unacast.

Senator Floyd Prozanski, Chair
Senator Kim Thatcher, Vice Chair
Senate Committee On Judiciary
900 Court Street
Salem, OR 97301

May 5, 2025

Dear Chair Prozanski and Vice Chair Thatcher:

I am writing to express my concerns over HB 2008, which is scheduled to be heard before the Committee on Judiciary (the "Committee") on May 5, 2025.

This bill, as presently drafted, would completely prohibit the sale of consumer location data without exception. The real-world impact of the destruction of access to location and mobility data solutions would have catastrophic consequences to individuals, businesses, communities, and municipalities living and operating throughout Oregon. As further outlined below, we implore the Committee to consider the severely negative consequences of passing such heavy-handed legislation. We further welcome additional discussions to craft legislation that will genuinely advance privacy interests, while still preserving the important business and social functions that rely on commercially available location data.

Value and Importance of Location Data

Location data currently allows for a variety of beneficial use cases that are essential for consumers and our communities throughout Oregon. Notable examples include:

- Studying food and health deserts to ensure equitable access to essential goods and services throughout Oregon.
- Improving traffic analytics throughout the greater Portland area, and the Portland-Salem corridor, to better understand commuting patterns and help develop solutions that reduce congestion.
- Evaluating and improving natural disaster and emergency response plans for the Federal Emergency Management Agency (FEMA).
- Helping locate missing children and victims of sex trafficking throughout Oregon, thanks to operations like Hotel Shield and the National Child Protection Task Force.
- Identifying and resolving transportation bottlenecks in the Pacific Northwest that negatively impact Oregon residents, including major freight and commuter delays along the I-5 corridor and the ongoing disruptions caused by infrastructure vulnerabilities such as landslides in the Columbia River Gorge and seismic risks to key bridges in Portland.

- Directly supporting the Environmental Protection Agency (EPA) to understand coastal erosion, beach and waterway usage, to adjust for the real-world impacts of climate change in the Oregon coast and other vulnerable regions of the Pacific Northwest.
- Helping business leaders and city planners in Oregon determine which types of businesses and infrastructure to bring to downtown areas based on the interests of its local residents.

Each of these important initiatives, among others, would be severely hampered if the location data solutions that power such projects were to suddenly disappear. We therefore implore the committee to consider other reasonable alternatives to an outright location data ban. Such alternatives include more targeted approaches like establishing limitations on geofencing of sensitive places of interest for certain use cases, as seen in other parts of the country like the Washington My Health My Data Act. We also strongly support the Oregon Consumer Privacy Act as a meaningful step toward protecting residents' personal data. We encourage the committee to ensure its continued successful implementation and consider future enhancements that maintain thoughtful enforcement of privacy standards, such as notice and transparency requirements, and strengthen consumer protections around consent, opt-outs, and individual control over personal data. These privacy standards allow companies like ours to responsibly develop mobility analytics solutions that proudly serve businesses and public-sector end users throughout Oregon.

Industry Privacy Initiatives and Updates

Our industry is keenly aware of the potential risks that come with the misuse of location data, especially in a post-Dobbs world. We too want to ensure that individuals seeking reproductive and/or gender-affirming healthcare are protected. We also strongly believe LGBT rights are best protected when people can celebrate life with whomever they please, without fear they will later be outed on the basis of their digital breadcrumbs.

Consequently, over the past several years our industry has responded to these concerns by developing new privacy controls to curtail access to location data from sensitive locations. Much of these efforts are captured in our company's new privacy-enhancing technology, PrivacyCheck. Originally developed in 2019, we later launched this tool as an outward facing product following the *Dobbs v. Jackson* ruling, to help other companies remove location signals associated with sensitive places of interest. This endeavor has been supported in part thanks to the efforts of the Network Advertising Initiative (NAI), which has published industry-accepted definitions of sensitive locations, and today forms a baseline geofence library for stakeholders to determine which places of interest within our communities deserve additional location data privacy protections.

The success of these industry-side privacy initiatives runs in parallel to the positive regulatory developments from the U.S. Federal Trade Commission (FTC). In recent years the FTC has entered into a series of consent orders mandating the establishment of certain privacy controls for companies who process location data. These sensitive location data programs have formalized pre-existing efforts to develop comprehensive lists of sensitive locations to prevent

the use, sale, licensing, transfer, sharing, or disclosure of sensitive location data, unless a legitimate use-case like national security would apply. Our company strongly supports the regulatory outcome of these efforts, which is why we were a proud signatory to such an Order in late 2024.

Today, our company enables private and public sector end users of all shapes and sizes to leverage location data with the data from such sensitive places removed. This outcome strikes a much needed balance between preserving the need and important functions of mobility data solutions, while also directly addressing the privacy concerns that stems from mobile device activity at certain locations within our communities.

H2008 would create government-sanctioned Big Tech monopolies

Increasingly, a small number of giant tech companies have been able to exploit their direct connection to consumer data to ensure that access to such data is exclusively on their terms. In doing so, Big Tech companies have come to dominate and manipulate previously democratized digital ecosystems by restricting access to these important datasets. A ban on the sale of location data would not disrupt this ability. In fact, it would make these companies more powerful.

For now, companies like ours are still able to provide a quasi-independent supply of data that is not under the direct control of Big Tech companies. Despite these efforts, the increasing deployment of digital walled gardens creates conditions where only a select few companies will be able to access these datasets. As time goes on, restrictions to the open access of commercially available data will block small and medium sized businesses from accessing this data, further preventing important stakeholders like researchers, universities, and others from having the opportunity to glean insights from these datasets.

Prohibiting the sale of location data will not stop the aggregation of location data. It will simply consolidate this data into the hands of a few global technology companies who have the exclusive ability to collect and monetize it. This will create a significant disadvantage for businesses in all other industries and the general public, who today greatly benefit from the equitable access to insights that only mobile location data can provide.

Oregon needs fair and open competition in its digital sector, not government-mandated monopolies that exclusively favor Big Tech.

Conclusion:

In conclusion, this bill, while well-intentioned, represents a flawed approach to the protection of individual and collective civil and privacy rights. They serve the interests of big tech rather than the general public. By making it illegal to sell and purchase location data, this legislation will make this critical data, and the intelligence it provides, unavailable to all but the world's biggest technology companies. Businesses in other industries, as well as government entities, would need to rely on big tech for the type of intelligence they glean from commercially available location data today, shoring up big tech's competitive advantage for another generation.

Together, we can craft legislation that protects consumer privacy rights while also ensuring that we can support the many commercial use cases for location data that exist and benefit our society as a whole. We look forward to working with you to achieve these shared goals.

Sincerely,

Jason Sarfati
Chief Privacy Officer & VP Legal