwC) emphasizes that the world has "megatrends" that are affecting the way our infrastructure is going to need to be reshaped.[12]

"Technology like this requires a lot of trial and error, but whether or not it should be released until those errors are sorted out remains a critical question that will remain at the center of our societal dialogue about these emerging technologies.

These megatrends include demographic shifts, economic power shifts, technological breakthroughs, accelerating urbanization, and climate change. These megatrends then combine with industry-changing technological breakthroughs to establish what types of mobility infrastructure will need to be developed. PwC articulates that the five infrastructure changes needed are:

1) Small, low cost cars
2) Powertrain electrification
3) Connectivity demand
4) Functional system convergence
5) New business models

[12] Leveraging Smart Infrastructure in Smart Cities for Urban Mobility. (2017). *PricewaterhouseCooper,*1-13. Retrieved from https://eu-smartcities.eu/sites/default/files/2017-10/Connected_and_Autonomous_Brussels.pdf

These five changes to our infrastructure will allow for a more prosperous growth of the autonomous vehicle industry.

A CSO article written in 2017 by Lohrmann, states that internet of things (IoT) technology is quickly developing and has become a hot topic, but cybersecurity and the known vulnerabilities associated with IOT technologies do not receive the attention that they should. One such example of IoT device hacking is what is known as a Distributed Denial of Service (DDoS) attack, which in certain instances has caused multiple utilities to be shutdown.[13] The Harvard Business Review stated:

> "Simple computer bugs can also cause significant glitches in control systems, leading to major technical problems for cities. Once hackers invade smart city control systems, they can send manipulated date to severs to exploit and crash entire data centers."[14]

As a whole, smart city infrastructure requires a lot more development before it can provide the general public with confidence in its abilities.

Nick Ismail with Information Age states that with the current influx of people moving into urban areas, the adjustment to smart city infrastructure could end up saving five trillion dollars by 2022.[15] He states that the use and development of IoT technology and other smart technologies will be the backing that smart city infrastructure will need to be successful, but that it will only grow if the "players", meaning the companies, politicians, and investors, all collaborate to create one single approach.[16]

Many questions remain surrounding the commercial deployment of autonomous vehicles. Having driverless commercial vehicles and commercial fleets means changes in supply chain, logistics, and freight shipping as well. According to Wortzel, 2003, the USA PATRIOT ACT's definition of critical infrastructure is:

> "…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[17]

One question to address in the future is, as connected infrastructure converges with commercial autonomous vehicles, will these vehicles become critical infrastructure? If so, what happens when autonomous vehicles become critical infrastructure?

---

[13] Lohrmann, D. (2017, July 05). Who cares about smart city security? Retrieved July 12, 2018, from https://www.csoonline.com/article/3205764/internet-of-things/who-cares-about-smart-city-security.html

[14] Thibodeaux, T. (2018, February 06). Smart Cities Are Going to Be a Security Nightmare. Retrieved July 12, 2018, from https://hbr.org/2017/04/smart-cities-are-going-to-be-a-security-nightmare

[15] Ismail, N. (2018, May 15). Smart cities could lead to cost savings of $5 trillion. Retrieved July 12, 2018, from https://www.information-age.com/smart-cities-lead-cost-savings-5-trillion-123469863/

[16] Ibid.

[17] Wortzel, L. (2003) Securing America's Critical Infrastructures: A top Priority for the Department of Homeland Security. *The Heritage Foundation.*

SMART REGULATIONS & INTERNATIONAL REGULATORY HURDLES

In nearly every sector, antiquated and static regulatory frameworks are being challenged by new and emerging technologies, and the automotive industry is no exception. Advancements in autonomous vehicle technology have presented a major challenge when it comes to the U.S. regulatory framework. Technological developments are progressing at a much faster rate than policymakers can keep up with. Current regulations are based, with good reason, on a tradition of motor vehicles that have been manually operated by humans. Yet even the technologies integrated into many vehicles that are on our roads today already assume certain responsibilities in the operation of themselves, stretching the efficacy of existing regulatory mechanisms. The eventual elimination of humans as chief operators all together will only exacerbate this tension. These unresolved issues have left local, state, and federal policymakers struggling to keep pace.

