Testimony of Branden Pearson
HB 3152
Joint Committee on Transportation
May 1, 2019

Co-Chairs Beyer and McKeown, Members of the Committee:

I am Branden Pearson. As an information technology professional charged with the securing protected consumer information, I urge you to reject HB 3512.

I am the Chief Information Officer for a $400 million organization headquartered in Beaverton, but I speak today as a concerned citizen who has been the victim of identity theft. My opinions are based solely on my training and 25 years of professional experience in the information technology and healthcare information technology industries.

Every day, I ensure data can flow through our organization to allow team members to be creative, efficient, and effective. I am also charged with safeguarding – against internal and external threats - our proprietary corporate data, our suppliers' data, and our customers' data. This is a balance that requires respect for data managers and consumers, trust in the IT systems we oversee, and a healthy respect for hackers and data thieves who are smart, relentless, and absolutely committed to stealing valuable information and intellectual property that will make them lots of money, regardless of the lives they ruin in the process.

To thwart potential threats, we have developed carefully crafted policies, procedures, and security postures. Employees' access to data is strictly monitored and individuals with access are screened and trained on privacy and security best practices. We ensure the minimum amount of necessary data is shared, and only with those who have a need to know. This is the most effective path to protecting sensitive data and is the standard best practice for companies around the globe.

To protect intellectual property and consumer privacy we use state-of-the-art monitoring and intrusion detection and penetration testing, and we constantly assess the vulnerability of our networks and data management systems.

The legislation before you leaves me confused. It would mandate unrestricted access to consumer data and is completely at odds with global privacy and security best practices. Forcing companies to open their systems to allow for easier access, by greater numbers of individuals and companies, will drastically increase the likelihood of data breach, data theft, and data misuse. This will increase the opportunity for hackers to breach previously secure data management systems and increase the likelihood of identity theft and extortion.

Cybersecurity is a process that is focused on continual improvement. The question is not whether you will have a breach of information, but when. Our business security best practices and laws must be aligned to make sure our personally identifiable information is secure. Despite these best efforts, no matter what we do, nefarious agents and bad actors will seek ways to obtain intellectual property and personally identifiable information. We should not have laws that require security conscious people and organizations to put out a welcome mat for individuals and groups who seek to do us harm.

Please reject this legislation.

Thank you.