
Mina J. Hanna, Synopsys
Shawn C. Kimmel, Booz Allen Hamilton

Current US government policies and activities impacting the development of automated driving systems are surveyed, with special emphasis on privacy, cybersecurity, safety regulation, energy and environment, and ethical issues.

Self-driving or automated driving systems (ADSs), as defined in SAE J3016, raise many economic, social, and security issues that draw federal attention. Given the various roles that the US government can and does play, technology developers might find it difficult or overwhelming to survey and navigate the federal government landscape. Furthermore, this landscape is constantly shifting as agencies adapt policies, regulations, and funding priorities to address emerging technologies. In September 2017 alone, the House of Representatives passed the SELF DRIVE Act (H.R. 3388) and the US Department of Transportation (USDOT) updated its automated driving systems guidance.

Although many developers and technologists might bemoan the complexity, pace, and ineptitude of government, others seek an edge by familiarizing themselves with the challenges and seizing opportunities in the policy arena. In this article, we survey current federal policies and activities impacting technology developers, with special emphasis on privacy, cybersecurity, safety regulation, energy and environment, and ethical issues.
ECONOMIC, SAFETY, AND ENERGY IMPACTS

We begin by summarizing ADSs’ potential economic, safety, and energy impacts, which are the principal drivers of both technology development and federal government action.

The advent of ADSs in US cities and on US highways is stirring the inevitable debate on how to regulate this technology. There is a forthcoming need for an overarching regulatory framework for ADSs that considers their ethical, legal, and safety aspects, as well as their commercial viability and effect on society at large. However, careful deliberation is warranted to balance the reach of such regulations in order not to stifle innovation but rather to incentivize sustained investments in the development, testing, integration, and deployment of ADSs on our roads. The US is poised to benefit immensely from such an opportunity because it creates another avenue to drive economic growth and help the nation maintain its technological leadership in the world. Technological fields such as AI, machine learning, the Internet of Things (IoT), and connected ADSs are expected to continue growing at an exponential rate over the next two decades. A Bank of America Merrill Lynch analysis calculates the total global market for robots and AI to reach $152.7 billion within the next three years, and estimates that adoption of these technologies will improve productivity by 30 percent in certain industries.¹

Automakers are increasingly outfitting their modern motor vehicles with sophisticated connected technologies that gather, process, store, and transmit vast amounts of information for augmenting passenger entertainment, reducing crash-related deaths and injuries, improving vehicle performance, and reducing traffic congestion. By the year 2020, there will be a quarter billion connected vehicles on the road (www.gartner.com/newsroom/id/2970017). That is to say, one in five vehicles on the road worldwide will be connected to the Internet. Thanks to the remarkable feat and fast-paced innovation of vehicle-to-vehicle communication, low-power high-performance computing, deep learning, and the IoT, safer automated driving systems are closer to reality than they have ever been. Still, real challenges to manufacturers, regulators, and technology developers in cybersecurity, data privacy, and building consumer trust in ADSs remain ahead, in addition to challenges to our national infrastructure, from roads to traffic management systems.

The economic opportunity presented by ADSs is unparalleled. The World Economic Forum estimates that ADSs could create $3.1 trillion potential value in societal benefits, save 1.2 million lives from fatal road accidents, and reduce 540 million metric tons in potential emissions over the next 10 years.² These societal benefits include $381 billion savings by consumers from reduced driver insurance premiums and reduced crashes by 2025, in addition to reduced vehicle ownership costs, reduced maintenance, reduced congestion, fuel savings, and lower carbon emissions.³

ADS technology fundamentally reinvents the commute-to-work and road-travel experience, creating a space for accelerated innovation; countless opportunities for revolutionary technology commercialization; disruptive business models; and next-generation human-centric, data-driven services focused on enhancing the passengers’ onboard experience. McKinsey and Company estimates that ADSs could free as much as 50 minutes per day for drivers to spend working, relaxing, or accessing entertainment.⁴ Onboard entertainment alone could contribute up to $65 billion to the industry value chain. This would generate $5 billion per year in global digital media revenue for every minute drivers spend online while in a car. Furthermore, McKinsey estimates that adoption of this service in key markets will grow to 30 percent in 2025 (from 4 percent in 2016).

