Testimony of Kimberly McCullough, Policy Director
In Support of HB 2866, with -1 and -2 Amendments
House Judiciary Committee
March 12, 2019

Chair Williamson and Members of the Committee:

The American Civil Liberties Union of Oregon[1] supports HB 2866, with the -1 and -2 amendments, which would provide much-needed protections for Oregonians' digital data.

We Need Stronger Data Transparency & Privacy Protection Laws in Oregon.

As Americans spend more and more of their lives online, **it's vital that we protect the Internet from efforts to turn it into a privacy-free zone** where our every keystroke and click is monitored, stored, and sold. According to a Pew Research survey, 91% of adults believe that consumers have lost control over how personal information is collected and used by companies.[2]

Many operators of commercial websites and online services collect a tremendous amount of highly personal information from Oregonians. This can include facts about our health, finances, location, politics, religion, sexual orientation, and shopping habits. **Many operators share this information with third parties**, including advertisers and data brokers. This information has great financial value, so pressure to collect and share it will continue to grow.

We live more and more of our lives online. Our sensitive personal information, pooled into ever-larger reservoirs of data, can be sold to the highest bidder, stolen by those who intend to abuse and misuse it, and seized by or sold to government investigators. Legislation is needed to protect the privacy and physical safety of Oregonians—particularly children and domestic violence and stalking victims—from dangers posed by the collection, sharing and selling of our data.

---

[1] The American Civil Liberties Union of Oregon (ACLU of Oregon) is a nonpartisan, nonprofit organization dedicated to preservation and enhancement of civil liberties and civil rights, with more than 45,000 members and supporters statewide.

[2] Pew Research Center, Public Perceptions of Privacy and Security in the Post-Snowden Era, http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

For example, computer scientists at Carnegie Mellon University concluded that a dozen or so popular Android apps collected device location—GPS coordinates accurate to within 50 meters—an average of 6,200 times, or roughly every three minutes, per participant over a two-week study period.[3]

A national study conducted by the National Network to End Domestic Violence found that 72 percent of victim services programs across the country have seen victims who were tracked through a stalking app installed on a mobile phone or a stand-alone GPS device.

In 2016, a company selling internet-connected stuffed animals exposed a database containing over 2 million voice recordings, many of them children, to hackers who held the database for ransom, at least twice, demanding payment from the company in exchange for the safe return of the data.[4]

Oregonians and their families need basic, common-sense laws that provide transparency and privacy protections.

"**Right to Know**" provisions in HB 2866 will empower visitors to learn what personal information is gathered about them when they visit websites and online services and use digital electronic devices that connect to the Internet, and who that information is shared with or sold to. This will ensure that people can obtain the information they need to make fact-based decisions about where and how they want to spend their time online and which applications and digital devices they want to use.

Geolocation privacy protections in HB 2866 will protect Oregonians by making it unlawful for private parties to track, share or sell geolocation information collected from our smartphones or other mobile devices without our explicit permission.

Audiovisual privacy protections in HB 2866 will protect data that may be collected when our devices' microphones listen and cameras watch our most intimate information. If a corporation is using an internet-connected device to listen or watch, or to share or sell that information, then it should clearly tell consumers when they will do so, for what purpose, and first obtain permission.

---

[3] Wall Street Journal, "Apps Track Users—Once Every 3 Minutes", https://www.wsj.com/articles/apps-track-usersonce-every-3-minutes-1427166955

[4] Huffington Post, "If You Have One Of These Toys In Your House, You May Want To Stop Using It", https://www.huffingtonpost.com/entry/cloudpet-hack-recordings-messages_us_58b4aef0e4b0a8a9b7857b45

These common-sense protections would not restrict any website or online service from gathering or sharing information. **Businesses will simply need to be more transparent,** and take the necessary steps to obtain permission before collecting and sharing particularly sensitive location information and audiovisual recordings. These simple and reasonable requirements are needed to protect the personal information of Oregon consumers and children.

A FAQ is attached to this testimony to provide greater understanding and clarity about the provisions of HB 2866 and the -1 and -2 amendments.

For these reasons, the ACLU of Oregon urges you to support HB 2866, with the -1 and -2 amendments. Please feel free to contact us if you have any questions, comments, or concerns.

HB 2866 FAQ

Q: What kind of information is protected by this bill?

A: The bill provides transparency and privacy protections for personal, audiovisual and geolocation information that is generated and collected about us when we use our phones, laptops, and other digital devices that connect to the Internet. This includes:

- The personal information that Facebook, Instagram, and other social media sites collect about us when we use their applications.
- Audio recordings collected by digital devices like Alexa.
- The location information collected by applications that we use on our cell phones. For example, Google Maps, Pokemon Go!, and Yelp.
- Phone applications that use the camera and microphone on our cell phones or laptops to record information. For example, Instagram, Snapchat, and Skype.

We understand that there has been some confusion about the scope of this bill's protections. We sought the -2 amendments to clarify things. Please see more information about this below.

Q: What protections are provided for our personal information?

A: The bill has two main components:

First, we are given a Right to Know exactly what personal information has been collected, shared, or sold by the companies that operate social media sites, phone applications, digital devices that connect to the Internet. We can request a copy of this information one time per year.

Second, our consent is required before companies can collect, share or sell the audiovisual and geolocation information that has been generated through our use of digital electronic devices.

