March 3, 2026

Regarding 2026 SB1516

I helped author significant portions of the ALPR section of SB1516, up to SB1516-12. As it is currently written, I strongly **oppose** SB1516, and request that you pass SB1516-15 to restore this bill to its intended language.

The entire content of SB1516-15 is:

> ‘End-to-end encryption’ means a method of data encryption that ensures only the owner of the captured license plate data possesses the capability to decrypt, access or grant access to the data.

I have been a software engineer for 30 years and have been responsible for defensive security and incident response at large organizations. I understand software, and technology generally, *very* well. My role in SB1516’s development was to provide technical guidance on the language of the bill to ensure that it accomplished the aims set forth by Senator Prozanski: to ensure that license plate data captured by ALPR systems stayed in the hands of local law enforcement.

The CISO and CIO of the state’s Enterprise Information Services department have recently issued two letters. Both of them are incorrect on technical grounds. The state CIO’s letter, dated March 1, states: “...we do not recommend defining security standards or architecture in statute due to the rapid rate at which technology changes.”

But, read the definition of end-to-end encryption above. It is written in plain English. Nothing about it will be impacted by changing technology, because it makes no statement about what technology to use; it just explains what the technology is supposed to accomplish.

What that single sentence does is explain, clearly and in plain English, that only law enforcement agencies should have access to ALPR data. That’s it.

ALPR companies have been fighting this language since the beginning of Senator Prozanski’s workgroup. This language prevents ALPR companies from making money off of their access to ALPR data by removing that access. It requires them to implement sensible controls that *ensure* that they cannot abuse their access to data in the way they have been.

Look carefully at the cc: at the bottom of both of those letters, and you’ll see “Rebecca David, OSP” (Oregon State Police). Rebecca David was a member of Senator Prozanski’s workgroup, and she worked directly on behalf of the ALPR vendor Axon to protect their business interests. She repeatedly took language developed in the workgroup back to Axon to get their permission for it. Axon was never invited to participate. After the workgroup concluded, Axon – fearing that it would lose the direct access to data that it treasures so much – used her to get state offices involved on their behalf. The state CISO’s letter *plainly* defends the business interests of a private company.

We had a conversation with the state CISO shortly before his letter. He had absolutely no understanding of ALPR technology or how the data was managed by those vendors. The words in these letters are not the words of tech professionals; they came from Axon.
The CIO’s letter states, “Testimony from the public, some of whom are information technology professionals, call for safeguards…” Look at the testimony that has been submitted to SB1516, both in person and in writing, and at the number of tech professionals with specializations in security. The safeguard they are calling for is **end to end encryption**, as described in the -15 amendment.

I could have explained any and all of this to any of you if I could have got just a few minutes of your time at any point in the process, but it seems that understanding the things we vote on is not a part of our culture.

Regards,

Rob Sheldon