EXPERT COMMENTARY

Federal U.S. Autonomous Vehicle Bill Would Update Safety Standards and Require Detailed Privacy and Cybersecurity Plans

Authored by Steven Wernikoff of Honigman LLP on Nov 02, 2020

On September 23, 2020, Representatives Bob Latta (R-Ohio) and Greg Walden (R-Ore.) re-introduced the "Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act" or the "SELF DRIVE Act" to create a federal framework for autonomous vehicles ("AVs"). The measure lacks bipartisan support and is not expected to reach the floor of the House of Representatives during this session. But the continued effort demonstrates the importance that many lawmakers put on promoting a U.S.-led effort in the development of self-driving vehicles. The matter likely will be among the key transportation themes before the next session of Congress, which convenes in January. On the Senate side, policymakers have not advanced autonomous vehicle bills. In the previous congressional session, an autonomous vehicle policy message advanced in the House but came up short in the Senate.

The SELF DRIVE Act would contain a number of key provisions, including:

Federal Motor Vehicle Safety Standards (FMVSSs)

The Department of Transportation would be required to update or issue new FMVSSs for highly automated vehicles on an expedited schedule.

The law would allow the Secretary of Transportation to grant exemptions to FMVSSs that require cars to have human operators. Initially, 25,000 vehicles per automaker could be operated if companies can prove they meet existing safety standards for traditional cars. After a 12-month period, the number of exemptions per manufacturer would increase to 50,000, and it would go up to 100,000 in the third and fourth years.

Safety Assessment Letters

Companies manufacturing highly automated vehicles would be required to issue safety assessment letters to the National Highway Traffic Safety Administration ("NHTSA") as contemplated by the Federal Automated Vehicles Policy issued in September 2016.

Cybersecurity Plan

Before selling any highly automated vehicle or automated driving system, manufacturers would be required to develop a cybersecurity plan that includes:

- a written cybersecurity policy with respect to the practices of the manufacturer for detecting and responding to cyber-attacks, unauthorized intrusions, and false and spurious messages or vehicle control commands, including:
    - a process for identifying, assessing, and mitigating reasonably foreseeable vulnerabilities from cyber-attacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands; and
    - a process for taking preventive and corrective action to mitigate against vulnerabilities in a highly automated vehicle or a vehicle that performs partial driving automation, including incident response plans, intrusion detection and prevention systems that safeguard key controls, systems and procedures through testing or monitoring, and updates to such process based on changed circumstances;
- the identification of an officer or other individual of the manufacturer as the point of contact with responsibility for the management of cybersecurity;
- a process for limiting access to automated driving systems; and
- a process for employee training and supervision for implementation and maintenance of the policies and procedures required by this section, including controls on employee access to automated driving systems.

Advisory Council

The NHTSA would be required to establish the Highly Automated Vehicle Advisory Council that would be responsible for, among other things, devising best practices and recommendations for cybersecurity for the testing, deployment, and updating of automated driving system as well as advancing mobility access for the disabled community and senior citizens.

Privacy Plan

The law would not allow a manufacturer to sell any highly automated vehicle or automated driving system unless the manufacturer developed a privacy plan that includes:

· a written privacy plan with respect to the collection, use, sharing, and storage of information about vehicle owners or occupants collected by a highly automated vehicle, vehicle that performs partial driving automation, or automated driving system that includes:

o the way that information about vehicle owners or occupants is collected, used, shared, or stored;

o the choices offered to vehicle owners or occupants regarding the collection, use, sharing, and storage of information;

o data minimization, de-identification, and retention of information about vehicle owners or occupants, and

o the practices of the manufacturer with respect to extending its privacy plan to the entities with which it shares such information;

· a method for providing notice to vehicle owners or occupants about the privacy plan;

· if information about vehicle owners or occupants is altered or combined so that the information can no longer reasonably be linked to the highly automated vehicle, vehicle that performs partial driving automation, or automated driving system from which the information is retrieved or to the vehicle owner or occupants, the manufacturer is not required to include the process or practices regarding that information in the privacy plan; and

· if information about an occupant is anonymized or encrypted, the manufacturer is not required to include the process or practices regarding that information in the privacy plan.

A violation of this provision would be treated as an unfair or deceptive act or practice under the Federal Trade Commission ("FTC") Act.

FTC Study

The law would require the FTC to conduct a study and submit a report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the highly automated vehicle marketplace, including an examination of the following issues:

· Which entities in the ecosystem have access to vehicle owner or occupant data?

· Which entities in the highly automated vehicle marketplace have privacy plans?

· What are the terms and disclosures made in such privacy plans, including regarding the collection, use, sharing, and storage of vehicle owner or occupant data?

· What disclosures are made to consumers about such privacy plans?

· What methods are available to enable deletion of information about vehicle owners or occupants from any data storage system within the vehicle (other than a system that is critical to the safety or operation of the vehicle) before the vehicle is sold, leased or rented, or otherwise occupied by a new owner or occupant?