February 19, 2019

The Honorable Jennifer Williamson
Chair, House Judiciary Committee
900 Court St. NE
Salem Oregon 97301

RE: HB 2395 - RELATING TO SECURITY MEASURES REQUIRED FOR DEVICES THAT CONNECT TO THE INTERNET - OPPOSE

Dear Representative Williamson:

Global Automakers, www.globalautomakers.org, is writing to inform you of **our opposition to HB 2395**, which requires manufactures of connected devices to equip the connected device with certain security features.

Global Automakers represents the U.S. operations of international motor vehicle manufacturers, original equipment suppliers, and other automotive-related trade associations. Our goal in Oregon (and elsewhere) is to foster an open and competitive automotive marketplace and to create public policy that improves motor vehicle safety, encourages technological innovation and protects our planet. Our members manufactured 53% of all new vehicles sold in the state and 61% of all green vehicles.

Our Position

Global Automakers opposes HB 2395 as introduced. HB 2395 is like legislation passed in California, however, HB 2395 lacks notable exemptions that were included in the California legislation. Like the California legislation, HB 2395 imposes vague and open-ended requirements that will require manufacturers to grapple with its interpretation when designing product security features.

However, HB 2395 lacks a critical exemption included in California's legislation. California's law states that its provisions do not apply to a device "the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority." Automobiles fall under this exemption because they are already covered by cybersecurity best practice guidance published by the National Highway Traffic Safety Administration.[1]

Additionally, the auto industry has taken proactive measures to protect consumer privacy by developing the automotive "Privacy Principles" which commit automakers to take certain steps

[1] https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

to protect the personal data generated by their vehicles.[2] The Principles' fundamentals are based on the Federal Trade Commission's (FTC) Fair Information Practice Principles (FIPPs), which, in turn, rest on privacy practice frameworks used in the United States and around the world for over forty years. These Privacy Principles have been expressly adopted by the vast majority of the auto industry and are enforceable by the Federal Trade Commission (FTC).

Additionally, given action at the federal level, HB 2395 is not necessary to protect consumers in Oregon. For example, the FTC, which has broad authority over consumer product safety under section 5 of the FTC Act, issued the Internet of Things Privacy & Security in a Connected World guidance document in 2015. The FTC has also taken enforcement action against connected device manufacturers, thus developing a set of regulatory expectations for manufacturers with respect to cybersecurity. Similarly, the FTC and the National Highway Traffic Safety Administration (NHTSA) held a workshop on security and safety of autonomous vehicles in June 2017, in part to discuss developing standards.

While the California law has serious problems with its overbroad and vague language, the exemption noted above provides a crucial level of clarity for manufacturers which is missing in HB 2395. At a minimum, HB 2395 should be amended to include this same exemption.

Global Automakers looks forward to working with members of the Oregon legislature to address these issues.

Please let us know if you have any questions.

Sincerely,

Josh Fisher
Senior Manager, State Government Affairs

[2] https://www.globalautomakers.org/posts/papers-reports/privacy-principles-vehicle-technologies-services