

**Testimony of in Support of HB 3284**  
**Senate Judiciary Committee**  
**May 6, 2021**  
**Christina Glabas, Gazelle Consulting**



Chair Prozanski and members of the Committee,

Thank you so much for the opportunity to speak with you today. My name is Christina Glabas I am the owner and founder of Gazelle Consulting, a HIPAA compliance and data privacy consulting firm in Portland. We work with a variety of different businesses including software developers, clinics, and nonprofits to help them comply with local privacy laws, such as the future HB3284, national privacy laws such as HIPAA, and international data privacy laws including GDPR in Europe, and PIPEDA in Canada.

This bill elevates our communication of privacy requirements significantly, by both simplifying the language and using forward thinking and broad terminology when describing technology.

**Exempting HIPAA**

In order to ensure that this bill does not conflict with HIPAA or inhibit the provision of care, we have included exemptions for covered entities under HIPAA, including healthcare providers, clearinghouses, and payers; as well as their vendors (known as business associates under HIPAA), to the extent that they are engaged in activities that are covered by HIPAA.

**De-identification**

We also want to ensure that this bill enables businesses to be successful in safeguarding data. Effective de-identification is critical to ensuring that data remains secure while allowing businesses to gather and use important data.

Therefore, the language in this bill has included de-identification requirements that match HIPAA de-identification standards, which are prescriptive regarding the 18 identifiers that must be removed. This includes “contextual identifiers,” such as an individual’s daily location activity, that could be used to infer identity. This is an important mechanism to protect minorities living in small communities and counties.

**Technology**

In terms of technology, we worked hard to ensure the language in this bill was as broad as possible. New forms of technology are evolving every day. Data that can be used to identify an individual’s locations can come from anything including wearables, household appliances, vehicles, mobile devices, videos, photos, and software.

But most importantly, AI and machine learning algorithms can use a variety of different data sources to infer an individual's location in ways that we can't necessarily predict. The language in the bill includes an up-to-date definition of geolocation data, which applies to all technology that could be used to identify an individual's location.

This bill includes multiple examples of this type of technology so that businesses understand how to comply, including but not limited to GPS, cell site data, and triangulated data from radio networks.

This bill also explicitly limits covered organizations from using personal health data for training machine learning algorithms related to or for subsequent use in commercial advertising or electronic commerce.

### **In Conclusion...**

It has been a true honor to participate in the development and revisions to this bill. I believe this bill is absolutely necessary to protect Oregonians and establish a framework for addressing data privacy in emergency or disaster situations.

AG Rosenblum, Kimberly McCullough, their team at the DOJ, and the team that they have assembled for the privacy work group is an impressive representation of consumer advocates, technologist, privacy specialist, and major technology companies.

I believe this bill will go far in protecting Oregonians and allowing businesses the flexibility to use the data to support their operations in an ethical way.