Legal Considerations for Ridesharing Companies in the Autonomous Vehicle Industry

February 8, 2018

While autonomous vehicles are still in the testing phase, more than 260 companies vie for Venture Capital funding as they drive the industry toward commercialization.¹ Car manufacturers, technology companies, and ridesharing companies are racing to develop safe autonomous vehicles and supporting infrastructure. During this competition, five major categories of legal considerations will steer the course of development and commercialization: privacy, liability, cybersecurity, copyright and patents, and regulations.

1. Privacy Considerations

Developers of autonomous vehicles—also called self-driving, driverless, or robotic vehicles—will be motivated to collect data beyond users’ driving habits and trip itineraries, such as credit card usage, medical records, or preferences for store visits.² The data will not solely be for the purpose of operating the car, but for providing information to companies for purposes such as targeted advertising, insurance underwriting, and law enforcement.³ Consumers and companies hotly debate data privacy when it comes to the control of this information, the protection of passengers’ anonymity, and the securitization of data transfer and storage.⁴ Yet there are limited state and federal regulations to guide the debate. States have yet to pass

Authors/Presenters

Shalem A. Massey
Co-Author
Partner
Irvine, California
shalem.massey@bclplaw.com

Jennifer R. Steeve
Co-Author
Associate
Irvine, California
jennifer.steeve@bclplaw.com
legislation specifically addressing data privacy for autonomous vehicles. California has only proposed such legislation: the Consumer Vehicle Information Choice and Control Act, which requires car manufacturers to disclose what information is being collected by owners’ cars. And while there are existing federal laws protecting data collection pertaining to children, credit reporting, and health, they fall short of mitigating the new risks posed by autonomous car data collection. Even when privacy protections are “the clearest and strongest,” such as those to keep the federal government from gaining access to GPS data or other car-tracking technology, the law is still unclear.

The autonomous vehicle industry should anticipate legislation that will address privacy issues more adequately, as Congress has already met on the topic. In the meantime, companies should look to past developments surrounding event-data recorders (EDRs) for help in predicting the impending legislative road. Since 1998, EDRs have been installed in cars to capture information about a vehicle in the final moments before a crash, much like digital flight data recorders for aircraft. Over ninety percent of new cars sold today in the United States come equipped with EDRs. Like autonomous vehicles, EDRs can collect more than crash-related data—i.e. from a driver’s speeding tendency to preference on seat position.

Before 2015, no federal standard governed the access and ownership of EDR data beyond what was required reporting by National Highway Traffic Safety Administration (“NHTSA”) regulations. In the absence of a federal roadblock and without the automotive industry’s help, states adopted varying standards on EDR data privacy. In 2015, Congress passed the Driver Privacy Act to set public and private limitations on data retrieval from EDRs. The Act declared car owners and policyholders as the owners of EDR data, and prohibited third-party access without owners’ consent. However, even with the Act’s passage, seventeen states have enacted statutes allowing for varying exceptions to the rule.

If the development of the laws and regulations surrounding EDR data privacy is any indication, resolving data privacy concerns for autonomous vehicles will be a messy endeavor. For now, companies are encouraged to seek counsel and establish robust privacy policies; provide notice and obtain affected individuals’ consent regarding such policies; limit the collection, retention, and use of personal information; limit disclosure to third parties only to the purposes specified in the notice; protect against unauthorized access; and, lastly, monitor company and individual compliance.
2. Liability Considerations

In 2015, NHTSA estimated that car crashes accounted for over 35,000 fatalities and 2.4 million injuries.\(^\text{19}\) Of these car crashes, NHTSA estimated that ninety-four percent were caused by human error.\(^\text{20}\) By inference, as more autonomous vehicles replace human drivers, the number of crashes should decrease dramatically. In other words, by removing the human driver and potential for human error, autonomous vehicles will save lives. However, with no driver at the wheel, the question remains—who will be held liable when accidents inevitably occur?

