Testimony on HB 3152
House Committee on Business and Labor
April 8, 2019

Sophia Anderson
Salem, OR

My name is Sophia Anderson. I am a Senior at Willamette University, majoring in computer science. I am also a founding member of the Student (Cyber) Security League, an effort I spearheaded to integrate cybersecurity education into our computer science curriculum.

I'd like to preface my statement by sharing that I had to read HB 3152 eight times and consult a politics professor to understand what it tries to accomplish. Quite frankly, I wasn't very impressed when I finally figured it out – and I'm still not.

History shows us that forcing companies that specialize in secure databases to allow arbitrary, external contractors of an automobile dealer to access billions of files of stored data (as defined in Section 2.2(a) – (c)) is not likely to end well.

In 2009, MySpace partnered with a company named RockYou to integrate external apps into their site. Neither company was aware RockYou's code had a known, 10-year old, SQL injection vulnerability; but when one hacker discovered the flaw, he navigated into the system and ultimately accessed 32 million MySpace login credentials. The credentials stolen are known as the "Rock You Wordlist" and is still used today -- by both professional hackers and script kiddies alike -- as a tool to crack insecure passwords.

Similarly, in 2013 Target Stores hired an HVAC company to work in several stores and gave the company network access to remotely monitor stores' energy consumption. A single hacker stole the credential of one HVAC employee and used those credentials to access Target's network – allowing them to install malware that siphoned off 40 million credit card numbers in 18 days.

These are just two examples, but they are analogous to the dangers this bill would create. Allowing arbitrary access to secure systems by unvetted third parties can leave a previously secure company very vulnerable. The stakes are even higher here than they were for MySpace or Target since we're talking about everything from drivers' license information to social security numbers.

These security protocols may make it harder for auto dealers to access the data they need or want to work with, but security is not about convenience — it's about making sure the personal data of consumers isn't stolen and misused. A system is only as strong as its weakest link, and believe me, you don't want to be the one that breaks that chain.

Thank you.