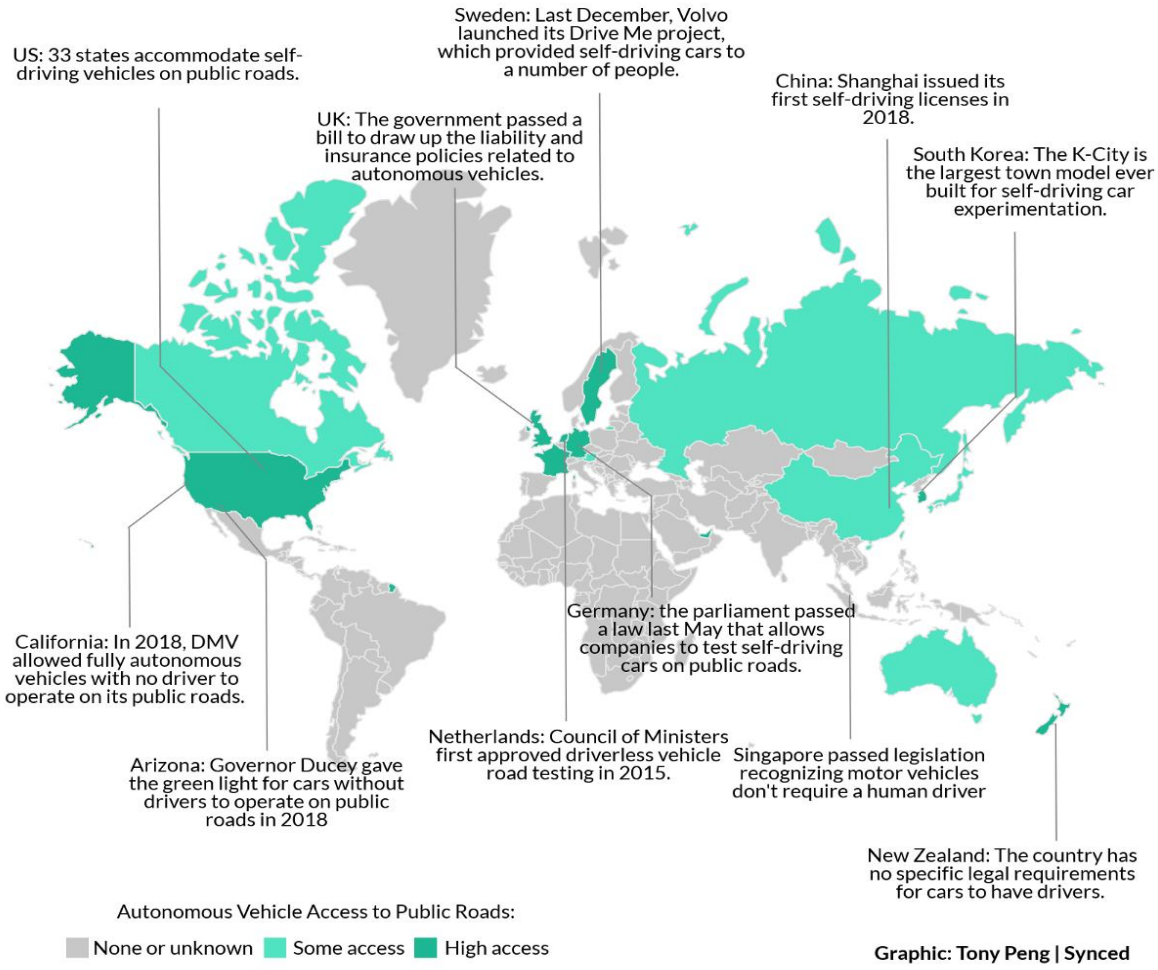

Figure 1: Major regions accommodating deployment and testing of autonomous vehicle technologies on public roads.

