Why Questions about Automated Vehicles Must be Addressed Now

Rosalee A. Clawson, Purdue University-Main Campus
Dustin Joshua Souders, Clemson University

Automated cars and trucks use sensors, radar, cameras, and global positioning service (GPS) navigation, to assist with driving. Much the way smartphones have fundamentally changed what a phone is and does, connected and automated cars and trucks are changing how the average person interacts with vehicles. These vehicles have the potential to limit human error in driving and therefore reduce fatalities. At the same time, public concern about the safety of automated vehicles can put the brakes on innovation, especially when the media highlight crashes and deaths caused by so-called self-driving cars. Safety is the ethical issue that has captured the attention of most observers thus far. Yet as vehicles become increasingly autonomous, there are additional ethical, legal, and social issues that also deserve careful consideration.

Privacy

Connected and automated vehicles produce huge amounts of data – on trip details, travel routes, and passengers. Manufacturers can use such data to track and improve vehicle performance. State departments of transportation can use this information to gain insight into infrastructure needs; and insurance companies want the data to assess liability in the case of accidents. Yet questions abound concerning the collection, storage, and management of data from automated vehicles. Who should own these data? Whose responsibility is it to ensure these data are protected, and who should have access? Who should be able to make money from these data; and under what conditions should information generated by automated vehicles be shared with law enforcement or other government agencies?

These questions need to be publicly debated and discussed now. Decisions about core issues should involve many stakeholders, including industry, interest groups, elected officials, government agencies, academia, and the public. As widespread adoption of connected and automated vehicles proceeds, the public must know what kinds of personal data are being collected, and people must gain trust that private information will be protected and shared only in ways that they approve or that conform to criminal law.

Cybersecurity

Connected and automated vehicles are, in essence, highly complex computers that just happen to travel on roads. As such, these vehicles are open to the same security attacks as other computers. Fully connected and automated vehicles will be able to communicate with one another, with roads and travel infrastructure, with manufacturers, and with many other entities yet to be imagined. All these kinds of communications will be potential targets for hackers.

Even at current levels of connectivity and automation, advanced vehicles and infrastructure constitute cybersecurity risks. Criminals can potentially hack vehicle systems and software to gain access to their data. Malicious actors might try to control vehicle systems or eventually even entire fleets of automated trucks, for example, to cause harm to passengers or bystanders. Connected infrastructure, particularly traffic control mechanisms, might be hacked to cause chaos. Most of these hacks required advanced computer skills and specialized knowledge. Others require only the use of default passwords that have never been changed.

Technological advances are urgently required to ensure the security of connected and automated vehicles. Policy steps are also critical – including regulations to ensure an appropriate level of security for self-driving cars. New policies require debate over key issues: What is the appropriate level of security to further public trust in automated vehicles? Who is responsible when an automated vehicle is hacked? These questions are just the tip of the iceberg. As vehicles and infrastructure become increasingly connected and automated, cybersecurity issues will become more and more important.

Workforce Impacts

Connected and automated vehicles will create many new job opportunities. Already there is high demand for highly skilled engineers, data scientists, and computer scientists who work on automated vehicles. Workers with technical backgrounds who also understand the ethical, legal, and social implications of automation will be especially valuable as the transportation industry moves to develop and deploy self-driving cars. In addition, many new opportunities will open for skilled workers who can maintain and repair these types of vehicles, as well as for workers with the expertise needed to retrofit existing roads with technologies able to communicate with automated vehicles. Academia, industry, and government can collaborate to train skilled people for the many jobs created by connected and automated vehicles.

Nevertheless, job disruptions are also bound to occur – especially in states like Indiana, Mississippi, and Wyoming with many people employed in driving occupations. Truck *drivers* are likely to become truck *operators,* who will need new sets of skills to maintain their jobs. In passenger transportation, limousine drivers, who offer a higher level of service, may be less affected than cab drivers, but both occupations are vulnerable to vehicle automation. People of color disproportionately work in driving occupations, and will be negatively impacted when those relatively well-paid jobs are no longer necessary.

The Way Forward

Industry, unions, government, and academia need to plan now for future job opportunities and challenges. They should anticipate needs for higher education and retraining programs, as well as for unemployment insurance and income supports needed to ensure that automation does not hurt the most vulnerable workers. Technological change is moving very quickly, outpacing policy and regulatory responses. Automated vehicles, including self-driving cars and trucks, will fundamentally transform social and economic life. Now is the time to tackle the ethical, security, and workforce issues that must be resolved to prepare everyone for the big changes to come.

Read more in Dustin Souders and Neil Charness "Challenges of Older Drivers’ Adoption of Advanced Driver Assistance Systems and Autonomous Vehicles," International Conference on Human Aspects of IT for the Aged Population, July 2016: 428-440.