Availability of these services will create more demand for increasingly sophisticated infotainment and digital-content creation, spawn new business models, create complete ecosystems of novel applications and, in the process, create hundreds
SELF-DRIVING CARS

of thousands of sustainable jobs. Even in retail, driverless trucks might be able to better coordinate their shipping routes based on real-time traffic data, reduce logistical and supply costs, increase sales, and improve profitability for retail businesses—all of which will favorably impact product pricing, thereby driving larger market demand and growing consumer surplus.

Safety is one of the most important public benefits of vehicle automation. USDOT cites that automation technology can save lives by addressing up to 94 percent of serious crashes that are due to human error. The health and economic impact of these accidents is staggering. In 2013 alone, on-the-job motor vehicle crashes cost US employers $25 billion.5

The environmental and mobility impacts of vehicle automation are highly uncertain, and are of great concern to the public sector. Initial estimates range from almost doubling to halving energy consumption due to ADSs.6 Vehicle automation has the potential to greatly improve accessibility for older adults and people with disabilities.7 There is a potential for reduced congestion through improved carpooling and parking traffic; however, that could also increase congestion with more vehicle miles traveled.8 Whether automation improves or worsens traffic flow will depend on the connectivity and interaction between ADSs’ algorithms and human drivers.9

CHALLENGES TO DEVELOPMENT AND DEPLOYMENT

Our discussion continues with a description of current policy and trends in five major issue areas: privacy, cybersecurity, safety regulation, energy and the environment, and ethical issues.

User data privacy

Vehicle automation increasingly relies on data to function, and the federal government is taking notice and grappling with defining its role in the area of privacy. Last year was an active one, with provisions in the SELF DRIVE Act requiring manufacturers to have a privacy plan, a joint National Highway Traffic Safety Administration (NHTSA)/Federal Trade Commission (FTC) vehicle-data privacy and security Request For Information and workshop, revisions to NHTSA’s automated driving systems policy eliminating privacy from the safety assessment letter, and a Government Accountability Office (GAO) report on current vehicle data privacy. The automotive industry released the Consumer Protection Privacy Principles in 2014 that outline best practices for the collection, use, and sharing of information from vehicle technologies and services. These principles are applicable to ADSs as well as conventional vehicles and are enforceable by the FTC. The FTC assesses that failure to implement reasonable security measures to protect consumers’ data might be in violation of the FTC’s Prohibition against Unfair, Deceptive or Abusive Acts or Practices Act, which protects consumers against reasonably foreseeable and avoidable substantial injury or breach of privacy. An additional GAO report on ADSs is due in late 2017, and the Senate is working on its own self-driving vehicles bill (AV START Act, S.1885; www.congress.gov/bill/115th-congress/senate-bill/1885), which on October 4th, passed the Commerce, Science and Transportation Committee.

Amid the shifting sands of federal policy, industry and certain government agencies are already collecting, using, and sharing data to provide services and conduct research and development. The USDOT Connected Vehicle pilot program is finding data privacy to be a major hurdle as cities, vendors, and researchers negotiate data-collection schemes that consider the concerns of many stakeholders.10 To help industry and state and local agencies with these challenges, the USDOT is developing data-sharing platforms (for example, the Research Data Exchange, www.its-rde.net; and the Operational Data Environment, www.itsforge.net/index.php/p-ode -announced), privacy tools for basic safety messages, and an Intelligent Transportation Systems (ITS) secure data common through the ITS Data Program, which serves as a “foundation for agile data sharing and privacy protection in the future transportation system.” These demonstrations,
tools, and platforms can be useful to technology developers and data owners as they seek to collect, use, and share sensitive data.

Over the long run, however, we believe that to increase consumer confidence, manufacturers will have to implement measures to ensure data privacy compliance, and follow best practices in implementing processes to continually monitor, discover, and resolve security vulnerabilities in their systems. Furthermore, they should implement a strategy to ensure that downstream data privacy and security are implemented by hardware and software acquired from third-party vendors, and contractors during the procurement process. Manufacturers would need to disclose the type of information self-driving cars are collecting about users and in what manner this data is being used as well as provide consumers with the choice to opt out of data collection.

