

ConsumersUnion®

POLICY & ACTION FROM CONSUMER REPORTS

September 6, 2017

U.S. House of Representatives
Washington, D.C. 20515

Dear Representative:

Consumers Union, the policy and mobilization division of Consumer Reports, writes regarding H.R. 3388, the SELF DRIVE Act, which the House is expected to consider later today. This legislation would establish a new legal framework for the testing and deployment of highly automated vehicles (HAVs). While several portions of the SELF DRIVE Act would benefit consumer safety, we are very concerned about other provisions in the bill that would change federal law in ways that would open regulatory gaps and fail to adequately protect consumers from vehicle safety hazards. Accordingly, we do not believe that the SELF DRIVE Act is ready to become the law of the land. The legislation needs critical improvements to ensure that it enhances the safety and security of Americans on our roads.

Self-driving cars have enormous potential to make our roads safer by significantly reducing crashes attributable to driver error, and to improve mobility for millions of older Americans, individuals with disabilities, and other consumers nationwide. In June testimony before a House Energy and Commerce subcommittee, Consumers Union urged companies and policymakers to follow a smart, safe path to realize this promise. We called on Congress to embrace both technological ambition and accountability by setting a clear expectation that HAVs should improve safety, and by requiring sensible, enforceable, evidence-based measures to protect consumers against new hazards that may emerge.

Several parts of the legislation are consistent with this path, including:

- Companies must submit safety assessment certifications for HAVs to the National Highway Traffic Safety Administration (NHTSA).
- NHTSA must regularly set a safety priority plan to help determine initiatives to prioritize.
- Companies must develop cybersecurity plans to safeguard occupants and their data from unauthorized intrusions.
- NHTSA must research and implement the most effective method and terminology for informing consumers about fully and partially automated vehicles' capabilities and limitations, helping drivers use those systems more safely.

The bill also includes a critically important provision to prevent child heatstroke in hot cars by requiring new vehicles to come equipped with a rear seat occupant alert. These

systems—some of which are in cars today—will save lives. Since just 1998, more than 700 children have died from heatstroke after being left in hot cars.¹

However, we are very concerned about several ways in which the bill fails to protect consumers or ensure that self-driving cars actually improve safety. We make several recommendations on ways the bill should be strengthened before enactment, including:

- First and foremost, cars must protect occupants in the event of a crash, regardless of whether vehicles are self-driving or not. No exemptions from motor vehicle safety standards should be granted that would undermine impact protection for occupants.
- Exemptions from federal safety standards for HAVs should be limited to equipment required exclusively for the driving task that may be fully replaced by automation, and granted only if backed by evidence that a new feature maintains and enhances safety.
- The overall number of vehicles that can receive safety exemptions should be significantly reduced, and neither the number of exempted vehicles nor the duration of exemptions should be increased without specific safety-related justifications as part of an official, public notice-and-comment process.
- NHTSA should have access to crash data for all automated vehicles, not just those receiving exemptions, in order to oversee the safety of these cars. Also, the quarterly reporting envisioned by the bill is too infrequent. Cars today already have the ability to quickly send crash data to automakers, and accordingly, there should be a shorter time frame for reporting to NHTSA. A 15-day deadline for reports would be appropriate.

With regard to the legal authority of states and localities, the preemption language in the bill could lead to a regulatory vacuum that would put consumers at risk. Where strong federal safety standards are absent, Congress should not limit states and localities' ability to keep roads safe or to close gaps in protection that exist. Any enacted bill should not undermine traditional state and local roles, including over consumer data privacy and the safe operation of vehicles on public roads.

Additionally, while we appreciate members' efforts to include data privacy and security considerations in the SELF DRIVE Act, the bill's protections should be significantly stronger. Despite requiring companies to develop a cybersecurity plan, the bill does not require automakers to notify consumers of system breaches or of updates to a car's security protections. Also, the bill's section on companies' privacy plans requires transparency about data practices only for HAVs—but not other cars that may collect just as much personal information—and it affords consumers no control over or access to the data generated by their vehicles. Nor does the bill provide protections regarding the commercial use or sale of drivers' personal information. In addition, the transparency requirements under the proposed privacy plans have broad, undefined exceptions for “anonymous” and “encrypted” data. “Anonymous” data should be carefully defined to ensure that such data is not reasonably linkable to a driver or vehicle,² while an

¹ Null, J., CCM. “Trends and Patterns in Pediatric Vehicular Heatstroke Deaths, 1998-2016,” San Jose State University Department of Meteorology and Climate Science (June 2017) (online at noheatstroke.org/Heatstroke_Trends.pdf).

² We recommend using the term “de-identified” as defined in the Federal Trade Commission's 2012 Privacy Report. Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change” (Mar. 2012) (online at

exception for encrypted data should be removed altogether, since encryption is an important security measure to prohibit outside attackers from accessing data, but it does not provide privacy protection if the manufacturer or service provider possess the ability to decrypt the data.

Finally, the House should authorize significantly increased funding in this bill. These resources would be critical for NHTSA—a chronically underfunded agency—to be able to more effectively fulfill its existing efforts to address persistent driving hazards as well as the requirements in the bill.

In considering H.R. 3388 on the House floor, improving the safety and security of Americans should be members' top priority. We urge members to ensure that any accelerated deployment of automated vehicles is evidence-based—requiring manufacturers to demonstrate how automated systems improve safety—and includes sensible, binding measures to protect consumers against new hazards that may emerge. Taking these steps would help companies and the government take a smart, safe path to automated vehicles that would save lives, promote consumer trust in the technology, and help to realize the promise of self-driving cars. Thank you for your time and attention to this important subject.

Sincerely,

David Friedman
Director, Cars and Product
Policy and Analysis
Consumers Union

William Wallace
Policy Analyst
Consumers Union