Perception plays a major role in the development of any new technology. With innovation comes questions, difficulties, and controversy. It is human nature to be wary of an unfamiliar concept, especially one as revolutionary as autonomous vehicles. Progress is closely tracked and any failures or obstacles that come up tend to be heavily scrutinized in the public eye.[18] Throughout all of this, it is easy to become focused on the pitfalls and forget about the potential long-term benefits that the technology offers. It is important that policymakers do not hastily impose restrictions and regulations that limit innovation. Keeping an open mind and remaining technology-neutral, meaning understanding that the way things have been done traditionally may not be the best solution to current challenges in the field, is crucial.[19]

Cooperation and support at all levels of government is vital to long-term success. While state and local governments are essential when it comes to enforcing traffic and transportation regulations, the federal government is the kingpin.[20] Agencies such as the Department of Transportation and NHTSA are key players in laying down the regulatory framework for the nation as a whole. Altogether, trying to accommodate a multitude of conflicting laws and regulations coming from various states will ultimately undermine innovation. Maintaining a constant dialogue between innovators, industry, and government will pave the way to success and progress in this fast-paced field.

Beyond just the United States, the supply chain is evolving for new technology needs and the development of new systems is a global issue. Human factors, HMI, and human use cases are not only relevant for the US market, they are important considerations for all markets. Today's software-centric systems and data-driven applications, and development and integration of new sensor technologies adhere less and less to political borders. Countries throughout North America, Europe, Asia, and Australia are all looking towards an autonomous future.[21] Although considerable progress has been made, each country faces its share of regulatory hurdles as well, due to their own governmental setups and regulatory traditions.

Competition can be a major driver of innovation; however, it can also be the downfall of individual countries' success. Countries like the UK, South Korea, and Singapore have tended to be more progressive when it comes to autonomous vehicle regulations and investments, while others such as China have been slower to provide support.[22] Varying levels of support and regulation have led to companies being attracted to developing within certain countries. NuTonomy, for example, is a Boston-based self-driving software company that ended up going to Singapore in 2016. They were able to launch a free trial

[18] Greenemeier, L. (2018, March 21). Uber Self-Driving Car Fatality Reveals the Technology's Blind Spots. Retrieved July 13, 13018, from Scientific American website: https://www.scientificamerican.com/article/uber-self-driving-car-fatality-reveals-the-technologys-blind-spots1/

[19] Angerholzer, M., III, Mahaffee, D., Vale, M., Kitfield, J., & Renner, H. (2017, March). The Autonomous Vehicle Revolution (Rep.). Retrieved July 11, 2018, from CSPC website: https://www.thepresidency.org/sites/default/files/pdf/The Autonomous Vehicle Revolution—Fostering Innovation with Smart Regulation.compressed.pdf

[20] Ibid.

[21] Peng, T. (March 15). World map of countries testing autonomous vehicle technologies. Retrieved July 16, 2018, from https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

[22] Peng, T. (2018, March 15). Global Survey of Autonomous Vehicle Regulations (M. Sarazen, Ed.). Retrieved July 11, 2018, from https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

autonomous taxi service and have plans to implement the service fully by the end of 2018.[23] With different countries progressing at different rates, those that do not begin to seriously focus on finding solutions and driving innovation will find themselves falling behind.

Finding the balance between competition and collaboration is a critical aspect in the international framework. If global leaders are not on the same page, it can and will lead to difficulties for everyone given the international level of cooperation that is needed. The supply chain in the new market is a combination of physical and virtual, whereas in the past the supply chain was largely physical and could be easily regulated by political borders. While it is easy for countries to get lost in the nuances of national regulatory challenges, it is important to remember that there is much to be learned and accomplished when the world works together as a whole.

CONVERGENCE: AUTONOMOUS VEHICLES, INFRASTRUCTURE, & FUTURE URBAN PLANNING NEEDS

As theorized, we will reach a day when smart city infrastructure, connected and autonomous vehicles, and ever individual users' mobile and wearable technologies will become seamlessly integrated with one another. Vehicles, people, buildings, even light posts, will symbiotically communicate with one another relaying data in real-time to create efficient and dynamic ecosystems.