To begin answering, the industry will have to change how it thinks about liability. Some insurance companies, chiming in with legal scholars, have stated that existing product liability laws are a good fit for determining liability in autonomous vehicle crashes.\(^\text{21}\) Generally under such laws, a driver who gets into an accident allegedly due to a manufacturing defect can hold the car manufacturer liable for damages.\(^\text{22}\) The frequency of holding manufacturers liable for crashes could increase under this framework. Consider that autonomous vehicles have 100 million lines of computer code—more than fourteen times the lines of code for a Boeing 787.\(^\text{23}\) On average, for every 4,000 lines of code, there is one defect.\(^\text{24}\) This means that each autonomous vehicle launches with an average of 25,000 possible defects that could serve as a reason to hold a car manufacturer liable.\(^\text{25}\) Defending against such liability suits will increase costs for manufacturers. As a result, manufacturers may demand greater access to autonomous vehicle data to track crashes, compromising passengers’ or owners’ privacy, or may price their technology at higher rates to make up for the difference.\(^\text{26}\)

Others advocate for another legal framework to determine liability in autonomous vehicle suits. They propose the expansion of the “no-fault” automobile insurance system—where insurance companies compensate victims in all crashes that cause injuries under a certain degree of severity.\(^\text{27}\) Proponents of this system argue that it would eliminate the difficult determination of who is at fault for a crash.

Alternatively, Congress could narrowly tailor liability for the autonomous vehicle industry as it has for industries involving vaccines, nuclear energy, aviation, and oil spills, respectively.\(^\text{28}\)

3. Cybersecurity Considerations

Over 27 million vehicles worldwide are already connected to wireless internet and are thus
susceptible to hackers.\textsuperscript{29} To date, NHTSA has recalled nearly 1.5 million vehicles due to cybersecurity vulnerabilities.\textsuperscript{30} As autonomous vehicles become more prevalent on the road, they join a more connected system where vehicles not only communicate with each other, but are also fed information from roadside infrastructure—such as traffic signals and road conditions—to help avoid accidents and maximize traffic flow.\textsuperscript{31} Amid vehicles’ wireless exchange of data, hackers can find even more opportunities to compromise the system.

As manufacturers collect more data beyond crash-related information, hackers are presented with stronger incentives to access such commercially valuable data. The question of who is liable for such a hack centers on data ownership.\textsuperscript{32} Companies that own autonomous vehicle data need to be careful with where and how they store and transmit their data. One suggestion is to anonymize the data.\textsuperscript{33} But “[e]ven if this data is scrubbed of unique individual identifying markers, for instance VIN-numbers, or IP- or MAC- addresses, data-mining techniques will almost certainly be able to reconstruct personal identifying information about particular vehicles, and by extension, their regular occupants.”\textsuperscript{34}

Guarding autonomous vehicle data, especially personally identifying data, against hacks and viruses will be a full-time job for companies in the industry. Of course, \textit{total} cyber security is nearly impossible to achieve as hackers will find new ways to infiltrate systems.\textsuperscript{35} Yet all companies in the autonomous car industry are advised to establish and maintain data retention and deletion protocols, work on seamless delivery of software updates, engineer systems for privacy and security, and continuously monitor their systems for threats.\textsuperscript{36}

\textbf{4. Copyright and Patent Considerations}

Autonomous vehicle software can be protected against unauthorized use by both patent and copyright laws.\textsuperscript{37} While there has been a trend among some companies to publicly share patents, other companies are investing heavily in procuring as many patents as possible for their autonomous vehicle technology.\textsuperscript{38} Over 5,800 worldwide patents related to autonomous driving were filed as of July 2017.\textsuperscript{39} With the significant number of patents in the market, companies in the industry need to prepare for a high risk of patent infringement litigation.\textsuperscript{40}

The same goes for copyright suits. However, companies are unable to use copyright law to protect the data generated by autonomous vehicles in the same way they protect their software code.\textsuperscript{41} The Copyright Office will not copyright “works produced [solely] by a
machine or mere mechanical process,” meaning data produced by autonomous vehicles do not fall under copyright protection. Additionally, companies should be wary of copyright laws that do not prevent car owners themselves from diagnosing, repairing, or modifying the software code of their own autonomous vehicles. This is because copying a vehicle’s code for a limited purpose or modifying it constitutes “fair use,” a protected activity under the Copyright Act.

