Written Testimony — SB 1516

Position: Support with amendments

To the House Committee on Rules,

My name is Evan Reese, and I am an IT professional and a constituent of Newberg. My statement is regarding Senate Bill 1516 and the regulation of Automated License Plate Readers (ALPRs). When establishing requirements for ALPR vendors, I believe that it is critical for the legislation to include accurate technical language and clear data retention timelines.

Defining End-to-End Encryption

My first request is for the committee to include an explicit definition of "end-to-end encryption" to ensure that only the law enforcement agency that owns the data can access the decryption keys, **such as the definition found in the -15 amendment**.

Without a strict definition of end-to-end encryption, vendors will continue to use the term to benefit themselves at the expense of public safety. This was observed with Zoom in 2020: just months after receiving an influx of users due to the pandemic, an FTC press release revealed that Zoom had significantly misrepresented its encryption standards [https://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement]. After claiming to use end-to-end encryption, it was found that Zoom held the technical capability to access, decrypt, and view recorded meetings, leaving users and their personal conversations fundamentally exposed.

Zoom is not a standalone case. In the last few years, multiple stories have reached mainstream news where companies claimed their users' data was protected by end to end encryption, when in reality it was not as secure as the public was made to believe. By creating this baseline definition of end-to-end encryption for ALPR vendors, we are setting ourselves up for long term success by significantly decreasing the opportunity for abuse of this deeply personal data that is being collected about every Oregonian on the road.

48hr Maximum Retention for ALPR Data

My second request is for the committee to set a retention period in this bill of no more than 48 hours for ALPR data that is not part of an active investigation. ALPR systems are designed to instantly match license plates against active hotlists like stolen vehicles or Amber Alerts. If a match is not found, there is no reason to retain this data for weeks or even days.

By storing data not associated with an investigation, we are creating avoidable opportunities for theft by cyber attack or abuse by an insider. These threats are not theoretical: in November, Chief Michael Steffman of the Braselton Police Department in Georgia was arrested and charged for multiple counts of stalking and harassment through the misuse of ALPR data [http://gbi.georgia.gov/press-releases/2025-11-19/gbi-arrests-braselton-police-chief-harassment-and-stalking]. Instances of stalking, harassment, and abuse using ALPR systems are sadly not rare. Decreasing the data retention period will reduce the risk of this abuse taking place in our state.

To summarize, I am requesting for a strict definition of end-to-end encryption and a 48hr maximum retention on ALPR data not associated with an investigation be amended into this bill. Thank you for your time and your commitment to protecting the privacy of Oregonians.

Sincerely,

Evan Reese

Newberg, Oregon