Cybersecurity

The National Telecommunications and Information Administration (NTIA) recently issued a Request For Comment (www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats), pursuant to the President’s Executive Order 13800, 82 FR 22391 (11 May 2017), “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” (www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-13800). The NTIA was commissioned by the Executive Order to suggest risk-management measures and mitigation strategies to guard the nation’s critical IT infrastructure and secure national data from unauthorized and malicious access attempts and form modification and/or perturbation of related services intended to threaten the state of public safety, public health, economic security, and national interest.

Additionally, NIST released the NIST Cybersecurity Framework11 that postulates for federal agencies the key cybersecurity risk-management standards and guidelines to implement and continuously improve their cybersecurity threat-prediction and mitigation processes. IoT devices, insecure mobile devices, and possibly self-driving vehicles are the most at risk of being compromised by botnets and distributed denial-of-service attacks, which could have negative repercussions for American public safety. Moreover, any one vehicle could be used as a node from which malicious hackers could launch attacks on other vehicles sharing the network, effectively building a remotely controlled automotive botnet.

Connected ADSs that access, process, store, and transmit a wealth of passenger information offer to be a prized asset for mischievous black hats. In this sense, to minimize the risk of exploitations of software vulnerabilities, ADS development should align with the NIST Cybersecurity Framework and NTIA’s risk-management and cyberthreat-mitigation strategies. Vehicles manufacturers and developers working on the next generation of Telematics systems (GM OnStar, Lexus Enform, Toyota Safety Connect, Hyundai Blue Link, and Infiniti Connection) should develop internal monitoring systems for hacking activities and Internet-enabled security software updates and patches. Recently, security researchers Charlie Miller and Chris Valasek were able to uncover a Uconnect flaw that affected 471,000 vulnerable vehicles on the road, and they managed to manipulate a Jeep’s steering wheel and gearbox and disable its brakes while it was driving on the highway.

Sen. Mark Warner (D-VA), Sen. Cory Gardner (R-CO), Sen. Ron Wyden (D-WA), and Sen. Steve Daines (R-MT) have introduced in the Senate the IoT Cybersecurity Improvement Act of 2017 (S.1691; www.congress.gov/bill/115th-congress/senate-bill/1691). The bill requires vendors of Internet-connected devices purchased by the federal government to ensure that their devices are patchable, rely on industry standard protocols, do not use hard-coded passwords, and do not contain any known security vulnerabilities. Furthermore, it exempts cybersecurity researchers from liability or prosecution under the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act (DMCA) when legally and safely engaging in good-faith research pursuant to adopted coordinated vulnerability disclosure guidelines. Today, some interpretations of the CFAA and the anticircumvention provisions of the DMCA are ambiguous regarding whether and how proprietary AI systems (including ADSs) might be reverse engineered and evaluated by academics and researchers probing them to uncover their critical security vulnerabilities.12 Designers and manufacturers should work openly and build trust with researchers and the white hat community to...
advances the securing of Internet-connected devices and ADSs.

Sen. Ed Markey (D-MA) and Sen. Richard Blumenthal (D-CT) introduced the SPY Car Act of 2015 in the 114th Congress (S.1806; www.congress.gov/bill/114th-congress/senate-bill/1806); however, it did not go to the floor for a vote. The bill proposed to commission the USDOT, NHTSA, and FTC to set new digital security standards for cars, including isolating critical software systems from the rest of a vehicle’s internal network, and the addition of onboard diagnostic systems to detect and counter malicious attacks on the car’s network. The bill also proposed to create a data privacy regulation, requiring carmakers to inform consumers how their data is collected and stored, and letting drivers choose not to allow the collection of their data, restricting any collection for marketing purposes only.

Safety: regulation and research

Although safety is a major incentive for quickly deploying ADSs, little data exist to prove safety benefits, and appropriate methods to verify, validate, and accredit safety are not yet mature. As discussed in the IEEE-USA Artificial Intelligence ad hoc Policy Committee’s Position Statement, an effective public policy on self-driving vehicles safety will have to assure public well-being while fostering a robust industry. Benefits estimation and safety regulation are two important governmental issues for technology developers to understand.