Thus, the industry should expect narrow copyright protections for autonomous vehicle code. Already, there are a multitude of “self-help” videos online explaining how an owner might bypass certain horsepower and speed limitation software. Companies would be well served to incorporate software which detects and then transmits any modification made by an unauthorized entity.

5. Regulatory Considerations

In May 2013, NHTSA released its “Preliminary Statement of Policy Concerning Automated Vehicles.” In it, the agency implied it was not ready to issue its own regulations on autonomous vehicle testing, instead deferring to the states and suggesting model state regulations. Nonetheless, the agency has stated it prefers that states not permit the operation of autonomous vehicles beyond the purpose of area-controlled testing. In fact, in its 2013 Preliminary Statement, NHTSA presumed that operating autonomous vehicles on public roads without an available driver was illegal in the absence of authorizing state and federal law.

Thus far, twenty-one states have enacted legislation governing testing, of which some pieces of legislation are at odds when crossing state lines. For example, when California first enacted its regulations, it required an available human driver behind the wheel at all times during testing on public roads; Michigan made no such requirement. (California is in the process of changing that standard, however, and revised regulations allowing test cars controlled by “remote operators” are pending approval by California’s Office of Administrative Law.)

In 2016, Google voiced its concern about the fragmented state of testing regulations: “We currently face a growing patchwork of state laws and regulations on self-driving cars that has the potential to become unworkable. . . . If every state is left to go its own way, it would be extremely impractical to operate an autonomous vehicle across state boundaries.” In September 2016, NHTSA partly cleared the way by providing guidance on the anticipated
division of responsibilities between the states and the federal government. The agency stated that it would be responsible for promulgating national standards for compliance, recall, certification, and safety, while states would need to address licensing and registration requirements, traffic laws, safety inspections, and insurance and liability procedures.

For safety standards, the agency has begun reviews of software technology, lidar (light detection and ranging laser technology), sensors, and other autonomous vehicle systems to ensure each has a robust security system in place before commercialization. No NHTSA standards are in place yet that directly address safety requirements for autonomous vehicles, but NHTSA released a 15-point safety assessment providing manufacturers with guidance on what future requirements to expect. For general standards, NHTSA plans to transition autonomous vehicles away from the status quo of self-regulation to standards that require pre-clearance from the agency—standards similarly seen in the aviation industry.

6. Conclusion

As with many technologies, it is too early to know the exact road of innovation. Rapid development of autonomous vehicles will no doubt present the above legal challenges to lawmakers, manufacturers, lawyers, and public and private parties. Companies in the industry will do well to aggressively address such challenges. This will allow them to concentrate on innovation rather than be mired later by legal and regulatory processes. The urgency to overcome these challenges will not diminish, as the development of autonomous vehicles shows no signs of slowing.

The authors would like to recognize summer associate Negah Daily for her contributions in drafting this article.

6. Id.
7. Lee, supra note 4, at 41.
8. Kohler, supra note 5, at 123.


12. Id. at 2.

13. Id. at 11.


16. Id.


25. Id.


27. Id. at 113.


30. Driverless Car Law, supra note 18, at 69.

31. Canis, supra note 11, at 11.

32. Driverless Car Law, supra note 18, at 118–19.

33. Lafrance, supra note 2.

34. Kohler, supra note 5, at 120–21.

35. Driverless Car Law, supra note 18.

36. Id.

37. Id.

38. Driverless Car Law, supra note 18, at 123.


40. Driverless Car Law, supra note 18.

41. Id.

42. Id.; see also Section 313.2, Compendium of the Copyright Office Practices (2014).

43. Balough, supra note 29.

44. Driverless Car Law, supra note 18.


46. Kohler, supra note 5, at 109.

47. Driverless Car Law, supra note 18.


53. Id.


**RELATED PRACTICES**

Connected and Autonomous Vehicle Team