The full effects of the arrival of such a digital ecosystem from an urban planning standpoint remains a speculation—it is simply too soon to say whether the effects will be minimal or revolutionary Towards demystifying this question, some firms, consortia, and universities are beginning to explore future urban planning, which is beginning to expand the conversation into research efforts and concept exploration. Companies such as Wi-Fiber, a smart-infrastructure developer, have already implemented their product on the streets of Las Vegas, doing so without substantial interference in the daily life of the Las Vegas Strip. Other urban sectors, such as public transportation, will require more interaction with the local community, but roll-out will have to come in waves. It will be impossible to fully apply every smart technology change in one attempt. As for planning, once the infrastructure is laid out, the new urban lifestyle and planning will adapt to those already implemented changes.

> "Finding the balance between competition and collaboration is a critical aspect in the international framework.

"How Driverless Cars Could Disrupt the Real Estate Industry", an article written by Ely Razin for Forbes, illustrates how technological advancements could alter contemporary notions of urban planning and development. He that public transportation hubs will become real estate hotspots. Prices around these

[23] Ibid.

hubs will increase as more people seek to live there, potentially causing a housing shortage in these areas, as demand will outstrip available supply.

Furthermore, according to statistics presented by Razin, private automobiles spend just 5% of their time actually in use, while these vehicles stayed parked during the remaining time. The need for parking has resulted in around 500 million parking spaces in this country, which is commercial real estate. In an age of ubiquitous autonomous vehicle fleets, in which vehicles could drop off their passengers and then return home or begin operating as ride-sharing services, the need for parking could diminish drastically. Not only could this spell important ramifications for commercial real estate, an abundance of cars able to provide ride-services to wanting individuals could have important implications for public transportation systems as well.[24]

ARE WE READY?

It is the Authors' opinion that a fully- autonomous future is imminent for this country and for the world. But questions remain: are we capable of undergoing the change needed to prepare for the arrival of such a future? We believe the answer is yes, the capability exists. But, much work remains to be done and many steps will be required to be taken before this country will be in a position to best implement autonomous vehicles and smart city infrastructure. Nor will such steps be merely technological in nature. While the underlying technologies must develop to a point where their deployment can be done in a safe manner, and there have indeed been great strides on the technological development and innovation front over the years, a shift in the mindset of both the general public and the government must accompany advancements in technology for adoption and acceptance to occur. There are still many unanswered questions and concerns surrounding autonomous vehicles and it is natural to be fearful of this uncertainty.

To be confident in the implementation, one must be confident in the system. At this moment, today, full confidence in these emerging systems is not present. Autonomous vehicles have a lot of needed development before trust and confidence can be given, and certainly before autonomous vehicles are ready to comingle with human-driven vehicles.

As far as security goes, tying every piece of smart technology together is a revolutionary concept, one that will come with its fair share of challenges. For instance, can it keep us and our information safe? Can I trust my autonomous car not to misjudge a road sign for the underside of a semi-truck? Many such questions must be addressed and answered before we can really gain support for these ideas. Trust in autonomous vehicles remains an important, and unresolved, issue.

[24] Razin, E. (2018, March 12). How Driverless Cars Could Disrupt The Real Estate Industry. Retrieved July 12, 2018, from https://www.forbes.com/sites/elyrazin/2018/03/11/how-driverless-cars-could-disrupt-the-real-estate-industry/#3f2c538113c1

So no, we are not ready yet for a fully-autonomous future, but we are not far off, and we are getting closer every day. The relentless forward march of technology means that soon the capability for autonomy will arrive. We must work to ensure that we are prepared on all other fronts for that day.

RECOMMENDATIONS

Keeping an open mind and thinking in the long-term is just as important as looking at the short-term. For example, safety has been a major concern with the multitude of accidents and failures that have been associated with autonomous vehicle testing and development. All of the concern is understandable, but it is also important that we do not shy away from continuing to make improvements and find solutions to these problems.

Education is a crucial component of any societal movement. Fear of the unknown is another natural reaction that we have as humans. It is important that policymakers and the public are kept up to date with enough transparency to understand what is going on in the industry. Knowledge is power and an educated public and government will be much more understanding and willing to find ways to overcome the multitude of hurdles that accompany the changing landscape.

