



March 12, 2019

TO: House Committee on Judiciary  
FR: Charlie Fisher, State Director, Oregon State Public Interest Research Group (OSPIRG)  
RE: HB 2866

OSPIRG supports HB 2866 with -1 and -2 amendments.

As more of our daily life, work, and commerce lives online, a proliferation of companies are now tracking, sharing, and selling literally thousands of data bits about us, often without express consent, usually just to sell us more stuff.

At the very least, when a consumers' information is tracked while using a website, an app on their phone, or any other digital device, they should know what information about them is being tracked and with whom it is being shared or sold.

This is especially true for geolocation information and the use of cameras or microphones in a device. Last December, the New York Times did a comprehensive investigation into the collection and sharing of geolocation information from smart phones.<sup>i</sup> What they found was shocking:

- Geolocation information from phones was recorded “as often as every two seconds” and “in some cases ... more than 14,000 times a day.”
- When notifications occurred they were often misleading. For example, “An app may tell users that granting access to their location will help them get traffic information, but not mention that the data will be shared and sold.” In the New York Times analysis, “Of the 17 apps that The Times saw sending precise location data, just three on iOS and one on Android told users in a prompt during the permission process that the information could be used for advertising.”
- Sale of location information is big business, “with sales of location-targeted advertising reaching an estimated \$21 billion” in 2018.

There are similar concerns for microphone and camera-enabled devices. In 2017, OSPIRG's annual review of toy safety highlighted a “smart doll” intended to interact with and respond to children four and up.<sup>ii</sup> When the doll, My Friend Cayla, is connected to its companion smartphone app, it sends the contents of the conversation to two companies, Genesis, the manufacturer, and Nuance a voice recognition company. If HB 2866 were adopted, these companies would be required to get permission from parents before using the microphone, and would be required to disclose what information about their child is being tracked and whether and with whom it is shared, or sold.

While geo-location information and the use of microphone or camera-enabled devices is especially personal, which is why it requires affirmative consent in the bill, this practice of buying, selling, and sharing personal information about consumers without their knowledge is incredibly widespread. That's why for all information that is tracked about consumers through their use of digital devices, they should have the right to know what that information is how it is being used.

HB 2866 puts in place commonsense disclosure requirements to consumers and creates specific protections for especially sensitive forms of tracking.

Please support HB 2866, the Digital Transparency and Privacy Protection Act.

---

<sup>i</sup> [Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret](#), New York Times; Dec. 10, 2018

<sup>ii</sup> [Trouble in Toyland 2017](#), OSPIRG Foundation; November 21, 2017