Safety regulation. As with many new technologies, existing regulations can pose challenges. USDOT has reviewed the Federal Motor Vehicle Safety Standards (FMVSS) and identified several challenges for ADSs complying with these regulations, such as not having pedals and steering wheels to conduct tests, and new occupant designs that change seating position and orientation. Interpretation and exemptions are two tools that give USDOT flexibility when dealing with new technologies and existing regulations. Google submitted a request to USDOT in which USDOT could interpret certain concepts favorably to the deployment of automation (for instance, equivalence of automated driving system and driver), but there were limitations to USDOT’s interpretation ability, in which case, exemptions or FMVSS updates would be necessary. The process for exempting vehicles from FMVSS requires that manufacturers demonstrate equivalent safety for these exemptions. Equivalent safety will be a challenge to demonstrate given the general lack of quantitative tools for addressing the safety of automated driving systems.

Beyond challenges with existing regulations, there may be a need to develop new safety regulations for an automated driving system that controls a vehicle in safety-critical situations. Developing new safety regulations for ADSs poses a major public-sector challenge and is being addressed at the federal, state, and international levels.

Internationally, governments and treaty organizations are seeking to update legal frameworks to accommodate vehicle automation. United Nations Economic Commission for Europe’s (UNECE) WP.1 and WP.29 are addressing issues with the Vienna and Geneva Conventions, especially with interpreting the term “driver” and permissible tasks for drivers at higher levels of automation. The UK has developed a code of practice to guide testing of systems. The US is part of the Geneva Convention and must be compliant with regulations and interpretations, and is in international agreements with other countries to leverage ongoing research and development for example, the US-EU-Japan trilateral agreement on Intelligent Transportation Systems; www.its.dot.gov/presentations/pdf/ITS_International ActivityOverview.pdf).

There has been activity at the state level, especially around registration, testing, and certification. California is working on a draft regulation that would address issues related to event data recording in case of incidents and would define operational design domains (www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/auto).

USDOT NHTSA recently released their new Automated Driving System 2.0 policy, which describes elements of a voluntary safety assessment letter to be submitted for testing and deployment of automated driving systems. It is important for technology developers to consider whether this voluntary safety assessment letter pertains to them, and to understand its elements.

Congress has also been active regarding the safety of automated driving systems. The proposed House SELF DRIVE Act and the related Senate AV START bill under revision seek to address the safety of ADSs in the US. The House legislation would
performance of automated driving systems to prevent a patchwork of state regulation,

› require manufacturers to file safety assessment letters to help assess safety, and

› issue regulations for future automation features.

The next year will be a very interesting time for policy as Congress seeks to pass a bill, USDOT evolves FMVSS and accepts safety assessment letters, and states look at their role in testing and certification.

Safety research and development. Government programs are seeking to address some of these important questions through research and development to bolster US leadership in automotive innovation. Research efforts and industry engagements are underway to better understand and characterize safety benefits and performance. To gather data on vehicle safety and work with industry, USDOT designated 10 ADS proving grounds in 2017. USDOT has developed a high-level benefits framework for discussing and estimating benefits. Still, more detailed benefits models and performance information are needed to assess safety benefits. These research activities and information-sharing activities provide an opportunity for technology developers to support data-driven decision making through research grants and data sharing with policy makers. Some of the biggest safety-related research challenges are

› validation, verification, and accreditation (VV&A)—existing frameworks, such as automotive functional safety standard ISO 26262, face challenges when applied to automation, such as demanding exorbitant test requirements due to Automotive Safety Integrity Levels (ASIL) triggered by the high level of vehicle control. New frameworks, such as model-based systems engineering and combined simulation, track testing, and on-road testing must be examined.

› fault tolerance—with so many lines of code and interrelated systems, the ability to identify and mitigate faults will depend on implementing new techniques such as redundancy (for example, two-out-of-three parallel-system output selection). New techniques for system testing, such as stress testing, offer potential for improving confidence.

