December 7, 2018

Dear Senator,

As consumer protection and privacy rights organizations, representing millions of members and supporters, we are writing to express serious concern with how the AV Start Act, S 1885, could affect consumer privacy. Some of us also have concerns with other elements of the bill, but we are united in asking that the Congress not move forward on the legislation until our privacy concerns are resolved.

Our major concern with the draft AV Start legislation is that it will preempt state laws and regulations to protect consumer privacy, prevent data breaches and prevent misuse of personal information.

Two separate provisions of the bill would or may preempt state laws and standards in these areas.

First, Section 3 establishes complete preemption of state standards "regulating the design, construction, or performance of a highly automated vehicle or automated driving system" in specified subject areas. Those subject areas, described in Section 9 (which creates the new 49 USC section 30107(b)) cover both data recording and cybersecurity. The definition of "data recording" in section 30107(b)(2)(C) in particular is very broad: "The collection by the vehicle of automated driving system performance information … to enable efforts to work with other entities."

Second, the newly created Section 25 would require companies to provide a notice of their privacy policies and authorize the Federal Trade Commission to enforce that requirement; it does not require them to provide consumers with any control over the collection, use and disclosure of their personal information. Although this notice provision would provide far less protection than state laws, missing from the bill is a savings clause guaranteeing the right of states to maintain and enforce stronger privacy regulations. Absent such a clause, in light of preemption, the notice requirement would serve as the sole protection – state or federal – of drivers' privacy.

Worries about data mining are not a peripheral issue when it comes to the auto industry. With self-driving and increasingly connected cars, auto makers and transportation network companies will have an astounding amount of profoundly personal information about their customers, and they are actively evaluating how they can monetize it, in ways that may profoundly aggrieve consumers.

Here's how Ford CEO Jim Hackett recently described the company's views on data mining:

> We have 100 million people in vehicles today that are sitting in Ford blue-oval vehicles. That's the case for monetizing opportunity versus an upstart who maybe has, I don't know, what, they got 120, or 200,000 vehicles in place now. And so just compare the two stacks: Which one would you like to have the data from?
>
> The issue in the vehicle, see, is: We already know and have data on our customers. By the way, we protect this securely; they trust us," Hackett said. "We know what people make. How do we know that? It's because they borrow money from us. And when you ask somebody what they make, we know where they work, you know. We know if they're married. We know how long they've lived in their house because these are all on the credit

> applications. We've never ever been challenged on how we use that. And that's the leverage we got here with the data.[1]

These efforts are already underway. In October, the Detroit Free Press reported that, on an experimental basis, GM tracked radio listening habits in an effort that one analyst called a forerunner of plans to "actively monetize their data from their connected vehicles."[2]

Things are fast-moving in this space. Neither we nor the auto and transportation network companies know what practices will emerge five years from now. Precisely because of that uncertainty, states—typically far more nimble than the federal government in responding to changing circumstances—must remain free to protect their citizens. Indeed, states such as California have already adopted robust privacy protections and many more are considering new privacy laws. Every state has adopted its own data breach law. Overriding state authority to protect consumer privacy, at least as regards self-driving and connected cars, would be profoundly misguided and leave consumers vulnerable to a wide array of abusive practices, some of which we can't yet imagine.

These serious matters must not be ignored in the rush to pass the AV Start legislation, and make particularly worrisome the prospect that the bill will be attached to must-pass funding legislation. We urge that the bill not be considered until these privacy concerns are addressed.

To follow up on any matter in this letter, please contact Public Citizen.

Thank you,

Center for Auto Safety
Center for Digital Democracy
Center for Media Justice
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumer Watchdog
Digital Privacy Alliance
Media Alliance
Privacy Rights Clearinghouse
Public Citizen
U.S. PIRG

---

[1] Quoted in Phoebe Wall Howard, "Data Could Be What Ford Sells Next as it Looks for New Revenue," Detroit Free Press, November 13, 2018, available at: https://www.freep.com/story/money/cars/2018/11/13/ford-motor-credit-data-new-revenue/1967077002, quoting Hacket from the Freakonomics podcast: http://freakonomics.com/podcast/ford/

[2] Jamie LaReau, "GM Tracked Radio Listening Habits for Three Months: Here's Why," Detroit Free Press, October 1, 2018, available at: https://www.freep.com/story/money/cars/general-motors/2018/10/01/gm-radio-listening-habits-advertising/1424294002.