Q: Doesn't this create a huge burden for companies that create social media websites, applications, and digital devices that connect to the Internet?

A: No. If companies can manage to collect, share and sell our personal information, it should not be too big of a burden to simply provide us with a copy of what has been shared and sold. If websites and applications can be designed to collect, share and sell our information, they can also be designed to request consent (through the use of a pop-up or other method) before collecting, sharing and selling our information.

Q: I've heard this bill will make it impossible for news media to video events and for convenience stores to use surveillance cameras. Is that true?

A: No. The intent of this bill is not to change the rules that dictate what has to happen before one person can record or photograph another person. That type of activity is regulated by a completely separate area of law (including our wiretapping and eavesdropping laws). HB 2866 only provides transparency and privacy protections for data that is generated about an Oregon resident when that resident uses a digital device. Put another way, this is about the data that is collected *about us* when we use *our own* digital devices. It is not about what we can and cannot capture using a device.

Again, we understand that there has been some confusion about the scope of the bill, so we sought the -2 amendments to clarify things.

Q: Will this law impact our wiretapping or eavesdropping laws?

A: No. Wiretapping and eavesdropping laws regulate when one person can record audio of another person. If person A wants to record what person B says, Oregon law requires notice under certain circumstances. This bill is instead about the information that is collected about person A when person A uses a digital device, and about businesses that have access to that information.

Q: How does this work with apps and devices that need to collect location or audiovisual information in order to function?

A: Consumers will need to be given information about exactly what is being collected, shared and sold, AND they will need to consent to the collection, sharing or selling of location and audiovisual information before it actually happens. This will essentially require a pop-up that provides disclosures and asks for consent. Consent could also be given by the consumer going to a website to read relevant disclosures and provide authorization there. The bill is intentionally written broadly to allow businesses to obtain consent in a manner that works with their business model.

For devices that require the collection of information to function, a person will need to consent before they can use the device. We assume that a person who has purchased a device that requires the collection of information to function will be likely to consent, because they will want to use the device. That said, if the information is also going to be sold or shared, and that is not required for the functioning of the device, we anticipate that the act of being asked for consent will empower consumers to push back and ask for choices about what happens to their information once it is collected, which will in turn encourage tech companies to give consumers more choices.

Q: Does this bill apply to government actors and law enforcement?

A: No. The bill is aimed at parties involved in the commercial market. More specifically, it exempts "public bodies" and "law enforcement" from the bill.

However, it will help us know when our information is being shared with or sold to the government and have a positive impact on the development of our privacy protections from the government. See the two following questions and answers for more about that.

Q: Will this help me know if my personal information is being shared with or sold to the government?

A: Yes! The Right to Know provisions included in HB 2866 will help consumers know exactly what information is being shared or sold with the government. This is crucially important for Oregonians. If consumers are fully informed about the fact that information collected about them by a website, phone application or digital device is being sold to the FBI, for example, then they will be empowered to make better decisions about whether or not they want to use that website, application or device.

Q: Will this bill have an impact on the development of privacy laws that relate to the government?

A: Yes! It is very difficult to pass privacy protective legislation that limits government surveillance, when private entities are able to easily obtain the same information that we are trying to limit the government from obtaining. By strengthening our privacy protections in the consumer realm, we can more easily argue for the strengthening of our privacy rights against government surveillance.

In addition, our federal constitutional protections from unreasonable search and seizure (under the Fourth Amendment) are currently dictated by what is referred to as the "reasonable expectations of privacy" test. This test looks to our expectations of privacy from other people and limits our privacy protections from the government wherever we have no reasonable expectation of privacy. We fear a future where our expectations of privacy are so eroded that our constitutional rights under the Fourth Amendment are rendered meaningless. By creating protections in the consumer realm, we are increasing our expectations of privacy, which can only have a positive impact on our protections under the "reasonable expectations of privacy" test.

Q: Are there amendments to HB 2866, and what do they do?

A: Yes. There are currently two sets of amendments to the bill, both of which were drafted at our request. We are also open to engaging in discussions and amending the bill further to create greater clarity or to alleviate concerns of various stakeholders.

The -1 amendments:

- Clarify that geolocation information is information that displays the location of a digital device on a map, removing extraneous language in the definition.
- Broaden the definition of "Resident Individual" to include natural persons within the Oregon state boundary. This clarifies that anyone who is physically in Oregon will benefit from our privacy laws, rather than needing to live here.
- Remove language that inadvertently created a loophole in the bill by allowing an unnecessary exception to the consent requirements related to audiovisual and location information.
- Add a clause that prohibits claims under the bill's private right of action from being subjected to arbitration, thus ensuring that Oregonians will be able to assert their rights in court and benefit from the court appeals process and the transparency associated with court proceedings. Arbitration of consumer claims limits consumer rights, and often means that the claims are never known about by the general public.
- Clarify that personal health information is subject to the bill's protections.
- Prohibit businesses from discriminating against consumers who exercise their privacy rights under the bill. This includes a prohibition on charging additional money to consumers who assert their privacy rights or degrading the level of service for those consumers.

The -2 amendments:

- Clarify that the bill is focused on what happens to the audiovisual information our phones, laptops, and other digital devices collect about us when we use them, rather than regulating the act of recording or photographing other people.
- Limit the definition of geolocation information to information that a digital electronic device generates for the purpose of accurately identifying the actual spatial location of the digital electronic device itself.