| | |
|---|---|
| Submitter: | Richard Zeller |
| On Behalf Of: | Self |
| Committee: | Senate Committee On Judiciary |
| Measure, Appointment or Topic: | SB1516 |

Dear Senator and Chair Prozanski, Vice Chair Thatcher, members of the Committee,

I write in support SB 1516 and in favor of strengthening certain provisions.

I'm concerned about the misuse of data from Automatic License Plate Readers (ALPR) and the serious risks it poses to Oregonians' privacy and safety. While this technology poses particular risks for immigrants, refugees, and those accessing reproductive healthcare, their proliferation represents a far more serious risk to the freedom of every Oregonian. I am proud to live in Eugene, where Flock cameras have been removed, because there are no current restrictions on how data from such cameras can be used.

In many places, data from Flock (the contractor for the systems Eugene has removed) has been used by law enforcement agencies and Palantir Technologies to integrate information for other than clear law enforcement purposes. This technology and the processes for data integration, however justifiable it may seem for enforcement of the law, open the door to government and private entity surveillance of the kind used by authoritarian regimes who have no respect for individual rights. That this is happening in the United States and is being expanded is frightful, to say the least.

With respect to the risks to immigrants, in Oregon and across the country ALPR data has been used by ICE, and there are documented cases of ALPR data being used to target people accessing abortion services. What might it be used for next? Tracking protesters at ICE offices? Monitoring individuals seeking other medical services (e.g., transitional services or surgery)? The integration of facial recognition with images recorded by these devices would risk incredible violations of individual privacy.

This bill should address at least:
1). Clear prohibitions on access by federal and out-of-state law enforcement agencies without a judicial warrant specific to the individual sought.
2). Strong data-security requirements, including for data to be protected with end-to-end encryption, for its use and storage in Oregon, and any sharing elsewhere.
3). Strict data retention limits less than 30 days. A 30-day retention period would allow the accumulation of large data troves that endanger vulnerable communities.

Thank you for the Committee's attention to this very important and sensitive issue.