› machine learning (ML)—ML algorithms are particularly challenging due to their non-deterministic and nonintuitive nature. Research efforts underway to address this challenge include USDOT work to identify test cases and technical standards’ needs, the DARPA Assured Autonomy Program, the NSF Cyber-Physical Systems Program, and the NASA Assured Autonomy for Aviation Systems. These funding programs present opportunities for technology developers to advance VV&A methods and inform public policy.

Ethical concerns

Ethical considerations regarding self-driving cars have captured the public’s imagination. For example, public debates often touch on the “trolley problem” (if a car is about to hit a group of people, but could swerve and hit fewer people, whom should it hit?), and on how a self-driving car should prioritize the driver over vulnerable road users. The public-policy issues reflect AI ethics more broadly and include challenging issues such as responsibility, transparency, explainability, and impact on employment.

Statistical ML algorithms can only draw meaningful conclusions from the raw data they are provided. Choice of data population is one way in which selection bias can inadvertently arise as a result of an unwarranted assumption, which can promulgate to the AI/ML module, thus leading to conclusions that are deceptively narrow but which appear statistically significant for the given data set.

Assuming generalizability, agency, or causality in regression and predictive models without sufficient evidence could result in faulty and harmful decision making. Selection bias takes many forms, such as sampling bias, self-selection bias, exclusion, overmatching, Berkson’s fallacy, Simpson’s Paradox, and many more, none of which are necessarily or purposefully discriminatory. The same could be said of observer bias arising from unconscious cognitive biases of the human administrator, who admittedly can project human’s core values as well as preconceived notions and judgments onto AI.

That is to say nothing of maleficent and deliberate manipulation of intelligent systems, intended to harm the most vulnerable in our society. Moreover, an impartial decision deemed beneficial for most of the population is not necessarily good in the case of every individual.
Hence, responsibility, transparency, and explainability of AI systems are tantamount, where the logic behind the decisions that the AI takes can be clearly explicated, showing how the decision has impartially considered all available and reliable data. The AI system has to be designed to be human centric.

A governance platform for ethical evaluation standards, enforcing accountability, ensuring data and decision decentralization and democratization of AI learning, is needed to avoid subjecting any group of people to harm, discrimination, misrepresentation of their interests and values in society, or deprivation of equal opportunities. This platform should be based on an auditing framework for checking how AI systems are meeting a defined set of decision fairness and ethicality metrics. This understanding is crucial to increase public confidence and trust in AI in general and is no less critical in the case of self-driving vehicles.

In Germany, a government-appointed committee comprising experts in ethics, law, and technology drew up an ethical guideline for driverless cars that directs that the programming of the underlying software should aim to avoid injury or death of people at all cost, meaning that it should decide on actions that will harm people the least, even at the cost of destroying property or hitting animals on the road. Furthermore, the software cannot, under any circumstance, base its decisions on the age, sex, or physical condition of the people involved.

The IEEE Standards Association has a number of standards working groups attempting to formulate industry best practices and codify ethical design principles to help advance the progress of self-driving cars and the ecosystem of AI systems in general. The IEEE Global Initiative for Ethical Autonomous Trucks, the freight industry could save $168 billion annually, of which $70 billion would arise from cutting labor.20 The US freight industry employs 3.5 million professional truck drivers to haul 10 billion tons of goods each year. Truck driving is the most common job in 29 states, therefore the adoption of ADSs will likely have a nontrivial impact on hundreds of thousands of families. The federal government must create vocational retraining and counseling programs that will help workers adapt, effectively compete, and take advantage of new employment opportunities in a rapidly evolving marketplace shaped by AI and ADS economics.

Energy and environment
The energy and environmental impacts and associated regulation of automated driving systems presents great opportunities and challenges for technology developers. Government regulations like Corporate Average Fuel Economy (CAFE) and National Ambient Air Quality Standards (NAAQS) impact new vehicle technologies. Where opportunities exist to make new vehicle technologies more efficient and less polluting, opportunities exist for federal research funding.