REFERENCES

Angerholzer, M., III, Mahaffee, D., Vale, M., Kitfield, J., & Renner, H. (2017, March). The Autonomous Vehicle Revolution (Rep.). Retrieved July 11, 2018, from CSPC website: https://www.thepresidency.org/sites/default/files/pdf/The Autonomous Vehicle Revolution—Fostering Innovation with Smart Regulation.compressed.pdf

Alert (ICS-ALERT-17-209-01). (2017, July 28). Retrieved July 10, 2018, from https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-209-01

Arlt, G. (November 22, 2016) Automotive Navigation Systems. Historic Vehicle Association. Retrieved July 14, 2018, from https://www.historicvehicle.org/automotive-navigation-systems/

Han, K., Weimerskirch, A., & Shin, K. G. (n.d.). Automotive Cybersecurity for In-Vehicle Communication. Retrieved July 10, 2018, from http://www.iqpc.com/media/1001748/37529.pdf

Ismail, N. (2018, May 15). Smart cities could lead to cost savings of $5 trillion. Retrieved July 12, 2018, from https://www.information-age.com/smart-cities-lead-cost-savings-5-trillion-123469863/

Kirkland, G. (2018, March 12). The Current State of Connected Cars: Can we be Secure? Retrieved July 10, 2018, from https://www.tripwire.com/state-of-security/featured/state-connected-cars-secure/

Leveraging Smart Infrastructure in Smart Cities for Urban Mobility. (2017). PricewaterhouseCooper,1-13. Retrieved from https://eu-smartcities.eu/sites/default/files/2017-10/Connected_and_Autonomous_Brussels.pdf

Lohrmann, D. (2017, July 05). Who cares about smart city security? Retrieved July 12, 2018, from https://www.csoonline.com/article/3205764/internet-of-things/who-cares-about-smart-city-security.html

Peng, T. (2018, March 15). Global Survey of Autonomous Vehicle Regulations (M. Sarazen, Ed.).Retrieved July 11, 2018, from https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

Peng, T. (March 15). World map of countries testing autonomous vehicle technologies. Retrieved July 16, 2018, from https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

Razin, E. (2018, March 12). How Driverless Cars Could Disrupt The Real Estate Industry. Retrieved July 12, 2018, from https://www.forbes.com/sites/elyrazin/2018/03/11/how-driverless-cars-could-disrupt-the-real-estate-industry/#3f2c538113c1

Thibodeaux, T. (2018, February 06). Smart Cities Are Going to Be a Security Nightmare. Retrieved July 12, 2018, from https://hbr.org/2017/04/smart-cities-are-going-to-be-a-security-nightmare

Vehicle Cybersecurity. (2018, April 13). Retrieved July 10, 2018, from https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

Weimerskirch, A., & Dominic, D. (2018). Assessing Risk: Identifying and Analyzing CybersecurityThreats to Automated Vehicles. University of Michigan,1-10. Retrieved July 10, 2018, from https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf

Wortzel, L. (2003) Securing America's Critical Infrastructures: A top Priority for the Department of Homeland Security. The Heritage Foundation.

Yoder, J. (2018, April 13). Vehicle Cybersecurity. Retrieved July 10, 2018, from https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

The opinions expressed in this article are those solely of the author.

Corresponding Author

JEREMY SPAULDING
jspaulding@autonebula.com

Founder and President, JMS Innovation & Strategy

Senior Vice President, Technology, AutoNebula Group

Spaulding has a master's degree in Industrial & Systems Engineering/Human Factors from Virginia Tech and over 15 years of experience in Human Factors Research, HMI development, usability analysis and user experience development for major corporations in the lighting, automotive, software, and healthcare industries. He is an active Advisory Board Member of the Woodrow Wilson Center's Science and Technology Innovation Center (STIP) in Washington DC.

The Wilson Center
Web: wilsoncenter.org
Facebook: WoodrowWilsonCenter
Twitter: @TheWilsonCenter
Phone: 202.691.4000

The Digital Futures Project
Web: wilsoncenter.org/program/digital-futuresproject
Email: digitalfutures@wilsoncenter.org
Facebook: WilsonCenterDFP
Twitter: @WilsonCenterDFP
Phone: 202.691.4002

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027