Autonomous Vehicles – Data Privacy Issues

June 13, 2018

In the next five years we will see more and more self-driving vehicles, or autonomous vehicles, hit the market. An “autonomous vehicle” is a vehicle capable of navigating roadways and interpreting traffic-control devices without a driver actively operating any of the vehicle’s control systems. Although self-driving vehicles have the potential to drastically reduce accidents, travel time, and the environmental impact of road travel, concerns remain that could delay widespread adoption. Of particular concern are data privacy and security risks.

Seventeen states—Arkansas, California, Colorado, Connecticut, Delaware, Maine, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Texas, Utah, Virginia, and Washington—and the District of Columbia have enacted statutes relating to the data privacy issues of data retrieval from event data recorders (“EDRs”).¹ EDRs capture driver behavior information, such as the speed of a vehicle, braking pattern, and collision information. These states require obtaining the consent of the vehicle owner or policyholder before one can download data collected from a motor vehicle's EDR. Although these seventeen states have addressed issues relating to data privacy by regulating data retrieval from EDRs, only North Dakota has enacted legislation that specifically mentions “data privacy.” That legislation requires the department of transportation to study the data and information stored and gathered by the use of self-driving vehicles.

In addition to these seventeen states, automotive industry representatives have passed their own self-regulatory guidelines to address the data privacy issues of self-driving vehicles. In 2014 the Alliance of Automobile Manufacturers and the Association of Global Automakers enacted a set of “Privacy Principles” for vehicle technology and services.² Participating automobile manufacturers commit to comply with seven Privacy Principles, which govern the collection, use, and disclosure of driver behavior information retrieved from self-driving vehicles. These seven Privacy Principles are listed below.
Along with the states and the automotive industry that have enacted regulations regarding data privacy and self-driving vehicles, the federal government has also addressed these unique privacy issues. In December 2016 the National Highway Traffic Safety Administration released a proposal to mandate privacy measures relating to vehicle-to-vehicle (V2V) communications technology, which is used between self-driving vehicles to communicate the speed and location of each vehicle, the number of passengers in each vehicle, and more.\(^3\) Amongst other things, the proposal establishes a system that issues, distributes, and revokes security credentials for V2V devices and reports misbehavior. Additionally, the Federal Trade Commission and the NHTSA held a joint workshop on June 28, 2017 to examine the consumer privacy and security issues posed by self-driving vehicles.\(^4\) The workshop brought together various stakeholders, including industry representatives, consumer advocates, academics, and government regulators to discuss numerous issues related to self-driving vehicles that collect data.

<table>
<thead>
<tr>
<th>75%</th>
<th>33</th>
<th>17</th>
<th>$137 billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The estimated percentage of road traffic that will be occupied by self-driving vehicles by 2040.(^5)</td>
<td>The number of states to date that have introduced legislation relating to self-driving vehicles.(^6)</td>
<td>The number of states as of December 2016 that have introduced legislation relating to both self-driving vehicles and data privacy.(^7)</td>
<td>The amount of money by which the autonomous vehicle technology could shrink the auto insurance sector by 2050.(^8)</td>
</tr>
</tbody>
</table>

Privacy Principles enacted by the Alliance of Automobile Manufacturers and the Association of Global Automakers:

1. **Transparency** - Members should provide owners and registered users with ready access to clear, meaningful notices about the member’s collection, use, and sharing of covered information.

2. **Choice** - Members should offer owners and registered users with certain choices regarding the collection, use, and sharing of covered information.

3. **Respect for Context** - Members should use and share covered information in ways that are consistent with the context in which the covered information was collected, taking account of the likely impact on owners and registered users.
4. **Data Minimization** - Members should collect covered information only as needed for legitimate business purposes and retaining covered information no longer than they determine necessary.

5. **Data Security** - Members should implement reasonable measures to protect covered information against loss and unauthorized access or use.

6. **Integrity and Access** - Members should implement reasonable measures to maintain the accuracy of covered information and give owners and registered users reasonable means to review and correct personal subscription information.

7. **Accountability** - Members should take reasonable steps to ensure that they and other entities that receive covered information adhere to these Privacy Principles.

Questions to consider when addressing data privacy issues of self-driving vehicles:

What type of information regarding driver behavior information do self-driving vehicles collect, store, and transmit?

1. Can someone track an individual or a vehicle through access to driver behavior information?
2. How do consumers benefit from the collection and use of their driver behavior information?
3. Who owns driver behavior information and what are their rights to its usage?
4. Will your company be required to grant law enforcement access to the driver behavior information?
5. If you have access to driver behavior information, how will you use this information? Will your company use it to serve advertisements?
6. Will the driver behavior information be provided to insurance companies for underwriting purposes or to third parties that develop some kind of a driving score related to where and when individuals travel?
7. How will your company communicate its privacy policies and practices with regard to driver behavior information to consumers?


5. Institute of Electrical and Electronics Engineers, You Won’t Need a Driver’s License by 2040 (Sep. 15, 2014), http://sites.ieee.org/itss/2014/09/15/you-wont-need-a-drivers-license-by-2040/.


This document provides a general summary and is for information/educational purposes only. It is not intended to be comprehensive, nor does it constitute legal advice. Specific legal advice should always be sought before taking or refraining from taking any action.