Insofar as automated driving systems impact fuel economy and air quality, they can be influenced by CAFE or NAAQS. CAFE drive cycles do not currently accommodate performance differences that might arise from automation, such as eco-approach, eco-departure, eco-routing, and platooning, but these might be the subjects of future CAFE credits if sufficient industry and federal support is gathered. Similarly, automated driving systems might impact NAAQS, especially in areas of nonattainment, where they...
could either help alleviate or contribute to criteria pollutant emissions and formation. The impacts of automation on fuel economy and emissions are not yet understood well enough to support policy changes in these areas, and further research is required.

Government research and development are important to informing policy and developing technologies that can improve energy independence and reduce negative environmental impacts. The US Department of Energy (DOE) is pursuing research to understand system level impacts (for example, the SMART ([Systems and Modeling for Accelerated Research in Transportation] Mobility Consortium) and develop energy efficient vehicle automation technologies (for example, the Advanced Research Projects Agency-Energy’s Next-Generation Energy Technologies for Connected and Autonomous On-Road Vehicles [NEXTCAR]), and USDOT is pursuing the Smart Cities Challenge and University Transportation Center programs to advance understanding of impacts. These programs have, and future programs will continue to provide, technology development and deployment opportunities for technology developers, ranging from universities to start-ups to large established businesses.

The introduction of such a disruptive technology as self-driving vehicles will change the federal legislative, regulatory, and research and development landscape. As the public discourse evolves on potentially divisive issues like safety and privacy, industry and practitioners will play an important role in educating the public and contributing to well-informed, data-driven policy. It is incumbent on experts to promote an educated public that understands the rewards and risks of self-driving cars, per a major recommendation of the IEEE-USA Artificial Intelligence Policy Committee’s Position Statement. Building trust and sharing information between industry and government agencies will be critical, especially with new entrants like Tesla and Waymo wading into a very traditional and risk-averse automotive regulatory environment. Although vehicles might one day update software as often as phones do, there are still many, many bricks to lay in the path towards a flexible regulatory regime that addresses safety concerns.

Federal funding of research and development is critical to international competitiveness, as discussed in the IEEE-USA Artificial Intelligence Policy Committee’s Position Statement. Technology developers and practitioners can benefit from research funding, data-sharing platforms, and tools that the government provides. Funding opportunities exist for start-ups, academics, and large companies alike, and can be a key enabler for commercialization and for incentivizing development of socially beneficial technologies. Agencies like NSF, DOE, USDOT, and NASA are funding research that create economic opportunities by enabling safety assurance, energy efficiency, security, and data sharing. Federal resources can help increase safety and energy benefits, accelerate innovation, and address privacy and security challenges.

It is imperative for the US to harness the great benefits of AI to transform our economy and create sustainable American jobs. Otherwise, it will face a competitive disadvantage that will strongly and negatively impact our economy. The US might lose its leadership position in the development of the technology of tomorrow. Hence, policymakers need to expeditiously devise careful, informed, and forward-looking policies to promote a safe space for technological innovation to thrive in this field while ensuring a prosperous future for all sectors of our society.

REFERENCES
SELF-DRIVING CARS

ABOUT THE AUTHORS

MINA J. HANNA is a senior software consultant at Synopsys, Inc., the current chair of the IEEE-USA Artificial Intelligence ad hoc Committee, and a member of the IEEE-USA Research and Development Policy Committee. He is also a member of the IEEE Computational Intelligence Society, IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems, and IEEE TechEthics. Hanna received an MS in electrical engineering from Stanford University. Contact him at mhanna@synopsys.com.

SHAWN KIMMEL is a senior lead engineer at Booz Allen Hamilton. He is a member of the IEEE-USA Artificial Intelligence ad hoc Committee and the Committee on Transportation and Aviation Policy. As a 2014–2015 IEEE Science and Engineering Congressional Fellow with Rep. Lipinski, he drafted automated vehicle legislation that was passed as part of the 2015 FAST Act. Kimmel received a PhD in mechanical engineering from the Colorado School of Mines. Contact him at Kimmel_Shawn@bah.com.

www.cdcfoundation.org/businesspulse/vehicle-safety.